July 2011

Communications and Radar Sensors Networks for Security Applications

Rajesh Namdev

IITM,Gwalior, rnamdev@gmail.com

Prateek Bhadauri

IITM,Gwalior, Bhadauria.prateek@gmail.com

Mahendra Singh Bhadoria

IITM,Gwalior, mahendra79bhadoria@rediffmail.com

Follow this and additional works at: <https://www.interscience.in/ijssan>

Part of the [Digital Communications and Networking Commons](#), and the [Electrical and Computer Engineering Commons](#)

Recommended Citation

Namdev, Rajesh; Bhadauri, Prateek; and Bhadoria, Mahendra Singh (2011) "Communications and Radar Sensors Networks for Security Applications," *International Journal of Smart Sensor and Adhoc Network*: Vol. 1 : Iss. 1 , Article 5.

DOI: 10.47893/IJSSAN.2011.1004

Available at: <https://www.interscience.in/ijssan/vol1/iss1/5>

This Article is brought to you for free and open access by the Interscience Journals at Interscience Research Network. It has been accepted for inclusion in International Journal of Smart Sensor and Adhoc Network by an authorized editor of Interscience Research Network. For more information, please contact sritampatnaik@gmail.com.

Communications and Radar Sensors Networks for Security Applications

1Rajesh Namdev, 2Prateek Bhadauria, 3Mahendra Singh Bhadoria
IITM, Gwalior

Email id: ¹Bhadauria.prateek@gmail.com, ²rnamdev@gmail.com, ³mahendra79bhadoria@rediffmail.com

Abstract: *In the area of security and safety applications, we are investigating the potential impact of emerging communications technologies for public safety. Cognitive radio is being studied for enhanced interoperability and availability of communication systems in EU-wide multi-national operational scenario. Sensor networks are being studied for surveillance of sensitive public areas.*

In the design domain, we investigate radio frequency (RF) threats and interference in communication and navigation systems. These can have serious impact on intelligent transportation systems and next generation ICT systems. Vulnerabilities of next generation information-communications systems are being studied as the architectures of next generation networks (NGN) are emerging and new relevant standards are being defined.

1. INTRODUCTION:

Defending against attack is the key successful factor for sensor network security. There are many approaches that can be used to detect and defend against attacks, yet few are focused on modeling attack distribution.

Knowing the distribution models of attacks can help system estimate the attack probability and thus defend against them effectively and efficiently. In this paper, we use assessment of technical specifications, protocols and standards for radio spectrum management – the foundation of wireless communication infrastructure. The deployment for safety aspect aims to design broad-based system architectures that can be used by a class of security solutions for a range of threat scenarios in public safety. This requires integration of diverse technologies from radars to sensor networks and wireless communication protocols into demonstrable technical solutions for public safety, crisis management and area surveillance.

2. Design for Security:

High performance Radar Network has been deployed for homeland security applications. Having the radars on

networks allow for increased coverage via multiple radars, as well as the communications of situational awareness in real time to multiple remote users. Sensor networks are very attractive for reconnaissance and surveillance applications as they provide more information from the same target, which helps to identify, classify, and track it. Furthermore, sensor networks possess a higher probability to survive if individual sensors fail. Defending against attacks is the key successful factor for sensor network security. Attack distribution model can help systems defend against attacks before they occur or if they have already occurred but have not been detected. Our models can be applied to many types of attacks. Many sensor networks have mission-critical tasks, such as above military applications. Thus, the security issues in WSNs are kept in the foreground among research areas. Compared with other wireless networks, such as ad hoc wireless LAN and cellular networks, security in WSNs is more complicated due to the constrained capabilities of sensor node hardware and the properties of the deployment environment. Security issues mainly come from attacks. If no attack occurred, there is no need for security. Thus, detecting and defending against attacks are important tasks of security mechanisms.

Fig-2.1-Security Mechanisms of WSN.

Sensor networks offer economically viable solutions for a variety of applications. For example, current implementations monitor factory instrumentation, pollution levels, freeway traffic, and the structural integrity of buildings.

3. Modeling of Radar sensor networks:

3.1. Network and Security Assumptions

The followings are assumptions of WSNs.

- (i) **Base station:** the base station is computationally robust, having the requisite processor speed, memory, and power to support the cryptographic and routing requirements of the sensor network. Adversaries can destroy the base station but they cannot compromise it within the limited time.
- (ii) **Sensor nodes:** the sensor nodes are similar to current generation sensor nodes in their computational and communication capabilities and their power resources. They can be deployed via aerial scattering or by physical installation. We assume that any sensor node will know the position of itself and its immediate neighbor nodes after deployment and the base station will know all the nodes' positions.
- (iii) **Adversary:** adversaries have unlimited energy and computing power. An attacker needs to spend some time to attack a node. In the attacking process, they will

not change the targets until the chosen target nodes were attacked. After attacking one node, the attacker will continue attacking a new good node without any halt, stop, or hibernation.

Fig-3.1,An Example of Radar System.

4. Challenges in Radar sensor Networks:

There are clear challenges to the further development and use of local radar sensor systems and networks as well as for their implications and impacts on individuals, organizations, and nations. One way to look at the challenges of sensor technologies is to consider the convergent hardware and software, which leads to great complexity and associated challenges. The convergence of micro-sensors, microelectronics, micro-controllers, semiconductor memories, and small radios, as well as components for monitoring battery energy and received RF-signal strength, requires dealing with a plethora of interfaces.

5. Conclusion:

This paper presents a new extended concept Radar sensor Networks which leads to get a better interoperability between systems mainly using internet protocols and

internet itself The goal is to share and receive relevant data in real time, when possible, so that survivability, responsiveness and efficiency can be improved. As sensors are becoming miniaturized, high resolution, cost-effective, consequently embedded in satellite, UAV, ground vehicles and thus more and more numerous it is necessary to sort, make synthesis and give priorities amounts of data via QoS management as long as bandwidth, data processing and computing capabilities are not infinite.

6. References:

- [1.] *Xiangqian Chen, KiaMakki, Kang Yen, and Niki Pissinou, EURASIP Journal on "Wireless Communications and working Volume 2008, Article ID 754252."*
- [2.] *David J. Nagel, "Wireless Sensor Systems and Networks Technologies, Applications, Implications and Impacts".*
- [3.] *Dr Pravir Chawdhry, "European Communities, 2009", CORSA. JRC55068.*
- [4.] *Tim.j.nohara, peter weber, graeme Jones, "Affordable high performance radar networks for homeland security applications".*
- [5.] *Laurent Enel, and Franck Guillem, "Improvements in Navy Data Networks and Tactical Communication Systems, World Academy of Science, Engineering and Technology 18 2006."*