Chapter 2

Quality of Sensor-Originated Information in Coalition Information Networks

Chatschik Bisdikian
IBM Research, USA

Lance M. Kaplan
U.S. Army Research Laboratory, USA

Mani B. Srivastava
University of California at Los Angeles, USA

David J. Thornley
Imperial College London, UK

Dinesh Verma
IBM Research, USA

Robert I. Young
Defence Science and Technology Laboratory, UK

ABSTRACT

Coalition operations greatly benefit from the exchange of information collected from a plethora of wirelessly communicating sensors deployed in the theater of operation. However, to make judicious use of this information and then act effectively based on this information, knowledge of its quality, and a common means of expressing and communicating this quality are necessary. This chapter considers quality of information (QoI) for sensor networks starting with building a definition of QoI from first principles and by exploiting industry efforts to define quality in other domains, notably quality of service. The definition touches upon two complementary yet distinct aspects of quality: (a) the inherent quality attributes that characterize information; and (b) the assessment of these attributes within the context of applications utilizing the information, referred as the value of information (VoI). It then discusses information as a service and the various QoI viewpoints that associate sensor-originated information providers with sensor-enabled applications in dynamic coalition environments. Then, information pro-

DOI: 10.4018/978-1-61520-855-5.ch002
INTRODUCTION

Achieving and then exploiting critical information advantage over adversaries is a key objective of military network-centric operations (NCO) (Alberts, Garstka, Hayes, & Signori, 2001). Such military operations may be executed by either single-nation units or, of particular interest to this book and this chapter, by multi-nation coalition partners. Critical information advantage allows coalition partners to gain a deep, common understanding of situations, i.e., shared situation awareness, at an accelerated pace. It allows the timely support of decision making regarding actions towards the situations of concern that are both effective with respect to their outcome and efficient with respect to the resources spent for and assets affected by these actions.

In pursuit of information advantage and, more broadly, information superiority, an intertwined web of various types of assets is utilized for the creation, manipulation, and dissemination of pertinent information and ensued knowledge. These assets—including physical, i.e., hardware; virtual, i.e., software; and human assets—are organized in a collection of layered networks including (from bottom-to-top):

- **physical networks**: comprising data sources, e.g., sensors and communication networks;
- **information networks**: comprising information technology (IT) systems and the processes and protocols they support for managing information, including processing, storing, indexing, retrieving, disseminating, and so on; and
- **user (or social) networks**: comprising the information consumers (computer applications, humans, and human-computer interfaces (HCI)) on behalf of which information is collected and knowledge about situations is shared.

The scope of an information network may extend to include not only the hardware and software system infrastructure but also the collection of all the information pieces that reside or are accessible through these systems as well as any linkages and references that exist to or can be made amongst these pieces.

Sensing systems of various types and configurations, including in situ or remote sensors, stationary or mobile multi-sensor platforms, sensor networks, and combinations thereof, are key enablers of the NCO objective for information superiority. With their ever increasing capabilities, with respect to sensing, communications, processing, operational lifetime, sensing systems are deployed to provide real (or, near real) time information of situations in ways that were never possible before or exposed humans to heightened danger otherwise. Note, however, that sensor-originated information is not necessarily a substitute for all kinds of human-collected intelligence—sensors are, for the foreseeable future, incapable of interpreting, on their own, the social and cultural contexts surrounding the situations they observe. Instead, depending on the circumstances, the two types of gathered in-
Related Content

Improving Cyber Defense Education through National Standard Alignment: Case Studies
www.igi-global.com/article/improving-cyber-defense-education-through-national-standard-alignment/210625?camid=4v1a

Next Generation Home Network and Home Gateway Associated with Optical Access
www.igi-global.com/chapter/next-generation-home-network-home/36335?camid=4v1a

The Blockchain Technology: Applications and Threats
www.igi-global.com/article/the-blockchain-technology/201093?camid=4v1a

A Survey on Chaos Based Encryption Technique
www.igi-global.com/chapter/a-survey-on-chaos-based-encryption-technique/214810?camid=4v1a