

Opportunistic Networks: The Concept and Research Challenges in Privacy and Security

Leszek Lilien, Zille Huma Kamal, Vijay Bhuse, and Ajay Gupta

WiSe (Wireless Sensornet) Lab
Department of Computer Science
Western Michigan University, Kalamazoo, MI 49008, USA
{llilien, zkamal, vsbhuse, gupta}@cs.wmich.edu

Abstract: We introduce a new paradigm and a new technology, which we call *opportunistic networks* or *oppnets*. An oppnet grows from its *seed*—the original set of nodes employed together at the time of the initial oppnet deployment. The seed grows into a larger network by extending invitations to join the oppnet to foreign devices, node clusters, or networks that it is able to contact. A new node that becomes a full-fledged member, or *helper*, may be allowed to invite external nodes. All helpers collaborate on realizing the goals of the oppnet. They can be employed to execute different kinds of tasks, even though in general they were not designed to become elements of the oppnet that invited them. Oppnets, as an epitome of pervasive computing, are subject to significant privacy and security challenges, inherent to all pervasive systems. To the best of our knowledge, we are the first to define and investigate opportunistic networks.

Keywords: Computer networks, opportunistic networks, privacy, security, pervasive computing, emergency response, disaster recovery

1. Introduction

We propose a new paradigm and a new technology of *opportunistic networks* or *oppnets* to enable an integration of the diverse communication, computation, sensing, storage and other resources that surround us more and more. We not only find ourselves in their midst but depend on them increasingly as necessities rather than luxuries. Few would deny that communications and computing are more and more pervasive.

The goal for oppnets is to leverage the wealth of pervasive resources and capabilities that are within our reach. This is often a treasure that remains useless due to “linguistic” barriers. Different devices and systems are either unable speak to each other, or do not even try to communicate. They remain on different wavelengths—sometimes literally, always at least metaphorically.

This occurs despite devices and systems gaining ground in autonomous behavior, self-organization abilities, adaptability to changing environments, or even self-healing when faced with component failures or malicious attacks. It might look somewhat ironic to a person unaware of interoperability challenges that such ever more powerful and intelligent entities are not making equally great strides in talking to each other.

With oppnets, we chart a new direction within the area of computer networks. To the best of our knowledge it is a direction not explored in this way by others. A co-author of this paper invented opportunistic *sensor* networks [BLWR04]. The idea was later generalized to opportunistic networks [LiGu06]. We are now the first to scrutinize oppnets and their inherent challenges.

The oppnets and their salient features can be characterized as follows. Typically, the nodes of a single network are all deployed together, with the size of the network and locations of its nodes pre-designed (either in a fully “deterministic” fashion, or with a certain degree of randomness, as is the case with ad hoc or mobile

networks). In contrast, the size of an oppnet and locations of all but the initial set of its nodes—known as the *seed nodes*—can not be even approximately predicted. This is the category of networks where diverse devices, *not* employed originally as its nodes, are invited to join the seed nodes to become oppnet *helpers*. Helpers perform certain tasks they have been invited (or ordered) to participate in. By integrating helpers into its fold, a *seed oppnet* grows into an *expanded oppnet*.

The oppnet goals can be realized by alleviating first of all the communication problems—including bottlenecks and gaps—that are often the root causes of resource shortages (similarly as transportation inadequacies—not a lack of food in the world—are the root causes of famines).

If the researchers, developers, and manufacturers succeed in building oppnets, the payoff will be swift and substantial. Armies of helpers, mobilized by oppnets, will be capable of contributing towards their objectives at a very low or no cost, especially in emergency situations.

The potential of oppnets in all kinds of emergency situations—including man-made and natural disasters—is especially noteworthy. In the past few years we have seen great disasters, such as 9/11 terrorist attack, tsunami in the Southeast Asia and Hurricane Katrina. The casualties and damages are too often compounded by problems faced by the first responders and relief agency workers. There is a common thread to all these problems: lack of adequate communication facilities in the disaster areas and beyond. Therefore, providing means of dependable communication in emergencies must be viewed as a fundamental challenge to communication and information technologies.

The following scenario illustrates a possible use of an oppnet deployed after an earthquake. One of its helpers, a surveillance system, “looks” at a public area scene with many objects. The image is passed to another helper that analyzes it, and recognizes one of the objects as an overturned car. Another helper decides that the license plate number of the car should be obtained, and (maybe another) image analysis helper provides this information. The plate number is used by another helper to check in a vehicle database whether the car is equipped with the OnStar™ communication system. If it is, the appropriate OnStar center facility is contacted, becomes a helper, and obtains a connection with the OnStar device in the car. The OnStar device in the car becomes a helper and is asked to contact BANs (body area networks) on and within bodies of car occupants. Each BAN available in the car becomes a helper and reports on the vital signs of its owner. The reports from BANs are analyzed by prioritizing helpers that schedule the responder teams to ensure that people in the most serious condition are rescued sooner than others. With the exception of the BAN link that is just a bit futuristic (its widespread availability could be measured in years not in decades), all other helper capabilities are already quite common.

With so many helper capabilities available, we need “only” to integrate them in a clever way. We believe that our paradigm provides a very useful framework—including a conceptual frame of thought—for such integration.

We can look at oppnets as an epitome of pervasive computing. The most critical problems inherent to pervasive computing were very aptly expressed as follows [Thib02]:

Pervasive computing has pervasive problems, not the least of which are interoperability, security and privacy.

Oppnets confront all three enumerated problems head on (though in this paper we concentrate on the discussion of privacy and security issues). Therefore, work on oppnets will be a test case for attacking the pervasive computing problems.

The next Section describes the basics of oppnet operation. Section 3 delineates scenarios for benevolent and malevolent uses for oppnets. Section 4 briefly presents areas of related work. Privacy and security challenges facing oppnets are presented in Sections 5 and 6. Finally, Section 7 concludes the paper and sketches directions for future work.

2. Basics of Oppnet Operation

A. Seed Oppnet and Its Growth

Each opportunistic network grows from a *seed* that is a set of nodes employed together at the time of the initial oppnet deployment. The seed is pre-designed (and can therefore be viewed as a network in its own right). In the extreme it can consist of a single node.

The seed grows into a larger network by extending invitations to join the oppnet to foreign devices, node clusters, networks, or other systems which it is able to contact. Any new node that becomes a full-fledged oppnet member, that is a *helper*, may be allowed to invite external nodes. By inviting “free” collaborative nodes, the opportunistic networks can be very competitive economically. The issues that have to be addressed are proper incentives or enforcements so that invited nodes are willing or required to join, and potentially lower credibility of invited collaborators that, in general, can’t be fully trusted (at least till they prove themselves). Helpers collaborate on realizing the oppnet’s goal. They can be deployed to execute all kinds of tasks even though, in general, they were not designed to become elements of an oppnet that invites them.

B. Oppnet Helpers

1) *Potential Oppnets Helpers:* The set of helpers includes even entities not usually thought of as network nodes, both wired and wireless, free-standing and embedded. Even nodes with no sensing capabilities, such as networked mainframes from LANs or wireless-equipped processors embedded in cars, can significantly contribute to processing or communication capabilities of an oppnet. After all, any networked PC or embedded processor has some useful sensing, processing, or communication capabilities. For example, information about user’s presence or absence, her work habits and Internet access patterns can be collected by her desktop and her PDA; information about user’s location – by his cellphone (even one without GPS can be triangulated); and data about food consumed by user’s household – by a processor embedded in a refrigerator and RFID-equipped food packages and containers. As an example, a PC becomes “invariable” once the seed identifies a subset of IP addresses located in its geographical area and contacts them. In larger areas, it is not difficult to do, with IP addresses hierarchically organized by location.

2) *Helper Functionalities:* It should be noted that, in general, working in the “disaster mode” does not require any new functionalities from the helpers. For example, in case of fire monitoring tasks, the weather sensornet that became a helper can be simply told to stop collecting precipitation data, and use the released resources to increase the sampling rates for temperature and wind direction.

It is possible that more powerful helpers could be reprogrammed on the fly. Also, oppnet nodes might be built with excess general-purpose communication, computation, storage, sensing, and other capabilities useful in case of unforeseen emergencies. For example, excess sensing capabilities could be facilitated by multisensor devices that are becoming cheaper and cheaper as new kinds of sensors are being developed all the time (for example, novel biosensors for detection of anthrax [IHRR02]).

C. Critical Mass for an Oppnet and Growth Limitations

1) *Critical Mass:* Oppnets can be really effective if they are able to build up their size (by inviting other nodes) enough to reach a certain “critical mass” in terms of size, node locations, and node capabilities. Once this threshold is passed, they are ready to communicate, calculate, and measure aspects of entities and physical environment in their midst in an unprecedented detail. They can gather data for damage assessment when used in emergencies or disaster recovery. Some sensornets that become helpers—such as sensor nodes embedded in roads, buildings, and bridges—are designed primarily for damage assessment. Others helpers (whether from sensornets or not) can gather data—legitimately or not—on general public, employees, or other monitored individuals.

2) *Growth Limitations:* The network stops inviting more nodes when it obtains enough helpers providing sufficient sensing, processing, and communication capabilities (cost/benefit analysis of inviting more nodes might be performed). It should avoid recruiting superfluous nodes that wouldn't help and might reduce performance by using resources just to "gawk." This does not mean that network configuration becomes frozen. As the area affected by the monitored activity (e.g., an earthquake) changes and the required monitoring level (due, say, to the severity of damage) in different locations shifts, the oppnet reconfigures dynamically, adapting its scope and its capabilities to its needs (e.g., to the current disaster recovery requirements).

D. Applications for Oppnets

1) *Emergency Applications:* We see important applications for opportunistic networks in all kinds of emergency situations, for example in hurricane disaster recovery and homeland security emergencies. We believe that they have the potential to significantly improve efficiency and effectiveness of relief and recovery operations. For predictable disasters (like hurricanes or firestorms, whose path can be predicted with some accuracy), seed oppnets can be put into action and their build-up started (or even completed) *before* the disaster, when it is still much easier to locate and invite other nodes and clusters into the oppnet. The first helpers invited by the seed could be the sensornets deployed for structural damage monitoring and assessment, such as the ones embedded in buildings, roads, and bridges.

2) *Benevolent and Malevolent Oppnet Applications:* As most technologies, opportunistic networks can be used to either benefit or harm humans, their artifacts, and technical infrastructure they rely upon. Invited nodes might be "kept in the dark" about the real goals of their host oppnets. Specifically, "good guys" could be cheated by a malevolent oppnet and believe that they will be used to benefit users. Similarly, "bad guys" might be fooled by a benevolent oppnet into believing that they collaborate on objectives to harm users, while in fact they would be closely controlled and participate in realizing positive goals.

On the negative side, home-based opportunistic networks could be the worst violators of individual's privacy, if they are able to exploit PCs, cellphones, computer-connected security cameras, embedded home appliance processors, etc.

3) *Counteracting Malevolent Oppnet Applications:* To counteract malevolent oppnets threats, *predator* networks that feed on all kinds of malevolent networks—including malevolent oppnets—can be created. They detect malevolent nets, plant spies in them, and use the spies to discover true goals of suspicious networks (some of the suspicious networks might actually be benevolent ones, victims of false positives). Conversely, intelligent adversaries can deploy malevolent predator networks that feed on all kinds of benevolent networks, including benevolent opportunistic networks.

3. Example Oppnet Use Scenarios

Below we show two example oppnet application scenarios: a benevolent one and a malevolent one. Both rely on some reconfiguration capabilities of non-opportunistic (regular) sensornets.

A. Benevolent Oppnet Scenario — "Citizens Called to Arms"

A seed oppnet is deployed in the area where an earthquake occurred. It is an ad hoc wireless network with nodes much more powerful than in a "typical" ad hoc network (more energy, computing and communication resources). Once activated, the seed tries to detect any nodes that can help in damage assessment and disaster recovery. It uses any available method for detection of other networks, including radio-based (including cellphone-based) detection, searching for nodes using the IP address range for the affected geographic area, and even AI-based visual detection of some appliances and PCs (after visual detection, the seed still needs to find a network contact for a node to be invited).

The oppnet "calls to arms" the optimal subset of detected and contacted "citizens," inviting all devices, clusters, and entire networks, which are able to help in communicating, computing, sensing, etc. In emergency

situations, entities with any sensing capabilities (whether members of sensornets or not), such as cellphones with GPS or desktops equipped with surveillance cameras, can be especially valuable for the oppnet.

Let us suppose that the oppnet is able to contact three independent sensornets in the disaster area, deployed for weather monitoring, water infrastructure control, and public space surveillance. They become helper candidates and are ordered (this is a life-or-death emergency!) to immediately abandon their normal daily functions and start assisting in performing disaster recovery actions. For example, the weather monitoring sensornet can be called upon to sense fires and flooding, the water infrastructure sensornet with multisensor capabilities (and positioned under road surfaces) —to sense vehicular movement and traffic jams, and the public space surveillance sensornet —to automatically search public spaces for images of human victims.

B. Malevolent Oppnet Scenario — “Bad Guys Gang Up”

Suppose that foreign info warriors use agents or people unaware of their goals to create an apparently harmless weather monitoring sensornet. Only they know that, when activated, the original sensornet becomes a seed of a malevolent oppnet. The sensornet starts recruiting helpers.

The seed will not reveal its true goals to any of its helpers. Instead, it uses a cover of a beneficial application, proclaiming to pursue weather monitoring for research. Actually, this opportunistic sensornet monitors weather but for malicious reasons: it analyzes wind patterns that can contribute to a faster spread of poisonous chemicals. Once the “critical mass” in terms of geographical spread and sensing capabilities is reached, the collected data can be used to make a decision on starting a chemical attack.

4. Related Work Areas

Oppnets might be perceived as networks that lie within the intersection of ad hoc networks, P2P systems, and sensor networks. They can use (after modifications) ad hoc node localization and self-organization techniques from ad hoc networks, growth-by-joining approaches from P2P systems, and data aggregation algorithms from sensornets. Hence, the fact that a lot of related work comes from these three areas should not be surprising. However, we look at three more categories of related work.

There are six major areas of related technologies useful for opportunistic networks, that we identified and explore for useful methods, protocols, and algorithms:

1. Ad hoc networks
2. Peer-to-peer systems
3. Sensornet
4. Grid computing (for resource integration and management)
5. Benevolent Trojans (for helper search)
6. Miscellaneous other (e.g., techniques from the CenWits project from the University of Colorado).

There is a tremendous amount of knowledge and experience in the above areas that we can learn from but we can not employ any of the existing techniques ‘as-is’ in our opportunistic networks, due to unique characteristic of oppnets.

We omit the details as not necessary in this Privacy and Security Research Challenges paper.

5. Privacy Challenges in Oppnets

The proposed opportunistic network technology is one of possible approaches for moving towards the ultimate goal of pervasive computing. Since huge privacy risks are associated with all pervasive computing approaches, oppnets—being such an approach—must face significant privacy perils.

Pervasiveness must breed privacy threats, as we explain in our 2004 paper [BLRW04]:

Pervasive devices with inherent communication capabilities might [...] self-organize into huge, opportunistic sensor networks, able to spy anywhere, anytime, on everybody and everything within their midst. [...] Without proper means of detection and neutralization, no one will be able to tell which and how many snoops are active, what data they collect, and who they work for (an advertiser? a nosy neighbor? Big Brother?). Questions such as “Can I trust my refrigerator?” will not be jokes—the refrigerator will be able to snitch on its owner’s dietary misbehavior to the owner’s doctor.

We very clearly recognize the crucial issue of privacy in oppnets (as well as in all other pervasive computing approaches). Privacy guarantees, are indispensable for realization of the promise of pervasive computing. We strongly believe that without proper privacy protection built into any technology attempting to become pervasive, the public will justifiably revolt against it. Any oppnet solution (or other pervasive computing solution) compromising on privacy protection is doomed to a total failure. Simply, *privacy protection is the “make it or break it” issue for oppnets and pervasive computing in general.*

There is no inherent reason why an oppnet would need to enslave the device asked to help it, exploiting its sensitive resources. There is no inherent reason why the helper device would need to disclose all such resources to the oppnet. In the simplest solution, the candidate helper will keep its private data in a secure vault (e.g., enciphered in its storage) before agreeing to join an oppnet that asked for help. In case of an involuntary conscription (in an emergency situation), the oppnet will allow the candidate helper to save private data in helper’s own vault before mustering it.

Other solution we consider will rely on a strict separation of private and public areas within the helper device or network. This will ensure that a benevolent oppnet will never (even when it malfunctions) attempt to capture helper’s private data. It will also provide protection against malevolent oppnets that might attack privacy of other devices or networks pretending they need them as their helpers.

Still other techniques—proposed in [Lili05]—include:

- Protecting privacy of entities (including oppnet helpers) that are under oppnet surveillance by, for example, assuring their anonymity or pseudonymity.
- Providing algorithms for detecting malevolent oppnet, which masquerade as benevolent oppnets in order to attack prospective helpers. Detection will deny them opportunity to compromise privacy of helpers.
- Developing methods to protect oppnets against all kinds of privacy attacks, and to disable malicious uses of oppnets for privacy attacks.

Some relaxation of the strictest privacy protection standards might be permissible in emergency situation, especially in life-and-death situations. For example, a victim searching for help will probably not object to an oppnet taking over her Body Area Network (BAN), controlling devices on and within her body. We will consider exploring this possibility with a full concern for legal and ethical issues involved. If we do, we will follow two basic assumptions: (1) an entity should give up only as much privacy as is indispensable for becoming a helper for the requesting oppnet; and (2) an entity’s privacy disclosure should be proportional to the benefits expected for the entity or to a broader common good. The latter is especially important in emergencies, when the goals like saving a life of one person takes precedence over the comfort of another.

Our earlier work on privacy includes a solution for privacy-preserving data dissemination [LiBh05], which we might adapt to improve the oppnet-helper relationships.

Finally, we need to note that privacy (and security) in pervasive computing is a very active investigation area. We can use many other privacy solutions conceived by other researchers working on networks and, in general, on pervasive computing.

6. Security and Privacy Challenges for Oppnets

One of the sources of privacy and security threats is the fact that authentication cannot, in general, be performed when devices join the network. It is not possible to *guarantee* that malicious devices will not join. Moreover we might not be able to classify or rate devices as malicious until they join the oppnet, and we detect their notorious behavior. Delivering secret keys securely to all non-malicious devices (and only to non-malicious devices) is very difficult in such an ad hoc environment. Hence, relying alone on cryptography-based authentication mechanisms (e.g., Kerberos) will not help in all situations. So, MITM, packet dropping, ID spoofing (masquerading), DoS and other attacks are even bigger threats in oppnets. If not controlled, they can defeat the purpose of oppnet.

Figure 1 displays general security scheme for oppnets. In the absence of initial authentication mechanism all five steps marked by outgoing arrows from the adder circle are mandatory.

The privacy and security challenges for opportunistic networks can be listed as follows (in the order in which, we think, they should be investigated):

- A. Increasing trust and secure routing
- B. Helper privacy and oppnet privacy
- C. Protecting data privacy
- D. Ensuring data integrity
- E. Identifying most dangerous attacks and sketching solutions
- F. Intrusion detection

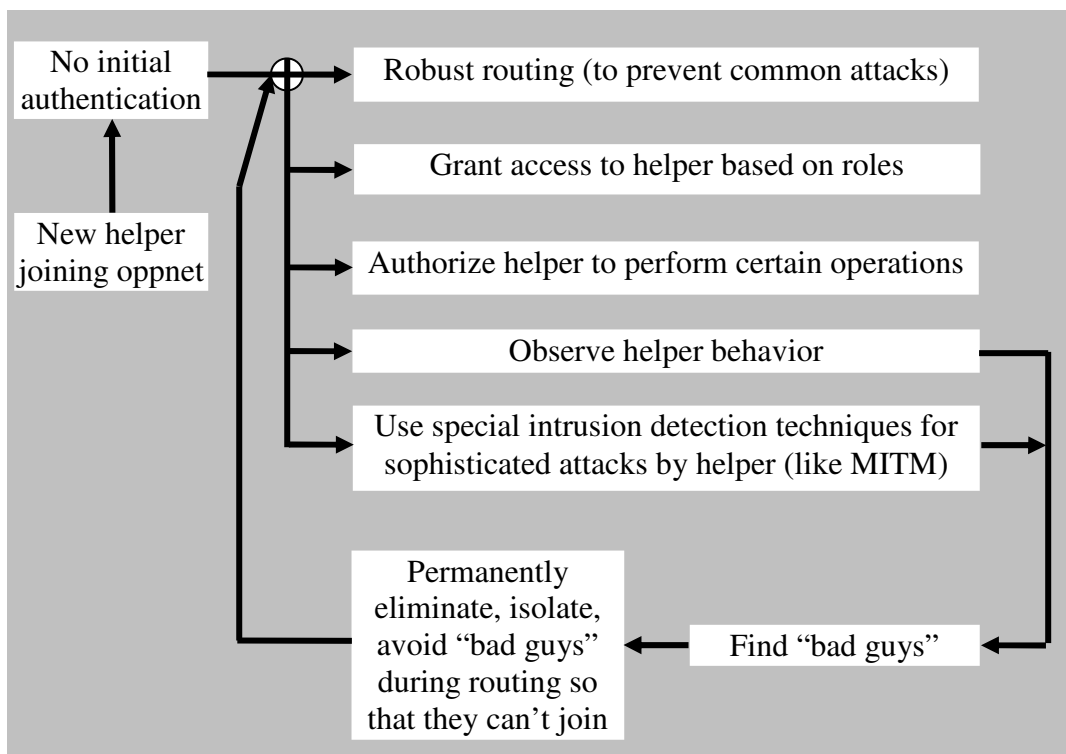


Fig. 1. General oppnet security scheme.

A. Increasing Trust and Secure Routing

A list of “more trusted” devices can be maintained. For example, we can trust more the devices owned by certain institutions, such as devices at police stations, government offices, hospitals, public libraries, universities or reputable companies. Once a list of trusted devices is made (which is a challenge), these devices will be used for more critical tasks than unknown devices or distrusted devices (such a ‘black list’ could be maintained as well). Secure routing can use both lists. Selecting a route that passes through only trusted devices (or as many trusted devices as possible) is challenging. Numerous papers have been written on individual ad hoc routing protocols. A survey of secure wireless ad hoc routing can be found in [HuPe04].

Secure wireless ad hoc routing protocol most relevant to oppnet is Ariadne [HuPJ02]. It is an on-demand protocol that works in the presence of compromised nodes. Ariadne uses symmetric cryptography. It authenticates routing messages using one of the three schemes:

- Shared secrets between each pair of nodes.
- Shared secrets between communicating nodes combined with broadcast authentication.
- Digital signatures.

Solutions proposed for securing routing protocols in wireless or ad hoc networks or the Internet cannot be used directly in oppnets because oppnets are highly heterogeneous. Their nodes have different processing abilities, power sources, modes of transmission (wired or wireless), etc. The proposed approaches—e.g., IPSec, WEP and ssh—use mostly cryptographic solutions to minimize the probability and effects of possible attacks.

Trusted devices with battery power should be used sparingly to increase their lifetime. This is necessary to maintain network connectivity, the goal of oppnet. This might be easier in oppnets than in other systems, as oppnets can rely on growth to amass needed resources (even with a big safety margin).

B. Helper Privacy and Oppnet Privacy

In this section, by “protecting privacy of the system” we mean no intrusions into the system, no illegal access to data, resources and software of systems. So by privacy we do not mean data privacy or confidentiality which is discussed in Subsection 6.C.

Oppnet can be feasible only if privacy of helpers can be guaranteed. Privacy of a helper can be guaranteed by its access controls (authentication and authorization) and by its intrusion prevention (using security primitives, relying on trust, secure routing etc.).

Intrusion detection should be used as the second line of privacy defense for helpers when prevention fails or cannot be used due to its inefficiency. Elimination or isolation of bad entities from oppnet via intrusion detection is very important for benevolent nodes. The problem of guaranteeing access control and performing real-time intrusion detection for oppnets are more difficult than for the Internet, wireless or ad hoc networks because of the highly heterogeneous nature of participating devices and the spontaneous manner in which oppnets are formed.

Privacy of oppnet is also important. Malicious entities can join the oppnet with the sheer purpose of violating privacy of oppnet members. A fear of having one’s privacy violated can prevent candidate helpers invited by an oppnet from joining, or can cause reluctance (a passive or an active resistance) of the candidate helpers ordered by an oppnet to join.

Since it is very difficult to uncover the motives of any device or system invited/ordered by an oppnet to join, the only way to find bad helpers is by intrusion detection.

C. Protecting Data Privacy

In the subcategory of oppnets that have a central controller, the following kinds of messages are most important.

1) *Broadcast from the controller*: Mostly some announcements may be made by the controller (for e.g. water

level will rise by 6 inches in half an hour in the whole city) for which privacy might not be desired. But there can be messages from the controller which may require privacy since they will be intended to only few nodes in the oppnet. The lack of shared secret or a key between the controller and intended recipients makes the problem of providing data privacy difficult. Even if we assume that there is a shared secret key (for symmetric key cryptography encryption) between controller and intended recipients, the biggest problem with the symmetric key cryptography is capture of even a single device (especially in crisis when providing physical protection is even more difficult) leading to the failure of the whole scheme.

2) *Messages from nodes to the controller:* These messages may require privacy. (You may have to tell something to your manager but may not want to share with your colleagues.) Encryption is a way of providing data privacy. Asymmetric key cryptography (or public key cryptography, using PKI) can be used to protect privacy of messages from nodes to the controller. The controller can broadcast its public key to all the devices in the oppnet. Devices can encrypt their data with the public key and the controller can decrypt them with its private key. So when data is traveling towards the controller, the nodes that forward them can see only their encrypted form.

A malicious device can pose as a controller by distributing its own public key. The above will not work if the controller cannot exclude such 'competition' in distributing its forged public key. We need a secure mechanism to broadcast a public key either before an emergency (for predictable emergencies, to potential helpers that can be identified), during an emergency, or after an emergency.

Apart from the above discussed messages, messages in oppnet might be sent from one device to another device (peer to peer), or there can be intra-cluster communication among devices in some specific area. A local cluster head (a trusted device doing an extra job) can use public key cryptography while communicating with its neighbors. A cluster head can announce its public key. Nodes can encrypt data with the public key and, upon receiving encrypted data, the cluster head can decrypt them with its private key. But a malicious device can pose as a cluster head and can distribute its own public key. So, this approach will not work if the cluster head cannot exclude such 'competition' in distributing its forged public key.

D. Ensuring Data Integrity

Data integrity is a part of data security, also a part of any secure communication. Digital signatures can be used to guarantee integrity of data. But they are too expensive computationally for weak devices (like cellphones, PDAs etc.) running on a limited battery power. Hence, alternatives should be devised to guarantee integrity of data packets.

Also, packet sizes may vary when it travels through an oppnet. Suppose that a packet is sent from a cellphone to the base station through a PC connected to the Internet. In this case, the packet size when it travels from the cellphone to the PC will be different from the packet size when it travels from the PC to the base station. If packet fragmentation and aggregation cannot be performed securely, the end-to-end security mechanisms could fail.

E. Identifying Most Dangerous Attacks and Sketching Solutions

Below we discuss some of the most important attacks, their effects and initial solutions to prevent those attacks.

- *MITM:* Suppose a malicious device is on the path connecting a person in the house that needs help and the central controller. In this case, if the person sends request destined to the controller, the malicious device instead of forwarding it might inform the person that help is on the way. It could also tamper with messages broadcast by the controller.

Solution: A person in need can send redundant messages to the controller through multiple neighbors. This will increase the chances that least one of the multiple message copies will reach the controller, even if there are attackers on some paths. So, redundancy of routes can be exploited to avoid the attackers.

- *Packet dropping:* The malicious device in the above scenario might drop some or all the packets between the

person in need and the controller. In the worst case, it might forward packets containing insignificant information and drop packets containing critical information.

Solution: The above proposed idea of sending redundant messages using multiple neighbors may work if no adversary is situated on at least one path. Again, redundancy of routes can be exploited to avoid the attackers.

- *DoS attacks by malicious devices:* False requests for help can be generated by malicious devices. They will keep the rescue team busy and unavailable for real emergencies.

Solution: Upper limit can be placed on the number of requests any device can generate. Thus, it will limit the number of times any device can send a false help request. In addition, the rescue team can attempt contacting the requester to confirm an emergency request.

- *DoS attacks on weak links:* DoS attacks may target a “weak” device, such as a cellphone that is critical to oppnet operation (e.g., if it is the only device that connects two parts of a city). The battery of the cellphone is a very precious resource and should be used sparingly till an alternative connection is found. Some attacks may target only critical weak devices. Such surgical attacks are capable of defeating the goal of oppnets, which is to maintain connectivity in crisis.

Solution: Identification of weak devices, their strengthening (e.g., providing backups for them), or minimizing their workload is a major task for maintaining connectivity in oppnets.

- *ID spoofing:* Mapping some node properties (like location) into node ID by a controller can be dangerous. A malicious device capable of masquerading can generate requests with multiple IDs, resulting in many false alarms for the rescue team. Services that need authentication can be misused if their IDs can be spoofed. A device capable of spoofing ID of a trusted node or a node with critical functions can pose many kinds of attacks.

Solution: Although it is difficult to guarantee that malicious nodes will not join the oppnet, nodes can watch their neighbors for possible attempts of ID spoofing. The SAVE protocol [LMRZ01] can provide routers with information needed for source address validation. This protocol needs to be modified to suit the heterogeneous nature of oppnets.

F. Intrusion Detection

Malicious devices or malicious networks will be able to join an oppnet because of the *lack* of an initial authentication mechanism. Therefore, there is a need to detect and isolate malicious nodes, clusters, or networks. Securely distributing information about malicious entities in the presence of malicious entities is a challenge. If shared securely, this second-hand reputation information can be used by all oppnet nodes to protect themselves from attackers. Even if that information could be distributed securely, avoiding those entities while maintaining connectivity is another challenge.

For a review of intrusion detection in wireless ad hoc networks we refer reader to [MiNP04]. However, we need to emphasize that the highly heterogeneous nature of oppnets makes real-time intrusion detection and response in them even more challenging than in other types of networks.

The intrusion detection approach most relevant for oppnets comes from the AAFID project [Zamb01], in which autonomous agents perform intrusion detection using embedded detectors. An embedded detector is an internal software sensor that has added logic for detecting conditions that indicate a specific type of attack or intrusion. Embedded detectors are more resistant to tampering or disabling, because they are a part of the program they monitor. Since they are not executing continuously, they impose a very low CPU overhead. They perform direct monitoring because they have access to the internal data of the programs they monitor. Such data does not have to travel through an external path (a log file, for example) between its generation and its use. This reduces the chances that data will be modified before an intrusion detection component gets it.

7. Conclusions

This paper presents the new concept of *opportunistic networks (oppnets)*, and presents related research challenges.

Oppnets constitute a newly identified category of computer networks. When deployed, oppnets attempt to detect systems existing in their relative vicinity—ranging from sensing and monitoring, to computing and communication systems—and integrate them under their own control. When such a system is detected, oppnet evaluates its potential benefit, and—if the evaluation is positive—invites it to become its *helper*. In this manner, an oppnet can grow from a small seed into a stupendous network with vast sensing, communication, and computation capabilities.

An integrated network has been called for in various critical or emergency situations [USGo01]. Oppnet can be used to enable connectivity in an area where any existing communication or information infrastructure has been fractured or partially destroyed. It integrates various systems that were not designed to work together to facilitate creation of a bigger and better picture of the region it is deployed in. The integration allows flow of information that, for example, can assist in rescue and recovery efforts for devastated areas, or can provide more data on phenomena that are just developing, such as wildfires or flash torrents.

Answering to the identified challenges in oppnets will contribute to advancing knowledge and understanding of the opportunistic networks, while simultaneously advancing the state of the art of the general-purpose computer networks.

We take on many challenges, continuing our investigation of oppnets, and designing oppnet architectures with their associated components: methods, protocols, and algorithms. The planned prototype opportunistic network will provide a proof of concept, as well as stimulation and feedback necessary for fine-tuning oppnet architectures and their components

Acknowledgements

This work was supported in part by the National Science Foundation under Grant IIS-0242840, and in part by the U.S. Department of Commerce under Grant BS123456.

The authors would also like to acknowledge Western Michigan University for its support and its contributions to the WiSe (Wireless SensorNet) Laboratory, Computational Science Center and Information Technology and Image Analysis (ITIA) Center.

L. Lilien, a co-PI on the NSF grant providing a partial support for this research, would like to thank Professor Bharat Bhargava from Purdue University, the PI for this grant. He is affiliated with the CERIAS security center at Purdue University.

Any opinions, finding, conclusions or recommendation expressed in the paper are those of the authors and do not necessarily reflect the views of the funding agencies or institutions.

References and Bibliography

- [AnYC05] Z. Anwar, W. Yurcik, and R. H. Campbell, "A Survey and Comparison of Peer-to-Peer Group Communication System Suitable for Network-Centric Warfare," *SPIE* 2005.
- [BaPa00] P. Bahl and V.N. Padmanabhan, "RADAR: An In-Building RF-based User Location and Tracking System," *INFOCOM* (2), March 2000, pp. 775-784.
- [BFHX05] X. Bao, B. Fang, M. Hu, and B. Xu, "Heterogeneous Search in Unstructured Peer-to-Peer Networks," *IEEE Distributed Systems Online*, vol. 6, no. 2, 2005.
- [BoGS03] A. Boulis, S. Ganeriwal, and M. Srivastava, "Aggregation in Sensor Networks: An Energy Accuracy Trade-off," *Proc. 1st IEEE Intl. Workshop on Sensor Network Protocols and Applications (SNPA'03)*, May 2003, Anchorage, Alaska.

- [BEGH01] N. Bulusu, D. Estrin, L. Girod and J. Heidemann, "Scalable Coordination for Wireless Sensor Networks: Self-Configuring Localization Systems," *Proc. Sixth Intl. Symp. on Communication Theory and Applications (ISCTA 2001)*, Ambleside, United Kingdom, July 2001.
- [BLRW04] B. Bhargava, L. Lilien, A. Rosenthal, and M. Winslett, "Pervasive Trust," *IEEE Intelligent Systems*, vol. 19(5), Sep./Oct.2004, pp. 74-77.
- [CeEs02] A. Cerpa and D. Estrin, "ASCENT: Adaptive Self-Configuring Sensor Networks Topologies," *Proc. Twenty First Intl. Annual Joint Conf. of the IEEE Computer and Communications Societies (INFOCOM 2002)*, New York, NY, June 2002.
- [ChHa03] S. Chatterjea, and P. Havinga, "A Dynamic Data Aggregation Scheme for Wireless Sensor Networks," *ProRISC 2003*, November 2003, Veldhoven, Netherlands.
- [ChBe02] W. Cheswick and S. Bellovin, *Firewalls and Internet Security*, 2nd ed., Addison-Wesley, 2002.
- [Flor03] R. A. Flores-Mendez, "Towards Standardization of Multi-Agent System Frameworks," 2003.
<http://turing.acm.org/crossroads/xrds5-4/multiagent.html>
- [Gong02] L. Gong, "Peer-to-Peer Networks in Action," *IEEE Internet Computing*, January – February 2002.
- [GuAA05] A. Gupta, D. Agrawal, and A. E. Abbadi, "Distributed Resource Discovery in Large Scale Computing," *SAINT 2005*.
- [Hein00] W. Heinzelman, "Application-Specific Protocol Architectures for Wireless Networks," Ph.D. Thesis, Department of Electrical Engineering and Computer Science, MIT, Cambridge, MA, June 2000.
- [HiBo01] J. Hightower and G. Borriello, "Location Systems for Ubiquitous Computing," *IEEE Computer*, August 2001.
- [HeCB00] W. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "Energy-efficient Communication Protocol for Wireless Microsensor Networks," *Proc. 33rd Intl. Conf. on System Sciences (HICSS)*, January 2000.
- [HSIG01] J. Heidemann, F. Silva, C. Intanagonwiwat, R. Govindan, D. Estrin, and D. Ganesan, "Building Efficient Wireless Sensor Networks with Low-Level Naming," *Proc. 18th ACM Symp. on Operating Systems Principles*, October 2001.
- [HVBW01] J. Hightower, C. Vakili, G. Borriello, and R. Want, "Design and Calibration of the SpotOn Ad-Hoc Location Sensing System," unpublished manuscript, August 2001.
- [HuPJ02] Y.-C. Hu, A. Perrig, and D.B. Johnson, "Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks," *Proc. 8th Ann. Int'l Conf. Mobile Computing and Networking (MobiCom 2002)*, Atlanta, Georgia, September 2002, pp. 12–23.
- [HuPe04] Y.-C. Hu and A. Perrig, "A Survey of Secure Wireless Ad Hoc Routing," *IEEE Security & Privacy*, Special Issue on Making Wireless Work, Vol. 2(3), May/June 2004, pp.28-39.
- [IHRR02] H. Inerowicz, S. Howell, F. Regnier, and R. Reifenberger, "Protein Microarray Fabrication for Immunosensing," *Proc. 224th American Chemical Society (ACS) National Meeting*, Aug. 2002.
- [ItGE00] C. Itanagonwiwat, R. Govindan, and D. Estrin, "Directed Diffusion: A Scalable and Robust Communication Paradigm for Sensor Networks," *Proc. Sixth Annual Intl. Conf. on Mobile Computing and Networks (MobiCom)*, 2000.
- [IyBr03] S. Iyenger and R. Brooks, *Distributed Sensor Networks*, CRC Press, Inc., 2003.

- [KrEW02] B. Krishnamachari, D. Estrin, and S. Wicker, "The Impact of Data Aggregation in Wireless Sensor Networks," *Proc. Intl. Workshop on Distributed Event Based Systems (DEBS)*, Vienna, Austria, July 2002.
- [KuWu01] H.T. Kung and C. H. Wu, "Hierarchical Peer-to-Peer Networks," Technical Report IIS-TR-02-015, Institute of Information Science, Academia Sinica, Taiwan, April 2001.
- [LiBh05] L. Lilien and B. Bhargava, "A Scheme for Privacy-preserving Data Dissemination," *IEEE Transactions Systems, Man, and Cybernetics*, accepted, final version submitted in October 2005, to appear.
- [LiGu06] L. Lilien and A. Gupta "Opportunistic Networks for Emergency Preparedness and Response," submitted for publication.
- [Lili05] L. Lilien, "Opportunistic Sensor Networks," Proposal to the Faculty Research and Creative Activities Support Fund (FRACASF), Western Michigan University, December 2, 2005.
- [LMRZ01] J. Li, J. Mirkovic, M. Wang, P. Reiher, and L. Zhang. "SAVE: Source Address Validity Enforcement Protocol," UCLA Technical Report 01-0004, Los Angeles, CA, 2001.
- [MiNP04] A. Mishra, K. Nadkarni, A. Patcha, "Intrusion Detection in Wireless Ad Hoc Networks", *IEEE Wireless Communications*, Vol. 11(1), February 2004, pp. 48-60.
- [Mena03] D.A. Menascé, "P2P Search," *IEEE Internet Computing*, March – April 2003.
- [MICA03] MICA2 Wireless Measurement System Datasheet, Crossbow Technology Inc., San Jose, CA, September 2003,
http://www.xbow.com/Products/Product_pdf_files/Wireless_pdf/6020-0042-01_A_MICA2.pdf.
- [MOWW04] T. Moscibroda, R. O'Dell, M. Wattenhofer, and R. Wattenhofer, "Virtual Coordinates for Ad Hoc and Sensor Networks," *ACM Joint Workshop on Foundations of Mobile Computing (DIALM-POMC)*, Philadelphia, Pennsylvania, USA, October 2004.
- [Mote03] Mote Documentation and Development Information, UC Berkeley, Berkeley, CA, 2003, <http://www.cs.berkeley.edu/~awoo/smartdus>.
- [OnSt05] "On Star Explained," Accessed on November 26, 2005,
http://www.onstar.com/us_english/jsp/explore/index.jsp
- [Oppe78] A. Oppenheim, *Applications of Digital Signal Processing*, Prentice-Hall, Inc., 1978.
- [PBSJ05] P.N. Pathirana, N. Bulusu, A.V. Savkin, and S. Jha, "Node Localization Using Mobile Robots in Delay-Tolerant Sensor Networks," *IEEE Transactions On Mobile Computing*, Vol. 4, No. 3, May/June 2005, pg 285-296.
- [PrCB00] N. Priyantha, A. Chakraborty, and H. Balakrishnan, "The Cricket Location Support System," *Proc. ACM Int'l Conf. Mobile Computing and Networking (MobiCom '00)*, pp. 32-43, Aug. 2000.
- [Ripe02] M. Ripeanu, "Peer-to-peer Architecture Case Study: Gnutella Network," *Internet2 Workshop: Collaborative Computing in Higher Education: Peer-to-Peer and Beyond*, January, 2002, Tempe, Arizona.
- [SaHS01] A. Savvides, C. Han, and M. Srivastava, "Dynamic Fine-Grained Localization in Ad-Hoc Networks of Sensors," *Proc. ACM Int'l Conf. Mobile Computing and Networking (MobiCom '01)*, pp. 166-179, July 2001.
- [SMKKB01] I. Stoica, R. Morris, D. Karger, M. F. Kaashoek, and H. Balakrishnan, "Chord: A scalable peer-to-peer lookup service for internet applications," *Proc 2001 Conf. on Applications, Technologies*,

Architectures, and Protocols for Computer Communications (SIGCOMM), pages 149–160. ACM Press, 2001.

- [TGBKS04] M. Terwilliger, A. Gupta, V. Bhuse, Z. Kamal, and M. Salahuddin “A Localization System Using Wireless Sensor Networks: A Comparison of Two Techniques.” *Workshop on Positioning, Navigation and Communication*, Hanover, Germany, 2004.
- [TeGC05a] M. Terwilliger, A. Gupta and C. Coullard, “Localization with Confidence in Sensor Networks,” submitted for publication, 2005.
- [TerGC05b] M. Terwilliger, A. Gupta and C. Coullard, “On Bounding Localization Errors,” submitted for publication, 2005.
- [Thib02] P. Thibodeau, “Pervasive computing has pervasive problems,” *ComputerWorld*, Vol.36(41), Oct. 7, 2002.
- [USGo01] U.S. Government Printing Office via GPO Access, "Combating Terrorism: Assessing the Threat of a Biological Weapons Attack." Online Resource last accessed on December 15, 2005.
http://www.armscontrolcenter.org/cbw/resources/hearings/snsvoir_20011012_combating_terrorism_assessing_biological_weapons_attack.htm
- [WhCu03] K. Whitehouse and D. Culler, “Macro-Calibration in Sensor/Actuator Networks,” *Mobile Networks and Applications*, Kluwer Academic Publishers 2003.
- [YHRC98] K. Yao, R. Hudson, C. Reed, D. Chen, and F. Lorenzelli, “Blind Beamforming on a Randomly Distributed Sensors Array System,” *Proc. 1998 IEEE Workshop on Signal Processing Systems (SiPS '98)*, October 1998.
- [Zamb01] D. Zamboni, “Using Internal Sensors for Computer Intrusion Detection”, CERIAS Technical Report 2001-42, CERIAS, Purdue University, West Lafayette, IN, August 2001.