A taxonomy of cyber attack and defence mechanisms for emergency management networks

George Loukas, Diane Gan, Tuan Vuong
School of Computing and Mathematical Sciences
University of Greenwich, London, United Kingdom
Email: {g.loukas, d.gan, t.p.vuong}@gre.ac.uk

***Abstract*—Emergency management is increasingly dependent on networks for information gathering, coordination and physical system control, and consequently is increasingly vulnerable to network failures. A cyber attack could cause such network failures intentionally, so as to impede the work of first responders and maximise the impact of a physical emergency. We propose a taxonomy of existing and potential research that is relevant in this setting, covering attack types that have already occurred or are likely to occur, and defence mechanisms that are already in use or would be applicable.**

***Keywords*-Survey; Pervasive Computing; Network-level security and protection; Physical Security**

I. Introduction

A number of computation and communication systems are already in use and several more have been proposed to improve the safety and to facilitate the coordination, communication and decision making of first responders during an emergency. For example, emergency management (EM) is one of the key areas of application for wireless sensor networks. They can contribute towards both early detection of emergency events [35] and improved situational awareness during a search and rescue operation, at the level of individual buildings [7] or larger geographical areas [36]. Autonomous systems and particularly autonomous vehicles are also commonly proposed in an EM context. Situational awareness and coordination may be improved with live aerial imagery provided by unmanned aerial vehicles [34] or with an ad hoc infrastructure of wireless robots that reach locations otherwise inaccessible to the first responders [10].

Yet, this increased use of networked systems introduces cyber vulnerabilities in the process of physical emergency response. Cyber attacks can facilitate a physical attack or directly cause physical damage themselves. Here, we focus on the former and specifically on attacks that would impede the work of first responders by disrupting their networked systems during a physical emergency. We start by articulating the cyber security challenges of EM and then provide a taxonomy of ongoing and potential future research in terms of testbeds, attacks and related defence mechanisms (Fig. 1). Our aim is to provide an overall view of the field and help researchers identify areas where they can contribute.

A. Cyber security challenges in emergency management

1) Time-criticality: Decisions during an emergency need to be taken and communicated quickly. A cyber attack that would target the integrity of the information could have an immediate effect on decision making that relies on that information. At the same time, a network availability attack could cut off communication between commanders and first responders. In such cases, reactive cyber defence systems that are based on analysing a log after a cyber incident might be too slow to be of use [19].

2) System interdependencies: Modern EM makes use of several private and public communication systems, from satellite communications to wireless sensor networks, cellular networks and the Internet. As a result, a security breach in one network can have an impact on the rest and ultimately on the success of an EM operation. At the same time, the prevalent use of cyber-physical systems means that a cyber attack that affects the network can also affect the operation of physical devices, such as control equipment and cameras.

3) The human element: During an emergency, human mistakes are naturally common. Time pressure, as well as the current lack of familiarisation of EM practitioners with concepts of cyber security [31], would make it relatively easy for cyber attackers to expoit human mistakes, possibly through social engineering.

II. Research testbeds

EM involves a large number of interdependent processes and technologies, which are difficult to replicate in a research environment. For this reason, researchers tend to use only small scale experimental implementations, often complemented by mathematical models and software simulators.

A. Mathematical

Mathematical modelling has traditionally been used in EM for optimisation, decision support and risk analysis. The introduction of cyber threats has added additional complexities that need to be captured mathematically. Such an example is the impact dependency graph model presented in [24], which evaluates the effect that a cyber attack has on the operational capacity of an ongoing mission.

978-1-6128-4937-9/13/$31.00 ©2013 IEEE

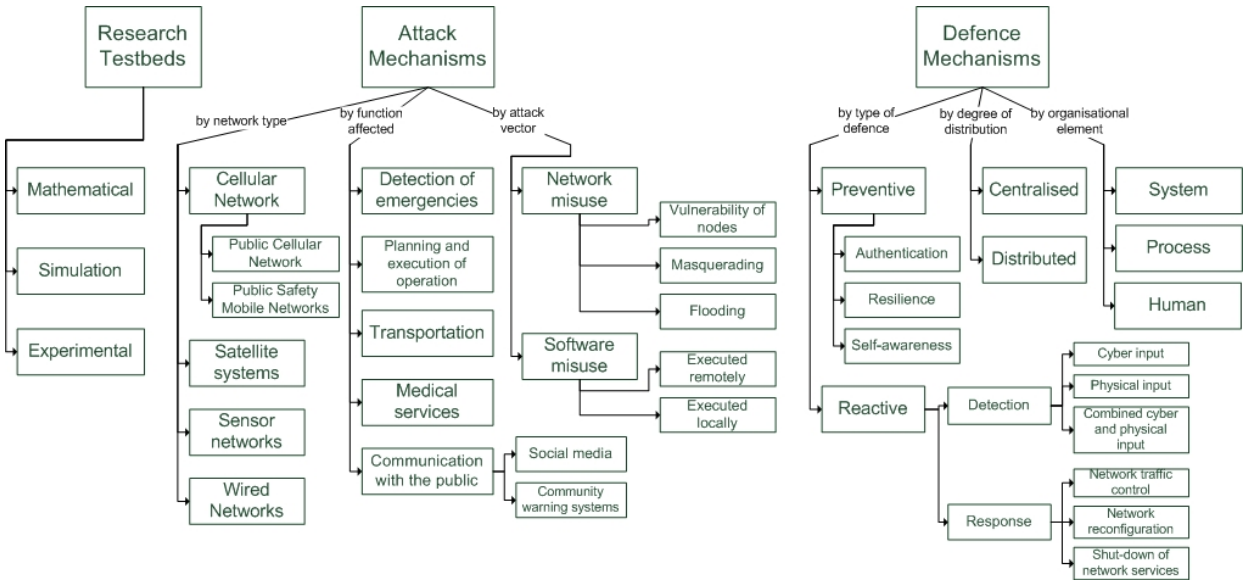

Figure 1. Taxonomy of research in cyber security for emergency management networks

B. Simulation

Existing software simulators for EM tend to represent the network infrastructure at a conceptual level, but to evaluate the impact of cyber attacks, more specialised simulators may be needed. An example is the distributed simulator presented in [11], which has been developed as a testbed to evaluate building evacuation technologies. The specific team has recently adapted this simulator to investigate the impact of cyber attacks in the cyber-physical-human context of a technology-assisted evacuation [37]. To date simulation results have shown that even a single attacker can have significant impact on an evacuation that is heavily dependent on communications.

C. Experimental

While mathematical modelling and simulation can often represent EM scenarios sufficiently, an actual scale testbed with real components naturally offers more realism. One such system is DHS Glanser, which is a collection of human-portable sensors and vehicle-mounted base stations used by the US emergency services. Mitchell and Chen have used the DHS Glanser system to experiment on detection mechanisms that would be applicable to cyber-physical systems [21].

III. Taxonomy of attack mechanisms

A. By network type

1) Cellular Networks:

a) Public Cellular Network: Text messaging is often used by the authorities and third parties to rapidly disseminate critical information during emergencies. However, recent research showed that these messages overload the cellular network and cause failures during the emergency that were previously not understood [33]. There is clearly no malicious intent behind emergency text messaging, but it has demonstrated the vulnerability of the cellular network to simple SMS flooding attacks during an emergency.

b) Public Safety Mobile Networks: Communication between EM personnel, vehicles and equipment is often based on domain-specific mobile radio technologies, such as Terrestrial Trunked Radio (TETRA). TETRA does not suffer the congestion issues of public cellular networks, but it provides low communication speeds in comparison to modern standards. Also, despite its relatively strong TEA2 encryption, researchers have shown that TETRA is unable to protect against attacks that clone both the terminal identifier and the authentication key if the latter were exposed when distributed to the authentication center [16].

2) Satellite systems: EM systems make extensive use of geographical positioning systems (GPS), which makes them vulnerable to GPS spoofing attacks, where illegitimate signals deceive GPS receivers about their location. Tippenhauer et al. have provided an analysis of GPS spoofing attacks with regards to their precision requirements [27] and a portable GPS civilian spoofer has been presented in [9].

3) Sensor Networks: There are a number of ways for a cyber attack to affect an EM sensor network. It may aim to capture nodes, inject bad data, disrupt connection or exhaust sensor batteries [21], so as to reduce the situational awareness of the first responders, delay the detection of the emergency and provide false or obsolete data to decision makers. For the purposes of this taxonomy, we include body area networks used by paramedics and firefighters as special cases of sensor networks.

4) Wired Networks: The back office functions of EM are predominately supported by private and public wired

networks and standard networking protocols, and as a result are vulnerable to the same cyber threats as most corporate local and wide area networks.

B. By function affected

1) Detection of emergencies: In 1992, a failure of Chevron's computerised emergency alert system delayed the authorities from detecting and notifying the public of a chemical release accident. The failure was caused by a disgruntled former employee who had gained control of the system's computers and had disabled its emergency alert function [6].

2) Planning and execution of operation: From information gathering to planning and sharing of plans, modern EM operations depend heavily on Emergency Management Information Systems (EMIS) that support interoperability between all EM functions and may involve multiple governmental organisations and the civilian population. They facilitate computerised modelling, prediction and risk analysis, allowing EM personnel to develop preparedness and contingency plans, and even quantify the true cost of an emergency. During an actual EM operation, they provide vital support for the tracking of resources and communication with first responders. Walker has suggested that the EM community would most likely be incapable of an effective response to a terrorist attack on a major metropolitan area if a cyber attack had previously crippled the EMIS communication and data networks [19].

3) Transportation: EM can be affected by the means of transportation used by affected citizens, the emergency response vehicles used to carry people and equipment to and from the scene of the disaster, as well as by the local traffic. Computer viruses and targeted cyber attacks affecting mass transportation are relatively common, especially in railways and airports [4]. The automotive industry is also increasingly showing interest in cyber threats, partly because of isolated incidents of cyber intrusions against specific car types and partly thanks to the pioneering work of Koscher et al. [17]. The latter demonstrated experimentally that it is possible to infect a car's networks via bluetooth and other mechanisms and gain control of its locks, brakes and engine. Most significantly though, it is the potential manipulation of satellite navigation signals that could affect EM more seriously by creating local congestion. Manipulation of local traffic could be used to maximise the number of civilians affected by a terrorist attack or to delay ambulances and fire engines.

4) Medical services: Accuracy and timeliness is critical for health early warning systems which use a networked infrastructure for collecting and disseminating information. At the same time, disaster medicine often involves the use of computerised and networked equipment. Reports of life-threatening malfunctions of computerised medical equipment date back to the 1980s and the Therac-25 radiation therapy overdoses that led to four deaths. Yet, there was little interest in the cyber threats to medical devices until 2008, when pacemakers and implantable cardiac defibrillators were shown to be remotely reprogrammable without authorisation [8]. More recently, Harries and Yellowlees presented evidence that the risk of cyber-terrorism targeting the US healthcare system is increasing and have provided best practice suggestions that can be adopted by healthcare organisations [39].

5) Communication with the public: Emergency services have been using community warning systems based on communication technologies for several years [14], and many have recently implemented social media strategies in their emergency response plans. This typically involves the local authorities broadcasting alerts to the followers of their twitter or Facebook accounts [12]. However, individual accounts of social network users are often hacked. So, it would not be unrealistic to consider an attacker gaining control of an emergency service's social network account to broadcast misleading information that would affect public safety or the success of an emergency response operation.

C. By attack vector used

1) Network misuse: A wide variety of different networks are used in EM, each with its own weaknesses. In fact, where the network supports cyber-physical systems, an attacker could block or alter network traffic in a manner that would trigger a coordinated series of physical actions and cause EM systems to respond in an unexpected manner.

a) Vulnerability of nodes: Network nodes that are physically exposed, such as wireless sensor network nodes, can be captured and be reprogrammed to transmit spoofed, altered or replayed data, or could simply be taken out of the network. The confidentiality of data from other nodes too can be compromised with a sinkhole attack [13].

b) Masquerading: An example of masquerading is the Sybil attack, where fake identities are generated, so as to make multiple nodes appear on the network and send false link layer acknowledgements or inject false data into the network [29]. Using a Hello flood attack, fake nodes can be created by sending "hello" routing messages throughout the network. It is also possible to create wormholes using low latency out-of-bound channels to link one part of the network to another and enable messages to be replayed [13].

c) Flooding: Flooding a network with traffic could increase network latency or deny service altogether and compromise its ability to respond in real time. This can be achieved by introducing external traffic or by subverting the routing protocols themselves to create excess traffic [13]. Even cellular networks are vulnerable to localised denial of service attacks generated by cheap close proximity jammers. If the data and control message channels can be identified, then a control jamming attack can be launched,

using significantly lower energy than what would be required to jam all communications channels [15].

2) Software misuse: The users of back end computers that support the planning and coordination of an EM operation may be infected with malware, especially if they are connected to the internet. Malware typically exploit vulnerabilities and may enable the execution of arbitrary code or take advantage of zero-day exploits.

a) Executed remotely: EM systems often rely on off-the-shelf database technologies to store and manage information, but this makes EM vulnerable to remote attacks that aim to collect critical information about personnel and operations. For example, SQL injection attacks are an unremitting threat to the confidentiality and integrity of data in SQL databases [22]. Password cracking programmes are also used against systems to gain access and to enable the attacker to escalate their privileges. Another service which is vulnerable to remotely launched attacks is the Domain Name Service (DNS), as bogus queries to it can lead to Denial of Service attacks, and flaws in the DNS protocol can lead to local cache poisoning, diverting EM network users to malicious web sites.

b) Executed locally: Malicious applications may also be executed locally and unknowingly by the user or deliberately in a Man-at-the-End attack [30]. Typical examples are trojan applications that trick Internet users into downloading them, and when activated by the users they deliver a malicious payload, which installs itself on the local computer. The payload may offer full access to an attacker, release a virus, or cause the infected computer to become part of a botnet. Such threats are not limited to PCs and the wired infrastructure, as mobile devices that are essential to responders are also vulnerable to the same types of locally executed malicious software. Of particular interest are apps installed on personal mobile phones of EM personnel that would reveal their location.

IV. Taxonomy of defence mechanisms

A. By type of defence

1) Preventive:

a) Authentication: Authentication of users and network traffic can prevent cyber attacks from affecting EM. An example is the access control scheme presented in [26] that proactively and dynamically modifies permissions during an emergency without explicit access requests. Another common approach is to strengthen the encryption of the messages sent or to block devices with MAC addresses that are not on a predefined list of the approved ones [32].

b) Resilience: A resilient EM network is one that ensures an acceptable level of operation in the presence of cyber threats. Resilience can be improved by ensuring that the first line of defence such as firewalls and other security components are patched and updated properly [31], but can also be engineered into the system's design. A network used for crisis communication may be designed based on an unusual configuration of protocols and topology, so as to confuse or delay a potential intruder for the duration of the emergency. Another common approach for achieving resilience is redundancy, but in the EM context where communications may be affected by physical damage too, one needs to ensure that redundant network links or nodes are not in the same physical location and cannot all be taken out by a single physical event, such as a fire [28].

c) Self-awareness: Self-awareness has been used in the context of network resilience to reduce the impact of denial of service attacks [5] and worms [18]. However, we argue that a defence system can achieve its objectives only if it is actually working when a cyber attack occurs, as a malicious user could disable it prior to an attack. Thus, a potential preventive approach would be the introduction of self-awareness to the defence mechanism itself, as opposed to only the network, effectively checking that it operates and that it would function should an attack occur.

2) Reactive:

a) Detection: Detection mechanisms aim to limit an attack's impact by identifying its existence and often its type. Their success depends largely on the input features that they use. As EM networks often connect cyber-physical systems for access control, early warning, sensing, and physical control, where computational, communication and physical processes have a direct impact on each other, we classify detection mechanisms based on the cyber or physical nature of their input features:

- *Cyber input*. Naturally most detection mechanisms proposed to defend against network attacks use computational and communication data, such as packet source, data rate and protocol-specific characteristics, as their input features.

- *Physical input*. An example of physical input would be the monitoring of the GPS signal strength, as Warner et al. have observed that GPS spoofing systems use signals of much greater strength than legitimate GPS signals [2].

- *Combined cyber and physical input*. In principle, this approach makes the best use of the dual nature of cyber-physical systems in EM. For example, by linking cyber detection with physical monitoring, such as video surveillance and a central security room to monitor and report incidents, one may facilitate detection of suspicious cyber-physical behaviour [38]. Chen et al. have proposed to use fuzzy logic to combine real-time network data and physical input features, including the differences between the values reported by neighbouring sensors [25].

b) Response: After an attack is detected, a number of actions may be taken as a response, triggered automatically by the detection mechanism or manually by a human administrator that has been alerted. We have identified the following families of applicable response mechanisms:

- *Network traffic control*. Network traffic that fails authorisation or appears suspicious may be rate-limited, filtered,

relegated to lower priority or simply dropped altogether [37].

- *Network reconfiguration*. Recovery can also be achieved by changing the configuration of the network, such as its logical or physical topology, the routing criteria, policies etc. A generic approach for an agent-based infrastructure that achieves self-healing through reconfiguration of an overlay network has been proposed in [3].

- *Shut-down of network services*. On some occasions, it may be preferable to shut down specific services or parts of the network, especially if a detected cyber attack is affecting the confidentiality or integrity of ongoing emergency communication.

B. By degree of distribution

Defence mechanisms can be centralised or distributed. In [37], a collaborative mechanism that is based on identity-based signatures and content-based message verification blocks malicious packets and malicious nodes employed to disrupt communications during a building evacuation. Network nodes communicate with each other to establish the consistency of emergency messages that are propagated through the network. Of course, the consistency of information could also be checked by a dedicated central system that would collect all information from the network nodes.

In fact, even the degree of distribution of the defence mechanism may change dynamically. The approach proposed in [23] uses a voting system to dynamically choose the optimal detection interval and number of sensor nodes participating in detection, based on a given set of false alarm probabilities and compromise rates.

C. By organisational element

From an organisational point of view, the defense of EM networks can be enhanced through strengthening both technical and managerial/administrative elements:

1) System: Each system of EM needs to be updated and patched regularly to avoid attacks on known vulnerabilities, as well as to keep appropriate logs for detecting and investigating malicious cyber events.

2) Process: Process practices and guidelines are recommended to keep the level of security of EMIS up to date with industrial standards and to assist auditing.

3) Human: Human mistakes and susceptibility to social engineering can be avoided through training programs for EM personnel, as well as through the introduction of strong cyber security policies on user privileges.

V. Conclusion

The effectiveness of modern emergency management relies on the uninterrupted operation of a range of information and communication systems. Our proposed taxonomies aim to provide a global view of the related cyber attack and defence mechanisms. We do not claim that they include all possible and future approaches, but we do believe that they can be used to facilitate collaboration between EM practitioners and researchers of different disciplines, from information security and control systems to disaster simulation and social networks.

References

[1] N.G. Leveson and C.S. Turner. An investigation of the Therac-25 accidents. IEEE Computer, Vol. 26(7), pp. 18-41, July 1993.

[2] J.S. Warner and R.G. Johnston. GPS Spoofing Countermeasures. Homeland Security Journal, LAUR-03-6163, pp. 22-30, Dec. 2003.

[3] F. Sheldon, S. Batsell, S. Prowell, and M. A. Langston, Position statement: Methodology to support dependable survivable cyber-secure infrastructure. Proc. 38th Annual Hawaii International Conference on System Sciences, Vol. 9, pp. 110, 03-06 Jan. 2005.

[4] R. J. Turk. Cyber Incidents Involving Control Systems. US-CERT Control Systems Security Center, Idaho Falls, Idaho 83415, INL/EXT-05-00671, Oct. 2005.

[5] E. Gelenbe and G. Loukas. A Self-Aware Approach to Denial of Service Defence. Computer Networks, 51(5):1299-1314, April 2007.

[6] S.S.P. Madhava and K. Jaishankar. Cyber Terrorism: Problems, Perspectives and Prescription. In F. Schmallager and M. Pittaro (Eds.), Crimes of the Internet, pp.593-611. Upper Saddle River, NJ: Prentice Hall, 2008.

[7] A. Filippoupolitis, L. Hey, G. Loukas, E. Gelenbe, and S. Timotheou. Emergency response simulation using wireless sensor networks. The 1st International Conference on Ambient Media and Systems, Quebec City, Canada, Feb. 2008.

[8] D. Halperin, T.S. Heydt-Benjamin, S.S. Clark, B. Defend, W. Morgan, K. Fu, T. Kohno, and W.H. Maisel. Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero-Power Defenses. IEEE Symp. on Security and Privacy, pp. 129-142, May 2008.

[9] T.E. Humphreys, B.M. Ledvina, M.L. Psiaki, B.W. O'Hanlon, and P.M. Kintner, Jr. Assessing the Spoofing Threat: Development of a Portable GPS Civilian Spoofer. Proc. ION GNSS Conference, Institute of Navigation, Savanna, GA, Sep. 2008.

[10] S. Timotheou and G. Loukas. Autonomous Networked Robots for the Establishment of Wireless Communication in Uncertain Emergency Response Scenarios. Proc. ACM Symp. on Applied Computing, pp. 1171-1175, Hawaii, USA, 8-12 Mar. 2009.

[11] A. Filippoupolitis, G. Loukas, S. Timotheou, N. Dimakis, and E. Gelenbe. Emergency response systems for disaster management in buildings. NATO Symp. on C3I for Crisis, Emergency and Consequence Management, Bucharest, May 2009.

[12] S.L. Magsino. Applications of Social Network Analysis for Building Community Disaster Resilience. ISBN: 978-0-309-14094-2, The National Academies Press, 2009.

[13] G.W. Skelton. Cyber-Physical Security for Wireless Sensor Networks. Workshop on Future Directions in Cyber-physical Systems Security, July 2009.

[14] D. Bunker and S. Smith. Disaster management and community warning systems: inter-organisational collaboration and ICT innovation. Proc. Pacific Asia Conference on Information Systems, 10-12 July 2009.

[15] P. Tague, M. Li and R. Poovendran. Mitigation of Control Channel Jamming under Node Capture Attacks, IEEE Transactions on Mobile Computing, 8(9), pp. 1221-1234, Sep. 2009.

[16] Y.-S. Park, C.-S. Kim and J.-C. Ryou. The vulnerability analysis and improvement of the TETRA authentication protocol. 12th International Conference on Advanced Communication Technology (ICACT), Vol. 2, pp. 1469-1473, 7-10 Feb. 2010.

[17] K. Koscher, A. Czeskis, F. Roesner, S. Patel, T. Kohno, S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, and S. Savage. Experimental Security Analysis of a Modern Automobile. Proc. IEEE Symposium on Security and Privacy, pp. 447-462, Oakland, USA, May 2010.

[18] G. Sakellari and E. Gelenbe. Demonstrating cognitive packet network resilience to worm attacks. Proc. 17th ACM conference on Computer and communications security, pp. 636-638, ISBN 978-1-4503-0245-6, Chicago, Il, USA, 4 - 8 Oct. 2010.

[19] J. Walker, B.J. Williams, and G.W. Skelton. Cyber security for emergency management. IEEE International Conference on Technologies for Homeland Security (HST), pp. 476-480, ISBN 978-1-4244-6047-2, Waltham, MA, USA, 8-10 Nov. 2010.

[20] R. Akella, H. Tang and B.M. McMillin. Analysis of Information Flow Security in Cyber-Physical Systems. International Journal of Critical Infrastructure Protection, Elsevier, Vol. 3-4, pp. 157-173, Dec. 2010.

[21] R. Mitchell and I.-R. Chen. A hierarchical performance model for intrusion detection in cyber-physical systems, Proc. IEEE Wireless Communications and Networking Conference (WCNC), pp. 2095 - 2100, 28 - 31 Mar. 2011.

[22] D.A. Kindy and A.K. Pathan. A survey on SQL injection: Vulnerabilities, attacks, and prevention techniques. Proc. IEEE International Symposium on Consumer Electronics, pp. 468 471, Singapore, 14 - 17 June 2011.

[23] R. Mitchell and I.-R. Chen. Survivability analysis of mobile cyber physical systems with voting-based intrusion detection. Proc. 7th International Wireless Communications and Mobile Computing Conference (IWCMC), ISBN 978-1-4244-9539-9, IEEE, Istanbul, Turkey, 4-8 July 2011.

[24] G. Jakobson. Mission cyber security situation assessment using impact dependency graphs. 14th International Conference on Information Fusion, Chicago, Il, USA, 5-8 July 2011.

[25] Y.-J. Chen, J.-S. Shih and S.-T. Cheng. A Cyber-Physical Integrated Security Framework with Fuzzy Logic Assessment for Cultural Heritages. Proc. of IEEE International Conference on Systems, Man and Cybernetics, pp. 1843-1847, ISBN 978-1-4577-0652-3, Anchorage, AK, USA, 9-12 Oct. 2011.

[26] G. Wu, D. Lu, F. Xia and L. Yao. A Fault-Tolerant Emergency-Aware Access Control Scheme for Cyber-Physical Systems. CORR, abs/1201.0205, 2012.

[27] N.O. Tippenhauer, C. Popper, K.B. Rasmussen, and S. Capkun. On the Requirements for Successful GPS Spoofing Attacks. Proc. 18th ACM conference on Computer and communications security, ISBN: 978-1-4503-0948-6, pp. 75-86, Chicago, USA, 17-21 Oct. 2011.

[28] J.P.G. Sterbenz, E.K. Cetinkaya, M.A. Hameed, A. Jabbar, S. Qian, and J.P. Rohrer. Evaluation of network resilience, survivability, and disruption tolerance: analysis, topology generation, simulation, and experimentation. Telecommunication Systems, Springer, DOI: 10.1007/s11235-011-9573-6, Dec. 2011.

[29] J. Lin, W. Yu, X. Yang, G. Xu, and W. Zhao. On false data injection attacks against distributed energy routing in smart grid. ACM/IEEE Third International Conference on Cyber-Physical Systems, Apr. 2012.

[30] P. Falcarin, C. Collberg, M. Atallah, and M. Jakubowski. Software Protection, Guest Editors' Introduction, IEEE Software, pp. 24-27, March 2011.

[31] J. Walker. Cyber Security Concerns for Emergency Management. Emergency Management, InTech, ISBN: 978-953-307-989-9, Jan. 2012.

[32] R. Haji, A. Hasbi, M. Ghallali, and B. El Ouahidi. Towards an adaptive QoS-oriented and secure framework for wireless sensor networks in emergency situations. International Conference on Multimedia Computing and Systems, pp. 1007-1011, 10-12 May 2012.

[33] P. Traynor. Characterizing the Security Implications of Third-Party Emergency Alert Systems over Cellular Text Messaging Services. IEEE Transactions on Mobile Computing, 11(6), pp. 983 - 994, June 2012.

[34] F.M. Delle Fave, A. Rogers and N.R. Jennings. ARGUS: A Coordination System to Provide First Responders with Live Aerial Imagery of the Scene of a Disaster (Demonstration). Proc. 11th International Conference on Autonomous Agents and Multiagent Systems. Vol. 3, pp. 1467-1468, 4 June 2012.

[35] E. Gelenbe and F.-J. Wu. Sensors in cyber-physical emergency systems. Proc. IET Conference on Wireless Sensor Systems, ISBN 978-1-84919-625-3, London, UK, June 2012.

[36] C. Du and S. Zhu. Research on urban public safety emergency management early warning system based on technologies for the internet of things. 2012 International Symposium on Safety Science and Technology. Procedia Engineering, 45, pp. 748-754, 2012.

[37] E. Gelenbe, G. Gorbil and F.-J. Wu. Emergency Cyber-Physical-Human Systems. 21st International Conference on Computer Communications and Networks (ICCCN), Munich, Germany, 30 June - 2 Aug. 2012.

[38] J. Rajamaki, P. Rathod, A. Ahlgren, J. Aho, M. Takari and S. Ahlgren. Resilience of Cyber-physical System: A Case Study of Safe School Environment. Intelligence and Security Informatics Conference (EISIC), 10.1109/EISIC.2012.10, Odense, 22-24 Aug. 2012.

[39] D. Harries and P.M. Yellowlees. Cyberterrorism: Is the U.S. Healthcare System Safe? Telemedicine and e-Health. 31 Oct. 2012.