Trustworthy opportunistic sensing: A Social Computing Paradigm

Henric Johnson, Niklas Lavesson, Daniela A. S. de Oliveira, Felix Wu

IEEE International Conference on Information Reuse and Integration

2011 Las Vegas

Trustworthy Opportunistic Sensing: A Social Computing Paradigm

Henric Johnson, Niklas Lavesson
Blekinge Institute of Technology
Karlskrona, Sweden
{hjo, nla}@bth.se

Daniela Oliveira
Bowdoin College
Brunswick, USA
doliveir@bowdoin.edu

S. Felix Wu
University of California at Davis
Davis, USA
wu@cs.ucdavis.edu

***Abstract*—In recent years, technological advances have lead to a society with communication platforms like iPhone and Kinect Xbox that are able to inject sensing presence into online social networks (OSNs). Thus, it is possible to create large-scale opportunistic networks by integrating sensors, applications and social networks and this development could also promote innovative collaborative cyber security models. In this position paper, we discuss how social informatics will play a crucial role in trustworthy pervasive computing. With regard to security, our primary computing paradigm is still about processing information content only in order to make decisions. Given the availability of both digitized social informatics and sensor content, we now have the option to examine these sources simultaneously. We refer to this new era as the Social Computing Paradigm, and we argue that it could be particularly useful in conjunction with opportunistic sensing.**

I. Introduction

Sensors and platforms for communication and entertainment have become a natural part of our everyday lives. For example, in the Xbox Kinect platform OSNs, games and media sharing are integrated, thus allowing sensors to recognize your body and mirror your movements and make you the controller. Sensors have been increasingly attached to individuals via their mobile phones and are then able to deliver information about various aspects of the real world to applications and users alike. Sensors provide a wide range of opportunities for measuring, collecting, processing and distributing information in a multitude of application domains. The term sensing is used in a broad sense in the paper, which means that the discussions are not limited to what can be achieved with typical physical sensors data. The new sensor paradigm leverages humans as part of the sensing environment. Therefore, the term opportunistic people centered sensing has been introduced to describe this new paradigm, in which mobile units, carried by individuals in their daily activities, sense information directly or indirectly related to human activity, as well as other aspects [1]. In opportunistic networks, the nodes come into contact with each other opportunistically and then connect wirelessly. For example, if an individual carries a mobile phone into an airport lounge, the phone might connect automatically to the wireless hotspot provided by the lounge and then the starting page of the browser in the phone might display relevant local information about restaurants, newsstands and lounges. These types of networks also mimic the way humans come into contact with each other and are therefore tightly coupled with human relationships and real world social networks. The widespread use of mobile phones like iPhone and Blackberry with integrated communication capabilities and sensors such as Wi-Fi, Bluetooth, Radio-frequency IDs (RFIDs), cameras, microphones, accelerometers and Global Positioning Systems (GPSes) along with other embedded sensors in vehicles and surveillance systems creates a large number of contact opportunities that are key to opportunistic sensing. However, the full potential utilization of opportunistic sensing requires new networking, security and computing paradigms. Many works in the literature [1] [2] [3] have discussed the security challenges for sensing networks, in which they focus on privacy; users want to control who may access information about themselves. Also, since the collected data may originate from devices that are out of their control, the integrity of the data comes into question as well as the availability of the infrastructure.

One the one hand, it has become increasingly evident that the integration of sensors, applications and OSNs creates new and interesting opportunities. On the other hand, the co-existence of several components also creates challenges that need to be addressed. We believe that, given the mentioned security challenges and the recent availability of both digitized social informatics (from OSNs) and sensor content, we now have the option to examine multiple sources of information simultaneously and then create innovative ways to create a trustworthy communication environment. Trust is based on reputation between individuals, which is a capital asset that people may invest great amount of resources in building it and that is acquired slowly but can be destroyed very quickly [4]–[6]. Therefore we consider trust between users as dynamic. Including social context into the information generation and delivery process provides greater assurance for receiving trustworthy content [7]–[9].

In this position paper, we use the term social informatics to refer to any digitized profile data, interaction data, or content available from the OSN. Therefore, social informatics includes the social relationships and their dynamics. Social relationship might change, while some of them might be temporary, virtually private, or, mission-oriented. Social informatics also includes the communication activities or interactions over a graph of social relationships, and the policy, such as privacy or anonymity, guarding those activities. In practice, the availability of the social informatics is usually constrained by the

programming interface.

II. Examples of Opportunistic Sensing

There is currently a big push in the direction towards opportunistic sensing. Several examples exist from the networking domain. For example, the Haggle project and the MetroSense project [10] develop new applications, classification techniques, privacy-enhancing approaches, and sensing paradigms for mobile devices enabling a global mobile sensor network capable of societal-scale sensing. Even though the development of new and smaller (energy efficient) sensors is emerging, we believe that the algorithm is currently more interesting than the sensors. Researchers typically put more emphasis on context engines and predictive analysis, that is, the focus is on software rather than hardware.

A recent project (WikiCity) at MIT aims at having a city that performs as a real time control system, in which devices collect the movement patterns of people and transportation systems, and their spatial and social usage of streets and neighborhoods. A more commercial application, performing similar real-time location data analysis, called CitySense, has been developed for iPhone and Blackberry mobile phones to analyze and aggregate human behavior and to visualize a live map of city activity. These kinds of sensor-enabled applications are still far from being widely deployed and opportunistic computing and sensing initiatives are still in their infancy [11]. However, it is not difficult to imagine how this development could become the future of social networking, in many ways. Firstly, the mobile phones will be the primary way for the younger generation to explore social networks and organize social activities and relationships. Secondly, with the next generation of web applications (in combination with sensor technology) we will move beyond the era in which information has been used primarily for visualization; instead, the information provided might influence decisions and actions to a greater extent.

Another interesting project is the CenceMe [12] system that leverage the growing integration of sensors into off-the-shelf consumer devices (e.g., cell phones and laptops to collect and learn about the device users). This personal sensing system enables members of social networks to share their sensing presence with their online friends, allowing for a new level of implicit communication.

Opportunistic sensing can also be used in many different application areas such as tactical networks, intelligent transportation systems and pervasive healthcare. Communication is also of crucial importance in order to handle accidents and critical situations. The OSN environment can be combined with sensor technology to collect user data in order to perform reliable crisis risk estimation and to distribute warning messages, news and information to the general public in the event of emergencies, extraordinary events and periods of high alert in order to enhance crisis management. There must exist well-defined communication links between those that manage a particular situation and those that are directly or indirectly involved as well as with the surrounding society. In some scenarios the infrastructure and communication network could also be damaged which make the situation even worse. From a crisis management perspective, it certainly helps greatly if the people involved share the same awareness of the situation (an earthquake, for example). Therefore, the collection and sharing of information between stakeholders further increases the cooperative capability between public-, private-, civic- and military organizations. A vastly different application that could benefit by integrating sensors and social network technology is match making, where the objective is to alleviate the process of meeting people with shared interests. Social networks have already been developed in order to facilitate match making. However, such networks can be further enhanced using sensor technology, for example, to indicate the proximity of people with common interests.

Finally, we would like to discuss the social computing paradigm in relation to a maritime surveillance system. One of the challenges with such a system is to perform automated anomaly detection. Such a highly advanced system has to utilize distributed computation from several sources to detect and visualize out-of-the ordinary behavior to aid operational decisions. Ports and coastal areas in particular, present many challenges such as the difficulty to observe and assess its domain with respect to vessel movements, activities, intentions and ownership. Hence it is imperative to make the best possible use of all available data, whether these are from sensors, direct observation (e.g. coast guard cutters), open source information, or from the vessels (e.g., Automatic Identification System, AIS), even though such data can be partial and unreliable (both unintentionally and intentionally).

The increased use of OSNs and the amount of open information that is available on the Internet (blogs, chats, OSNs, corporate websites), shipspotter information and new sensor information available from, e.g. Smartphones, opens up new opportunities for data and information fusion. Based on actual scenarios, we have initially discovered that information fusion from open sources improved the capability for early identification of malicious vessels. This discovery has, for instance, helped the Swedish Coast Guard to monitor the right vessel at the right time and increased the time window to prepare necessary actions before the vessel arrives at the harbor. Therefore, we consider open source information and OSNs as a valuable and complimentary input to the ordinary surveillance systems used by the authorities today.

III. Security Limitations

Current detection and prevention security solutions in opportunistic sensing and pervasive computing usually work by distinguishing malicious and benign pieces of data, program or behaviors, and information flow traces. These approaches lack in diversity are automated and target a particular defined threat. Therefore, we would like to elaborate on why we believe certain security solutions are not keeping up with the current generation of attackers.

The current communication platforms as well as many applications do not provide enough controllability for its end users. Today, each communication device receives a routable identity, e.g., an IP-address. It is not easy to make the address

unknown to the network. If it is an IP-address you are always visible for a Denial-of-Service attack. Another issue in communication is trust between parties. When devices or users communicate, both parties should know how much trust they share. This trust value could then be used to handle the message differently. Because of the lack in trust determination we believe this is a major reason for having so many large-scale attacks in the networking community.

From the perspective of the physical sensors, it is necessary to consider the tradeoff between performance and security, due to the limited resources. Sensing could also contribute to new privacy threats because sensors will be carried by people that could trace human behavior and positioning. Remember that in opportunistic sensing the users might not always be fully aware of ongoing monitoring, thus introducing new privacy concerns.

From a system security perspective, there have been previous efforts on designing Intrusion Detection Systems (IDSs) [13] for pervasive computing. IDSs can be broadly divided into three classes (i) misuse detection (often also called signature based detection) (ii) anomaly detection and (iii) specification-based detection. The problem with these systems is that they cannot detect new unknown (zero-days) attacks. Anomaly detection simply tries to look for behaviors that deviate from normal and expected behaviors. Statistical techniques are used to infer an anomaly; however, this can lead to false positives. These schemes are also sensitive to the choice of the threshold to determine an anomaly. Choosing a stringent threshold (very close to expected behavior) may trigger a large number of false positives; if the threshold is loose, then, attackers will be able to evade detection. Moreover, reputation systems have also received some attention [14]. In most of these efforts, the idea is to increase or decrease the trust associated with a neighbor node based on observations with regards to the node. Unfortunately, the behavior of a node cannot be examined in isolation.

IV. Identifying the Gaps

Although the aforementioned solutions have proven to be successful for particular types of threats, the computing paradigm from which they stem from does not seem to keep up in defeating the new and creative generation of attackers that is motivated and supported by a growing underground economy. We ask the question of what is missing: as described, nearly all current security models work by distinguishing trusted from untrusted pieces of data (stream of bytes, software programs and patches, URL content, network packets, files, messages, and so on) and program behaviors. These approaches are automated, rigid, threat-specific, and are lacking in diversity of operation. Moreover, with the shift to the Web-based computing paradigm [15], where users are meeting most of their computing needs through a Web browser, the task of distinguishing trusted from untrusted information automatically becomes much more complex. Leveraging social trust to distinguish a continuum of trusted/untrusted values can add flexibility to security solutions, which is important in order to thwart attacker strategies by making it harder to predict a certain host behavior in the face of a particular threat. We believe that human collaboration and its intrinsic definition of trust is key to move towards a new socially aware paradigm for trustworthy opportunistic sensing. Trust is dynamic and subjective and will most probably change or fluctuate across time, depending on real life relationships between individuals. We believe that trust is not only a technical issue but it also depends on social behavior from real situations. Therefore, more types of social research need to be integrated into the future Internet design and sensor networking in order to mimic real human communication.

V. Key Trends

In the last few years we have observed three key trends. The first trend is the rise in popularity of OSNs. As an example, Facebook is reported to now have about 500 million active users (users who have returned to the site in the last 30 days) and this number is still growing. Secondly, we observe the increase in complexity of the security landscape and modus operandi of attackers. The current generation of attackers is extremely creative, financially or politically motivated, and organized. Traditional security models based on distinguishing trusted from untrusted pieces of data and program behavior continue to face difficulties in keeping up with the level of sophistication and ingenuity of such attackers. Thirdly, we recognize the fact that there now exist new technological platforms (such as XBox Kinect) and embedded sensors in mobile devices coupled with wireless communication stacks that put powerful sensor technology in the hands of the individual. These new sensing capabilities stimulate the users to interact and share information within their social networks and thus help in transforming the traditional Internet from a technical environment into a social platform. However, we note that these capabilities also increase the demands for privacy and security approaches in order to maintain a trustworthy communication architecture.

VI. Integrating Social and Sensor Networks

Opportunistic sensing tends to integrate communication more closely with human behavior. Therefore, the integration of sensors with social networks will lead to new possibilities to share real-time data and more useful applications. When referring to sensors and sensor data in this paper, we do not limit our ideas and the discussion to encompass only the typical sensor, which is arguably the physical sensor, but also consider other types of sensors. The cyber sensor is one such example and its functionality can be described as that of sensing online digital information, which in turn can comprise media content, written text, or details concerning social interactions. Consequently, individuals can participate in events and campaigns originated by other users, according to common interests, and make use of the social links and communities offered by innovative social networking tools. The recruitment of individuals to sense the personal environment will be the determinant factor for the success of their outcome. Therefore, it is crucial that the initiator of campaigns, either being organizations or creative individuals,

find the needs that motivates participation and activates devices into sensing mode. OSNs have, in this case, proven to be a popular participative web tool and have caused a shift in the Internet design and function with regard to connecting people. We expect a great interest to bring social networks and the physical world one step closer. This integration could lead to innovative applications that can sense context of the user with a higher accuracy, thus providing a more personalized solution.

VII. Research Challenges with Hybrid networks

Sensing technology creates new opportunities for collecting and analyzing information. With the growing ubiquity of the Internet and OSNs, the exchange of information has also increased on a global scale. For some, the exchange of personal information via technologies such as blogs, instant message, SMS or social network applications has become a primary mean for human interaction (especially among the youth). However, the integration of opportunistic sensing and social information has created a few challenges and opportunities as follows:

A. Interception and manipulation of online social informatics

Most users will engage with several application that provides different functionalities to collect, analyze and/or communicate data. Most likely the majority of the applications are in fact developed by individual developers that you have little information about. Therefore, to ensure that social informatics are retrieved properly and securely it is important to design a system that enhance the management of social data [16]. One way to solve this issue is to log the activities of applications to assist the user with valuable information in making more secure decisions. Users should then be able to configure certain settings to minimize potential privacy leaks etc. In general, such a system would work as some sort of a firewall, controlling outgoing and incoming social informatics. The Davis Social Link research group has created such an infrastructure called FAITH (Facebook Applications: Identifications Transformation & Hypervisor) to provide more trustworthy and flexible services to OSN users [16]. FAITH itself is a Facebook application, but works as a proxy between users and Facebook. It can hook other applications and provide services to the applications. Currently FAITH has about ten different applications of various kinds and it is running on the ProtoGENI [17] platform. FAITH provides several major functions such as privacy shield and anonymity, social network structural analysis and transformation, and application behavior profiling and social influences. In general, these functions/applications are able to monitor and log sensing applications to perform anomaly and intrusion detection. Users can also customize the API to their personal information that an application can call. Moreover, simplifying and automating the process of creating privacy policies [18] and determine how well an OSN application (potentially related to sensing) conforms to the user's privacy settings is further presented in [19].

B. Large-scale online knowledge collaboration

Human users play a critical role in obtaining a trustworthy system or network. The employment of online collaboration may for example help in decreasing the gap between experts and novices with regard to security and privacy issues. Consequently, large-scale social networks could serve as a valuable way for novice users with a limited knowledge of security to improve their awareness. It is therefore important to add the role of human users into the trustworthy computing model, thus yielding a collaborative model. It has already been shown that different groups of users (for example, experts and novices of a certain subject) can be identified by performing data mining on online collaborative data [20]. We believe that the incorporation of human users can make a significant improvement in terms of trust and security. One particular challenge is that the widespread lack of security awareness causes users to make poor decisions online. Some of these decisions are difficult to prevent using existing software solutions. We argue that social informatics can bridge the gap in awareness by providing good collaborative models that depend on social trust and which allow users to defend themselves more effectively against different attacks. Zhao *et al.* [21] present such a collaboration model that can further be developed and used in an opportunistic sensing system to obtain a neutrality policy from the injecting sensors or users. This is an important issue for trustworthy collaboration in a large scale and open network environment since conflicts among users and dissenting opinions could give rise to unreliable content. Another important issue is how to leverage the power of social networks to automatically manage reputation and trust within a network.

C. The Socially-Aware Operating System

Each of the devices in an opportunistic sensing system will contain an operating system (OS) and we believe that the OS should not merely manage processes, memory, and I/O devices syntactically. Applications and the OS should become socially-aware and leverage social trust to enhance the robustness and diversity of their security mechanisms. We envision a model that would allow OSN users to assign trust values to other users and pieces of data (software programs, URLs, files, e-mail addresses) that can be consumed by a socially-aware OS and architecture. This would allow fine-grained trust decisions about data that take into account user context, thus adding sophistication and diversity to a host behavior.

With the integration of social and sensor network we envision an architecture for the OS with the following components (Figure 1): (i) an extended Facebook-like OSN infrastructure that maintains not only user profiles and their social networks, but also an optional trust repository per user, (ii) users that can assign trust values to their friends in a privacy-preserving fashion and feed their trust repository with trust values for objects such as URLs, IP addresses, files, e-mail addresses, and (iii) a socially-aware OS capable of retrieving and managing trust repositories locally and exporting a trust interface to user applications. These applications retrieve information (through the OS trust interface) from a user trust repository to make

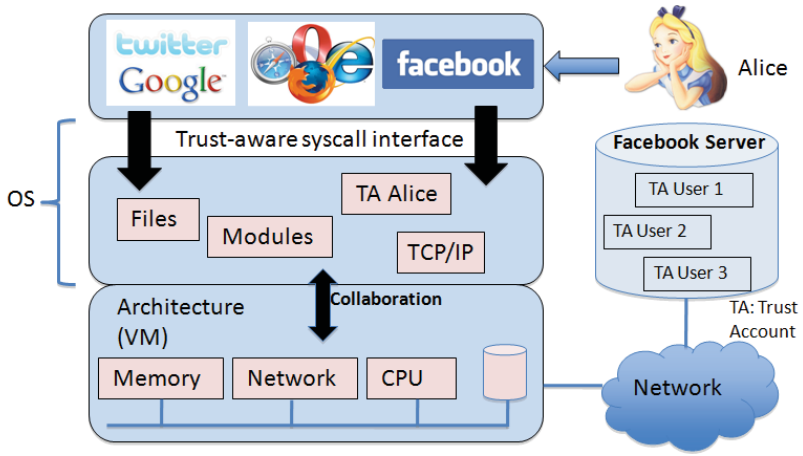

Fig. 1. The socially-aware OS.

better decisions about the security or trust level of the objects they access. The socially-aware OS also leverages the trust repository data to employ strong and fine-grained security policies about processes, files, modules in the systems and to propagate trust values in collaboration with the architecture layer through a virtual machine (VM) by employing dynamic information flow tracking systems (DIFT) [22].

D. User relationship controllability

Hijacking and identity thefts attacks have caused severe problems over the years. These attacks can be used for impersonation, gaining illicit access into target networks, execute anonymous attacks, embezzling sensitive data and many more malicious activities. How do we handle the situation where two users or sensors claim to have the same identity? For instance, on February 24th 2008, Pakistan Telecomm announced a more specific IP address (208.65.153.0/24) of YouTube (208.65.152.0/22) to its Border Gateway Protocol (BGP) peers. This hijack attack caused inaccessibility to YouTube from a significant portion of the Internet for over two hours. This attack can be characterized as two Autonomous Systems (AS) simultaneously announcing the same related prefixes. The resolution is always: Which AS is truly authorized to announce a prefix? If any Public Key Infrastructure, Domain Name Server, or even a web browser is compromised, our ground truth might not be the real one any more. With this in mind, our vision is to allow any sensor or user announcing them as any name or organization. Following our ongoing research and the social computing paradigm, we believe that the relationships and the social paths in the network are key to thwart user relationship controllability.

VIII. The Socially Aware Opportunistic Sensing System

For the next generation of sensing systems, we envision designing an architecture based on the control and management of trustworthy social computing and providing socially aware network services. A socially aware sensing system is about the relationship between social informatics and trustworthy computing. At the same time as we enhance the trustworthiness for an application, we simultaneously need to ensure that whatever social informatics is being consumed and processed we will not compromise any of the users privacy requirements.

Figure 2 shows the different layers for the envisioned socially aware opportunistic sensing framework. The lower layer contains the different sensors that could either be located outside (wirelessly connected) or embedded in the sensing device. In case of multiple sensors, a meta data access point performs data fusion for the above layers. To build a trusted social relationship path between collaborating sensors, protocols like KarmaNet [23] could be used to create judicious forwarders and cut off malicious nodes and adapt to dynamic changes in behavior. Depending on the type of sensing, a specific application to perform the opportunistic task will collaborate with the OSN and make use of the available social informatics and sensor information. This integration of social and sensor networks creates a high-level trustworthy and socially aware system for individual users. We further envision a future, in which there will be open Application Programming Interfaces (APIs) for developers to integrate the sensors with applications in connection with social networks. Developers with a novel idea and some basic programming skills can quite easily create innovative applications. Today there are several hundred thousands of applications for the Facebook community.

There are several research challenges in the design and development of the framework presented in Figure 2. For instance, how do we determine the appropriate boundary for social informatics and how do we quantitatively measure the value of social informatics? How do we balance the concern of privacy and anonymity, by introducing a socially aware system? How can we make sure that we do not create any new or unexpected vulnerability? Finally, what should be the process for the sensing and social community to form a converging and collaboratively decision of how to obtain a high level of security?

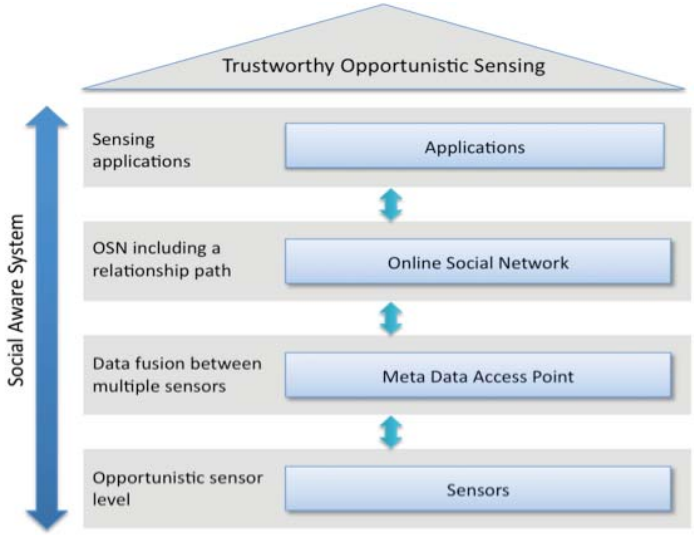

Fig. 2. The social aware opportunistic sensing framework.

IX. Conclusion

The development and widespread adoption of online social networks have already changed the way people interact and share information. By combining physical and cyber sensors with online social networks it is possible to more closely mimic real-world interactions and situations. This new type of hybrid networks can be used in a multitude of domains to, for example: monitor individuals, enhance communication capabilities, and to increase collaboration efficiency in crisis management. However, these hybrid networks also present challenges and issues that need to be addressed especially in terms of new forms of security threats. Even without sensor input, online social networks have already been shown to be prone to identity theft and it has been argued that individuals are exposed to government agencies and companies in a manner which compromises privacy. Moreover, the hybrid networks may also be more susceptible to hacker attacks. For example, if one system component is hacked, several dependent components may stop working or could at least be compromised. At the same time, it is reasonable to argue that many of our currently existing security threats may be resolved by combining sensors with social informatics since we may be able to obtain better a means for determining trust values between communicating parties. Finally, by incorporating the role of human users and social informatics, it will become possible to increase the diversity in host behavior, which would likely decrease the success rate of attacks and thus result in a significant improvement in cyber security.

References

[1] A. Kapadia, D. Kotz, and N. Triandopoulos, "Opportunistic sensing: Security challenges for the new paradigm," *First International Conference on Communication Systems and Network*, pp. 134–141, 2009.

[2] S. F. Wu, H. Johnson, and A. Nilsson, "SOLA: Lightweight Security for Access Control in IEEE 802.11," *IEEE CS Journal IT Professional*, vol. 6, pp. 10–16, May/June 2004.

[3] A. Perrig, R. Szewczyk, V. Wen, D. Culler, and J. D. Tygar, "SPINS: Security protocols for sensor networks," *Wireless Networks*, vol. 8, pp. 521–534, Sept. 2002.

[4] N. Luhmann, *Trust and Power*. Wiley, 1979.

[5] D. Lewis and A. Weigert, "Trust as a social reality," *Social Forces*, vol. 63, no. 4, pp. 967–985, 1985.

[6] D. Gambetta, *Trust: Making and Breaking Cooperative Relations*. Blackwell, 1990.

[7] J. Golbeck, "Computing with social trust," *Human-Computer Interaction Series*, 2009.

[8] K. K. M. Sirivianos and X. Yang, "Facetrust: Assessing the credibility of online personas via social network," *Usenix Workshop on Hot Topics in Security*, 2009.

[9] H. Johnson, N. Lavesson, H. Zhao, and S. F. Wu, *On the Concept of Trust in Online Social Networks - Trustworthy Internet*. Springer, 2011.

[10] L. Pelusi, A. Passarella, and M. Conti, "Opportunistic networking: Data forwarding in disconnected mobile ad hoc networks," *IEEE Communications Magazine*, pp. 1–10, 2006.

[11] H. Lu, N. D. Lane, S. B. Eisenman, and A. T. Campbell, "Bubble-sensing: Binding sensing tasks to the physical world.," *Journal of Pervasive and Mobile Computing*, pp. 58–71, 2010.

[12] E. Miluzzo, N. D. Lane, K. Fodor, R. Peterson, H. Lu, M. Musolesi, S. B. Eisenman, X. Zheng, and A. T. Campbell, "Sensing Meets Mobile Social Networks: the Design, Implementation and Evaluation of the CenceMe Application," in *Proceedings of the 6th ACM Conference on Embedded Network Sensor Systems (SenSys '08)*, (New York, NY, USA), pp. 337–350, ACM, November 2008.

[13] F. Anjum and P. Mouchtaris, *Security for Wireless and Ad Hoc Networks*. John Wiley, 2007.

[14] P. Michiardi and R. Molva, "Core: A collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks," pp. 107–121, 2001.

[15] H. J. Wang, A. Moshchuk, and A. Bush, "Convergence of desktop and web applications on a multi-service os," *USENIX Workshop on Hot Topics in Security*, August 2009.

[16] R. Lee, R. Nia, S. Ye, J. Hsu, K. N. Levitt, J. Rowe, and S. F. Wu, "Design and Implementation of FAITH, An Experimental System to Intercept and Manipulate Online Social Informatics," in *Proceedings of the International Conference on Advances in Social Networks Analysis and Mining (Asonam 2011)*, July 2011.

[17] Protogeni, "http://www.protogeni.net/trac/protogeni."

[18] L. Banks and S. F. Wu, "Toward a behavioral approach to privacy for online social networks," *Second international conference on Social informatics (SocInfo)*, 2010.

[19] N. Lavesson and H. Johnson, "Measuring profile distance in online social networks," *International Conference on Web Intelligence, Mining and Semantics (WIMS)*, 2011.

[20] D. Perera, J. Kay, I. Koprinska, K. Yacef, and O. Zaiane, "Clustering and sequential data mining of online collaborative learning data," *IEEE Transactions on Knowledge and Data Engineering*, vol. 21, no. 6, pp. 759–772, 2009.

[21] H. Zhao, S. Ye, P. Bhattacharyya, K. Gribble, and S. F. Wu, "Socialwiki: Bring order to wiki systems with social context," *Second International Conference on Social Informatics (SocInfo)*, 2010.

[22] M. I. Al-Saleh and J. R. Crandall, "On information flow for intrusion detection: What if accurate full-system dynamic information flow tracking was possible?," *New Security Paradigms Workshop*, 2010.

[23] M. Spear, X. Lu, N. Matloff, and S. F. Wu, "Karmanet: Leveraging trusted social paths to create judicious forwarders," *First International Conference on Future Information Networks*, 2009.