

SAFEST: A Framework for Early Security Triggers in Public Spaces

E. Baccelli¹, L. Gerhold⁶, C. Guettier⁴, J. Schiller³, T. C. Schmidt², G. Sella⁴, U. Meissen⁵, A. Voisard^{3,5},
M. Wählich³, G. Wittenburg¹

¹INRIA, HIPERCOM Team, École Polytechnique LIX, Route de Saclay, 91128 Palaiseau (CEDEX), France

²Hamburg University of Applied Sciences, Department of Computer Science, Berliner Tor 7, 20099 Hamburg, Germany

³Freie Universität Berlin, Institut für Informatik, Takustraße 9, 14195 Berlin, Germany

⁴SAGEM Défense Sécurité, 100 Avenue de Paris 91300 Massy, France

⁵Fraunhofer-Institut für Software- und Systemtechnik (ISST), Steinplatz 2, 10623, Berlin, Germany

⁶Research Forum on Public Safety and Security, Fabeckstr. 15, 14195 Berlin, Germany

emmanuel.baccelli@inria.fr, lars.gerhold@fu-berlin.de, christophe.guettier@sagem.com, jochen.schiller@fu-berlin.de,
schmidt@informatik.haw-hamburg.de, genevieve.sella@sagem.com, ulrich.meissen@isst.fraunhofer.de,
agnes.voisard@fu-berlin.de, m.waehlich@fu-berlin.de, georg.wittenburg@inria.fr

Abstract – Public spaces such as airports, railway stations or stadiums bring together large numbers of people on a quite limited space to use a security-sensitive infrastructure. Electronic security systems may help to provide better and faster security, as well as safety for the general public. Application scenarios may include intrusion detection and monitoring of large crowds in order to provide guidance in case of unexpected events (e.g., a mass panic). However, current security systems used within the public infrastructure are typically expensive, non-trivial to deploy, difficult to operate and maintain, prone to malfunction due to individual component failures, and generally lack citizen privacy-friendliness. The advent of novel, large-scale distributed security systems based on wireless, lightweight sensors may enhance security and safety in public spaces. In this realm, SAFEST is a project aiming at analyzing the social context of area surveillance and developing a system that can fulfill this task, both in terms of technology as well as acceptance by the general public. The targeted system will operate in a distributed way, collect anonymized data, securely transfer this data to a central location for evaluation, and – if necessary – notify the operator or issue alerts directly to the general public. Work on the technical aspects of the system is accompanied by social studies investigating the individual perception of risk and the methods for reaching public acceptance of the technical solutions.

1. Introduction

In public spaces with integrated infrastructure support, civil security refers to the following two distinct items: First, the general population must be protected from the dangers of unexpected events (e.g., a fire). Such events – independently of whether they are caused intentionally or accidentally – typically lead to irrational behavior of the affected persons. In crowded places, this may result in a mass panic, thus multiplying the danger posed by the initial threat. Second, critical infrastructure (e.g., an airport) must be protected against unauthorized access. Unauthorized access to a critical infrastructure may result in damage or sabotage, both of which undermine security and thus endanger the general public. The direct protection

of the population as well as the protection of critical infrastructure can both be ensured through a combination of observation of the environment, processing of security-relevant events, and (semi-)automatic initiation of appropriate reactions to avert or contain the crisis.

The successful implementation of civil security is bound to social and technical conditions. In this paper, we consider technology as a tool to enable enhanced civil security under social constraints. This paper describes SAFEST, a project aiming to provide a comprehensive solution to ensure the safety and security of the general public and critical infrastructures. Specifically, SAFEST addresses the problems of intrusion detection and crowd control by the means of socio-cultural analysis and a



distributed system for sensing and alerting. This interdisciplinary approach is one of the key strengths of this project.

The technical goal of SAFEST is to design a system that is equally suited for the protection of critical infrastructures and for the protection of individuals in large crowds. Critical infrastructures will be protected through the detection of illegal access; persons in crowded environments will be protected through intelligent crowd guidance, thus mitigating the risk of a mass panic. The dual application of this system – which uses largely the same hardware components for both application scenarios – is interesting for end-users since it effectively lowers the investment required to ensure an adequate protection. In contrast to video surveillance systems, our approach preserves the privacy of citizens since we do not rely on technology that is capable of identifying individual persons. Additionally, our system incorporates automatic event detection and alerting technology to ensure rapid dissemination of critical information, may it be to security staff or directly to the general public in the affected area via cellular phones or PDAs.

The approach followed by the SAFEST consortium is thus holistic in two ways: Scientifically, it is holistic in that it considers both the social as well as the technical dimensions of area surveillance, intrusion detection, and crowd control. Method-wise, it is holistic in that it closes the entire processing loop related to ensuring public safety: distributed sensing, secure communication, complex event processing, and targeted alerting. These properties set SAFEST apart from other, more focused approaches, e.g., FluSs¹.

The relevance of the results of the SAFEST project will be measured through continuous feedback from the public safety community actors such as the research forum on public safety and security (FÖS) and from end-users such as FBS². Applicability will be verified by the means of a demonstrator deployed at the Berlin Brandenburg International (BBI) airport. This setting is particularly adequate since airports present a very challenging and diverse use case with the highest security requirements: operational challenges include the protection of passengers, staff, and critical infrastructure from serious risks such as criminal or terrorist activities in a busy, crowded environment. Given these properties of the selected use case, it is well conceivable that the SAFEST approach will be equally applicable to similar scenarios such as railway stations or stadiums in the future.

This paper is organized as follows. Section 2 relates on the context and describes the major social and economic issues. Section 3 gives the outline of the technical approach. Section 4 describes the related work in different areas. Finally, Section 5 concludes the paper and presents some of our future work.

2. Context, Social and Economic Issues

The global market for security systems, excluding IT security is expanding with potential for considerable growth. Today the global market for security sensors exceeds 500 M€ and the share of autonomous sensors, comprising unattended ground sensor systems (UGSS) and wireless sensor networks (WSN), is expected to grow rapidly after an industrial development phase.

Ensuring public safety by the means of access and crowd control is however challenging given the right to freedom of assembly in most public spaces. The effectiveness and public acceptance of security measures in these spaces is thus mainly a question of the security culture, i.e. the collective understanding by members and organizations of a society which events should be declared as a risk and how to face them. In particular, area surveillance is prone to significant subjective criteria in perceiving risks and threats: the population evaluates dangers and risks in public spaces by criteria which may not reflect the objective situation [1]. People neither can assess the exposure of public spaces (e.g., airports or railway stations), nor evaluate reasonable preventive measures (e.g., new monitoring technologies).

The set of diverse opinions of citizens is of major importance in the public sector, because the dichotomy between objectively increased security and subjective loss of freedom is highly pronounced. As a consequence, efforts towards increased civil security need not only to provide system and technology concepts as well as appropriate tools, but also to answer the following two questions:

1. Which frictions between security and freedom can be identified and how are they assessed by different sections of the population?
2. Which is the relation between the fulfillment of subjective security desires and the objective threat estimates by experts, including their suggestions of how to cope with identified threats?

The subjective perception of risks has been analyzed from different scientific perspectives [2][3][4][5]. A fundamental result is the observation that there exists usually a significant gap between the subjective perception and the objective reduction of the security due to risks. People are not able to objectively evaluate the real degree of security in macroscopic situations, nor are they able to evaluate appropriate preventive actions. Nevertheless, people form an opinion about threat scenarios and define expectations how to deal with anticipated risks. Surveying this set of opinions is part of the SAFEST project. The more fundamental problem in this field is that of an

¹ <http://www.flughafensicherungssystem.de/>

² Flughafen Berlin Schönefeld GmbH (FBS)

acceptable trade-off, i.e., which degree of freedom people are willing to give up in favor of increased security. As this problem is being addressed, it results in a dilemma as there are positive as well as negative rationales for both perspectives: Freedom as well as safety should be guaranteed.

The outcome of the socio-scientific study conducted in this project will provide a basis to discuss how much security is reasonable and needed for a society, and which perspective the population has in this context. Security is an utmost subjective construct. This subjectivity within the perspective of the population as well as objective insights into risks and dangers must guide basic principles of political strategies and technological innovations.

3. Technical Approach Outline

The SAFEST consortium gathers academics and industrial partners with backgrounds in a variety of appropriate fields including secure mobile communication, scalable data communications, sensing and data fusion, complex event processing, warning and response systems, both on the hardware and software aspects.

In order to address the problem of securing public and security-sensitive spaces, SAFEST proposes to apply current research from the ICT domain that is conducted under the term *Internet of Things (IoT)*. The IoT is envisioned consisting of a huge number of embedded devices, which will be able to communicate with each other over the Internet. With the advent of the IoT, physical and virtual objects will communicate with people and with each other to accomplish the applications that combine information and data sets of the physical world with those from the virtual world. This technology is ideally suited for creating highly reliable monitoring systems that are capable of exceeding the current level of protection for public spaces and critical infrastructures.

Current technical approaches to securing public and security-sensitive spaces have several shortcomings, including the ones listed below.

- They produce huge amounts of data, which cannot be processed automatically. In the case of video surveillance system, the sheer volume of video material, which ideally should be monitored in real-time, causes humans in charge of evaluating this material to be easily overwhelmed. This results in security-relevant incidents not being recognized as such in due time, i.e., false negative detections reduce the accuracy of the monitoring system.
- Current technology also excessively relies on video data to protect public/private spaces. Depending on the characteristics of the area, other data sources may in fact be more suitable to

identify certain kinds of threats. In particular, intruders or crowd movement are only detectable via visual inspection to a certain degree. Other types of sensor provide a more suitable method of detection in closed and confined spaces. Additionally, extensive deployments of video surveillance systems have acceptance problems due to privacy concerns.

- The underlying network is not considered even though it is used to connect monitoring equipment and is vital for the basic distribution of monitoring data. Decentralized, multi-hop communication systems that provide resilience in large-scale deployments, however, induce new security risks. They rely upon adaptive routing and end-to-end security, both of which are non-trivial to implement and deploy correctly.

SAFEST thus proposes to develop the required technical capabilities to enable rapid and inexpensive deployments of embedded sensing devices and to securely access the data. Our system will employ technologies comprising unattended ground sensor systems (UGSS) and wireless sensor networks (WSN) on-site to gather security relevant data. Individual nodes in these remotely deployed networks will be accessible over the Internet using IPv4/v6. The collected data will be transmitted securely over existing Internet connections for central monitoring by designated entities. Furthermore, we also plan to support remote administration and access control of the remotely deployed devices. As a result, a deployed IoT-based system with appropriately equipped sensing devices will be able to provide relevant data. The observed data will be centrally evaluated by an alerting and response system, which consolidates observations and extracts context-specific events. Based on the events, notification messages will be created and delivered to people on-site. Considering the use-case of crowd control, persons may be guided to leave a building securely using on-demand information transmitted to their cellular phone or PDA.

In particular, SAFEST's goal is to define a platform meeting the particular requirements of monitoring human movement and contribute to the threat assessment model. On top of this, SAFEST also aims at providing a reliable multi-hop communication mechanism that is required for covering large areas. SAFEST will then aim at providing a mechanism establishing end-to-end security between the participating devices. Based upon this platform, SAFEST will aim at providing a mechanism detecting security-relevant situations, e.g., intruders and dangerous crowd density and movement, as well as a scheme to aggregate extracted information in order to alert and guide potentially affected individuals based on geo information. SAFEST will also provide video compression solutions that allow for additional visual inspection of the reported events, as well as mobile video software client for the guidance

system. The overall architecture of the system envisioned by the SAFEST project is illustrated in Figure 1.

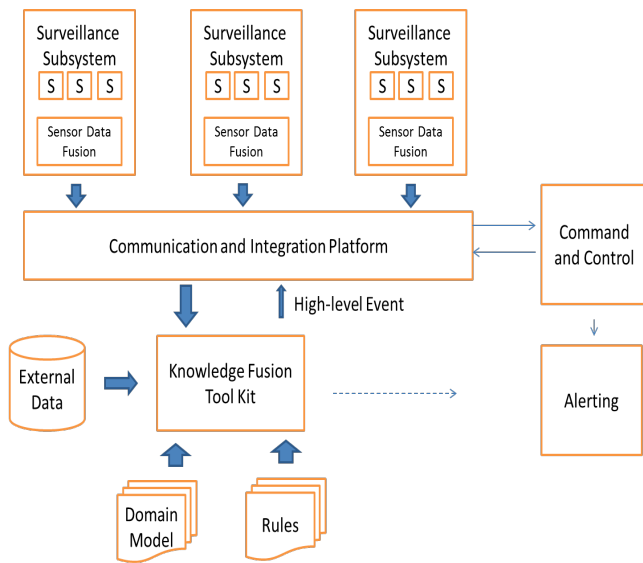


Figure 1: Architectural overview

4. Related Work

This section reviews related work in various fields in the realm of security and safety systems in public spaces, such as individual risks assessment, secure wireless sensor networks for public security, complex event processing and knowledge fusion, dependable and embedded networking.

4.1.1 Secure Wireless Sensor Networks for Public Security

Some recent projects have focused on the usage of Wireless Sensor Networks (WSNs) or Wireless Sensor and Actuator Networks (WSANs) for safety critical applications. The UbiSecSens project – “Ubiquitous Sensing and Security for the European Homeland” [6] focused on developing a purely software-based lightweight security toolbox to configure restricted devices with respect to various security objectives derived from concrete applications. The WSAN4CIP project – “Wireless Sensor and Actuator Networks for Critical Infrastructure Protection” [7] focuses on secured and reliable sensor network technology used in two use cases: protecting as well as controlling water distribution systems on one hand, and providing continuous health monitoring of power plants on the other hand. The overall WSAN4CIP objectives were to enhance the reliability of critical infrastructures by providing surveillance data for the management of the CI to increase the dependability of critical infrastructures security, by providing self-healing and dependability modules for the WSAN. Another similar

effort is the BSI project Trusted Sensor Node (TSN) [8] the focus of which was on building a trustworthy sensor node being applied as a bridge between simple sensor nodes and the base-station. The trusted sensor node is equipped with hardware accelerators for cryptographic methods like AES, ECC and SHA1.

4.1.2 Individual Risks Assessment

Criteria for the evaluation of risks and threats do not follow rational aspects with respect to stochastic risk analysis. Usually, they are based on subjective functioning heuristics, e.g., availability heuristics: As soon as potential threats are conceivable (e.g., a mass panic), they will be assumed as more likely, simply because they are already known. In addition, anchoring and adjustment heuristics are common: In case of limited data about a threat, minimal information will be ranked as quite important [28]. Current results show that the population evaluates risks based on these self-defined and weighted heuristics. These heuristics do not conform to objective criteria. In the long run, the perception pattern is based on cultural conditions, i.e., the set of existing action patterns that suggest how members of a society (should) react to risks and threats. However, if all people form their opinion based on these criteria, different perceptions of the “same” uncertainty arise [5].

4.1.3 Complex Event Processing and Knowledge Fusion

Complex Event Processing (CEP) has received increasing attention in the past decade, mostly due to the availability of data, for instance coming from sensors. CEP targets various use cases, ranging from application-related event definition to data capturing at the sensor level. In this context, SAFEST considers an approach close to the Event-Condition-Action (ECA) paradigm, according to which an action can be the fact of alerting specific groups from the general public. Focus is thus put on the following three aspects of CEP: situation recognition, event correlation, and alerting. Recognizing situations is an essential component of such systems. Situations are modeled as a multi-dimensional context that is associated with an entity and that is valid during a time interval. The entity can be of any type including an individual or a group of individuals. Situation recognition relies on attribute fusion as described for instance in [9].

Event correlation is another relevant technique for extracting events of interests in a mass of available events. Employing techniques related to data mining, it has been in use in telecommunications and IT service management for decades. In sensor-based systems, event correlation received attention only recently and many evaluation engines are now available on the market from major vendors. While some work has been carried out on situation modeling and algebras in general [19] and on

handling ontologies for situations [20], to the best of our knowledge, the identification of relevant situations for the entities at stake in intrusion detection and crowd control has not been addressed until now, mostly for reasons of confidentiality.

In the field of alerting [22, 23], recent work has focused on the implementation of multi-channel alerting systems in order to increase reliability and reduce the vulnerability of the systems. Recently developed multi-hazard alerting systems can be used flexibly for a plethora of alerting situations, thus allowing the exploitation of synergies as well as economies of scale. Most recent trends in alerting target the end-user as an individual and try to increase usability and alert compliance through increased personalization and contextualization [21].

4.1.4 Dependable, Embedded Networking

Wireless sensor networking is a key element of the Internet of Things (IoT), a substantial part of the billions of smart objects that are soon to blend into the global IP network, from actuators to home appliances, from smart meters, to smart dust. Sensor nodes are devices used for distributed and automated monitoring of various parameters such as temperature, movement, noise or radioactivity levels etc. Sensors are scattered with minimum planning with respect to their precise physical position (including the central role of the sink, if any), and the set of peers with which a sensor can directly communicate through its wireless interface may change rapidly over time due to asynchronous sleep mode strategies, fluctuations in the radio environment, device failure or mobility. Through its wireless interface, a sensor thus connects to a communication link with undetermined connectivity properties [24, 25].

Sensor networks are a challenge to current IP standards, since on the one hand these protocols were designed to work on wired links and on the other hand these protocols were designed to work on machines that do not have drastic constraints in terms of CPU, power capacities, and memory, as sensor nodes do. In consequence, several key standard protocols (including TCP, UDP, DHCP, NDP, SLAAC, and OSPF) do not function correctly in this environment. Nevertheless, IPv6-based sensor networking is a viable long term goal because it would enable generic, large scale, seamless integration of millions of sensing devices using heterogeneous radio technologies, at a low cost, and in a future-proof manner.

The Internet Engineering Task Force (IETF) is currently engaged into multiple efforts addressing the limitations of existing standards concerning wireless sensor IP networking. Some of the standards under construction [10, 11] aim at fitting IP formats, especially IPv6 formats, to direct wireless communications using low power radio technologies such as IEEE 802.15.4, which require IP format compression. Other standards in development [26, 27, 12-16], aim at providing multi-hop wireless sensor communication with IPv6, which requires specific routing

protocols. Yet another family of IETF standards under construction focuses on self-management protocols [25], [17, 18] that enable sensors to auto-configure their IP addresses, network prefixes, and security checks so that routing protocols and higher layer applications can function correctly [29].

5. Conclusion and Future Work

The SAFEST project aims at providing a comprehensive solution to ensure the safety and security of the general public and critical infrastructures in public spaces. Specifically, SAFEST addresses the problems of intrusion detection and crowd control by the means of a socio-cultural analysis and distributed system for sensing and alerting, hence leveraging the wireless sensor networking and the Internet of Things. This paper gave an overview of its main features. The interdisciplinary approach taken here is a cornerstone of this project – the kick off of which is planned in Spring 2012.

References

- [1] C. Gusy, „Sicherheitskultur - Sicherheitspolitik - Sicherheitsrecht,“ *Kritische Vierteljahresschrift für Gesetzgebung und Rechtswissenschaft (KritV)*, vol. 92, no. 2, pp. 111-128, 2010.
- [2] G. Bechmann, Ed., *Risiko und Gesellschaft. Grundlagen und Ergebnisse interdisziplinärer Risikoforschung*. Opladen: Westdeutscher Verlag, 1993.
- [3] R. Buergin, „Handeln unter Unsicherheit und Risiko. Eine Zusammenschau verschiedener Zugänge und disziplinärer Forschungslinien,“ *Albert-Ludwigs-Universität Freiburg. Institut für Forstökonomie, Freiburg im Breisgau, Arbeitsbericht 27{99, 1999*.
- [4] G. de Haan, „Ungewisse Zukunft, Kompetenzerwerb und Bildung,“ in *Bildung: Angebot oder Zumutung?*, Y. Ehrenspeck, G. de Haan, and F. Thiel, Eds. Wiesbaden: VS Verlag für Sozialwissenschaften, 2008, pp. 25-44.
- [5] L. Gerhold, *Umgang mit makrosozialer Unsicherheit. Zur Wahrnehmung und Bewältigung gesellschaftlich-politischer Phänomene*. Lengerich: Pabst Science Publishers, 2009.
- [6] “The UbiSecSens project,” <http://www.ist-ubisecsens.org/>, 2011.
- [7] “The WSan4CIP project,” <http://www.wsan4cip.eu/>, 2011.
- [8] P. Langendörfer, F. Vater, T. Basmer, and O. Stecklina, „Trusted Sensor Node,“ *Abschlussbericht*, 2009.
- [9] E. Shahbazian, G. Rogova, and P. Valin, *Data Fusion for Situation Monitoring, Incident Detection, Alert and Response Management*, ser. NATO Science Series. 3: Computer and Systems Sciences. Amsterdam: IOS Press, 2005.

- [10] J. Hui and P. Thubert, "Compression Format for IPv6 Datagrams in 6LoWPAN Networks," IETF Internet Draft draft-ietf-6lowpan-hc, September 2010.
- [11] N. Kushalnagar, G. Montenegro, and C. Schumacher, "IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs): Overview, Assumptions, Problem Statement, and Goals," IETF Request for Comments RFC 4919, August 2007.
- [12] T. Winter and P. Thubert (eds.), "IPv6 Routing Protocol for Low power and Lossy Networks," IETF Internet Draft draft-ietf-roll-rpl, November 2010.
- [13] J. P. Vasseur, M. Kim, K. Pister, N. Dejean, and D. Barthel, "Routing Metrics used for Path Calculation in Low Power and Lossy Networks," IETF Internet Draft draft-ietf-roll-routing-metrics, September 2010.
- [14] P. Thubert, "RPL Objective Function 0," IETF Internet Draft draft-ietf-roll-of0, July 2010.
- [15] J. Martocci, P. D. Mil, N. Riou, and W. Vermeylen, "Building Automation Routing Requirements in Low-Power and Lossy Networks," IETF Request for Comments RFC 5867, June 2010.
- [16] Z. Shelby, B. Frank, and D. Sturek, "Constrained Application Protocol (CoAP)," IETF Internet Draft draft-ietf-core-coap, October 2010.
- [17] Z. Shelby, S. Chakrabarti, and E. Nordmark, "Neighbor Discovery Optimization for Low-power and Lossy Networks," IETF Internet Draft draft-ietf-6lowpan-nd, October 2010.
- [18] T. Tsao, R. Alexander, M. Dohler, V. Daza, and A. Lozano, "A Security Framework for Routing over Low Power and Lossy Networks," IETF Internet Draft draft-ietf-roll-security-framework, September 2010.
- [19] U. Meissen, S. Pfennigschmidt, A. Voisard, and T. Wahnfried, "Context- and Situation-awareness in Information Logistics," in Proceedings Intl. Workshop on Pervasive Information Management (PIM), ser. Lecture Notes in Computer Science, vol. 3268. Berlin Heidelberg: Springer-Verlag, June 2004, pp. 448-451.
- [20] N. Weibenberg, A. Voisard, and R. Gartmann, "An Ontology-based Approach to Personalized Situationaware Mobile Service Supply," *GeoInformatica*, vol. 10, no. 1, pp. 38-55, 2006.
- [21] U. Meissen and A. Voisard, "the Effectiveness of Early Warning via Context-aware Alerting," in Proceedings of the 5th International ISCRAM Conference, F. Fiedrich and B. V. de Walle, Eds., 2008, pp. 431-440.
- [22] U. Meissen and A. Voisard, "Current State and Solutions for Future Challenges in Early Warning Systems and Alerting Technologies," in *Advanced ICTs for Disaster Management and Threat Detection: Collaborative and Distributed Frameworks*, E. Asimakopoulou and E. Bessis, Eds. Hershey, PA, USA: IGI Global, 2010, pp. 108-130.
- [23] U. Meissen and A. Voisard, "Towards a Reference Architecture for Early Warning Systems," in Proc. Intl. Workshop on Computational Intelligence for Disaster Management (CIDM-2010) held with the Intl. Conf. on Intelligent Networking and Collaborative Systems (INCoS-2010). Los Alamitos, CA, USA: IEEE Computer Society, 2010, pp. 513-518.
- [24] E. Baccelli and C. Perkins, "Multi-hop Ad Hoc Wireless Communication," IETF Internet Draft draft-baccelli-multi-hop-wireless-communication, October 2010.
- [25] E. Baccelli and M. Townsley, "IP Addressing Model in Ad Hoc Networks," IETF Request for Comments RFC 5889, September 2010.
- [26] M. Goyal and E. Baccelli, "Reactive Discovery of Point-to-Point Routes in Low Power and Lossy Networks," IETF Internet Draft draft-ietf-roll-p2p-rpl, October 2010.
- [27] P. Levis, T. Clausen, J. Hui, O. Gnawali, and J. Ko, "The Trickle Algorithm," IETF Internet Draft draft-ietf-roll-trickle, August 2010.
- [28] P. Slovic, B. Fischhoff, and S. Lichtenstein, "Cognitive Processes and Societal Risk Taking," in *The Perception of Risk*, P. Slovic, Ed. London: Earthscan Publications Ltd., 2000, pp. 32-50.
- [29] E. Baccelli, "Address Autoconfiguration for MANET: Terminology and Problem Statement," IETF Internet Draft, draft-ietf-autoconf-statement, February 2008.