ABSTRACT
Integration of trusted information is an important requirement from business application. As business applications adaption relies on sensor data, that information must be trustworthy enough in order to prevent any misuse of sensor data. For example, the use of un-trustworthy information in healthcare system can have severe consequence on patient life. But it appears that sensors are not tamper resistant enough in order to prevent any capture of cryptographic material stored on the nodes. Therefore, a soft security alternative of hardening security mechanisms is to ensure trustworthiness of sensor data. From its production on the node to its delivery to the business application, and including its processing and forwarding, the authors propose to assess sensor data along its life-cycle. In this paper, the authors propose a framework for the assessment of sensor data trustworthiness, from the acquisition at the node to their delivery to business applications, including any intermediary routing or processing. The assessment aims at identifying erroneous sensor data caused intentionally or unintentionally. In addition, the authors evaluate their approach with real sensor data acquired in the scope of the WASP project (http://www.wasp-project.org - Wirelessly Accessible Sensor Populations - IST 034963) during a herd control experiment.

Keywords: Computer Science, Herd Control, Sensor Networks, Subjective Logic, Trust Management

1. INTRODUCTION
Apart from technical issues (e.g., data routing, WSN discovery), business applications come along with strong trust requirements on sensor data delivered by WSN. Therefore, when WSNs are integrated into business processes, the delivered data can severely influence the applications choices and the actions taken in the real world. A good example is remote patient monitoring: a patient is equipped with a Body Sensor Network (BSN) (Zhang, 2006) which monitors vital information (e.g., heart rate, body temperature, SPO2) and activities (e.g., walking, running, falling). Erroneous sensor data can lead to a wrong therapy for this person. If an emergency is undetected, it can result in the death of the person.

DOI: 10.4018/ijaeis.2013100101
Erroneous or non-trustworthy sensor data can have two different reasons: Intentional misbehavior and unintentional errors (Raya et al., 2007). Unintentional sensor data errors are caused by malfunction of the hardware (broken or obstructed sensors), mis-positioning of the node (untied or incorrectly attached node) or exhausted batteries. Intentional misbehavior is caused by attackers, exploiting security vulnerabilities of WSNs, e.g. in the routing protocols.

In order to target intentional misbehavior in WSN, several security mechanisms, especially tailored for WSN, have been proposed in the literature (Hämäläinen et al., 2006; Chaouchi & Laurent-Maknavicius, 2009). The most efficient of one consider are traded with the energy saving requirements and the limited resources (memory, CPU) on nodes. But, implementing “cheaper” security solutions can open more exploitable flaws. Relating to the capability of easy deployment and mobility, WSN nodes are often easily accessible and rarely tamper-resistant (Zhang et al., 2006). Hijacking of nodes and extraction of cryptographic material is quite easy and gives the attacker the possibility to add malicious nodes or inject bogus data into the network.

Instead of hardening the security in WSNs, assessing the trustworthiness of sensor data is an alternative solution. The goal of the trustworthiness assessment is to assist business applications in decision making, by determining whether they can rely on the data or not. Trustworthiness is defined as the probability that sensor data really corresponds to the measurement in the physical world. This approach has two main advantages: (i) it allows business applications to separate erroneous sensor data from trustworthy ones, and (ii) it supports energy optimization in WSNs. Energy saving can be achieved when non-trustworthy sensor data is already filtered out on the sensor or within the network considering that data transmission is the most energy consuming task in WSN.

In this paper, we propose a framework for the assessment of sensor data trustworthiness, from the acquisition at the node to their delivery to business applications, including any intermediary routing or processing. The assessment aims at identifying erroneous sensor data caused intentionally or unintentionally. In order to properly assess trustworthiness of sensor data, we formalize the life cycle of sensor data, from its acquisition on the nodes, to their delivery to business applications, including intermediary processing or routing.

This life cycle supports us with the definition of trust model for sensor data. We then choose to apply subjective logic to our trust model. Among others, subjective logic framework appears to be the well tailored to capture the trustworthiness of sensor data. It incorporates the notion of uncertainty on sensor data trustworthiness. Even though subjective logic fits our trust model, we identify the need for the definition of new operators for sensor data state along its life-cycle, especially for aggregation or fusion.

We finally evaluate this approach with sensor data collected during a herd control experiment developed in the context of WASP (Mol et al., 2009). In this scenario, we discuss the feasibility and the results obtained with our trustworthiness assessment approach. Our goal is to provide to end-users clear trust indicators over sensor data and derived information, in order to support them with their final decision making.

This paper is organized as follows. In Section Background, we discuss the state of the art related to trust assessment of sensor data. In Section Trust Model for Sensor Data, we introduce a trust model for sensor data, along the sensor data life cycle. In Section A Subjective Logic Approach, we define a set of new operators which support the trustworthiness assessment at acquisition, processing and routing time. At last, we evaluate the feasibility of our approach in Section Implementation and Evaluation. Future work and conclusion are finally discussed.
Analysis of Material and Information Flows and Formulation of an ICT Waste Management Model
www.igi-global.com/article/analysis-of-material-and-information-flows-and-formulation-of-an-ict-waste-management-model/120471?camid=4v1a