LARUS

21st Century Territorial Security

a sensor networking approach

November 2011
Larus Technologies Corporation

Abstract

Territorial security deals with the prevention, detection, and response to unauthorized persons and/or goods from crossing a perimeter. It deals with large territories of strategic importance, such as international borders, transportation and critical infrastructure. Sensor networks are novel data routing and processing structures that enable data-centric applications, such as the continuous monitoring of an elderly person's health. In this white paper, we concentrate on the challenges presented in applying the concepts of sensor networking and data fusion to the problem of territorial security, and how we plan to resolve them. We first introduce the conventional techniques and their drawbacks, then briefly present our solution and the steps involved in its development.

Territorial Security

Preventing, detecting, and responding to unauthorized persons and/or goods crossing a perimeter is a security concern of individual, corporate, and international scope. State-of-the-art perimeter-security solutions use physical barriers, sensors (indoor motion, cameras, audio/vibration), and human personnel (a camera operator, entrance guard, and patrolling security guards). These procedures are effective in a limited scenario, where a few entrance points are constrained by well-delineated physical boundaries.

Territorial security, however, deals with large territories of strategic importance, such as international borders, transportation (airports, rail yards, public transit), and critical infrastructure (energy, water & agriculture, emergency services, etc.) [1]. When dealing with such a scope, a number of challenges present themselves. First, a linked security system of this size is inflexible and expensive to setup. Second, system operators frequently suffer from overload, stress, and inattention due to the substantial influx of data. Finally, it is increasingly important for territorial security systems to allow for the sharing of knowledge to authorized users and systems.

Larus Technologies proposes a novel, real-time decision-support-system intended to provide overall territorial security for an area of strategic importance. The proposed system starts by sensing the environment.

Sensor Networks

Current perimeter-security systems demonstrate the effectiveness of fixed, wired sensor networks. A network of sensor nodes positioned along a perimeter collects disparate and diverse types of relevant data [2]. As examples of perimeter-security

sensor suites: color and infrared cameras enable the detection and recognition of intruders; acoustic sensors sense activities near a barrier, such as digging; while sonar and radar provide the location of marine or air-based objects. Due to the problem size, territorial security must be more flexible from a deployment standpoint, than traditional perimeter security. In our proposed solution, sensor nodes themselves need not be stationary; in fact, they may reside on mobile platforms such as manned/unmanned ground/aerial vehicles. This sensor node mobility provides the requisite flexibility for large-area deployment and decreases initial setup costs.

To provide such mobility, Larus intends to equip stationary and mobile platforms with a sensor payload that includes video, acoustic data capture, radar, and a Global Positioning System (GPS). The system design is flexible, allowing the use of a variety of data sources. In addition, Larus has recently demonstrated the extraction of relevant features on visual data streams which allows one to selectively transmit relevant information to downstream networks. This not only saves bandwidth but also power if the application is energy-constrained. Larus' state-of-the-art intelligent video analytics technology includes motion detection, object tracking, face/vehicle detection, and license plate recognition. For example, in Figure 1 (left), the system tracks movement of a foreground object, a person, crossing an operator-defined polygon denoting a fence. Moreover, Figure 1 (right) shows the tracking of a stopped object as well as an abandoned object. The detection capability is robust against compression artifacts, imperfect focusing, and certain changing environmental conditions (e.g. light wind, rain, lighting variability).

Figure 1. Detecting object intrusion (left), stopped, and abandoned objects (right).

Data Fusion

In order to detect intrusions along a long perimeter, the tide of incoming data must be interpreted. This data is not limited to sensor readings; it can include databases, operator reports, and other sources of information (see Figure 2). The Larus Fusion Engine (LFE)

fuses these data streams in real-time, issuing alerts when anomalous behaviors are detected. Furthermore, the raw data is mined for patterns that represent information, with the set of patterns representing the knowledge attained by the system. This combination of data mining and fusion forms a decision-support system (DSS) and alleviates the strain on the operator by reducing the influx of information to a manageable level.

The operator's system display screen provides global and local informational views, aggregating the relevant system events and alerts. Moreover, the display screen, processing, and storage module can even be ruggedized and located within moving vehicles [3]. This gives operators and the response team wide flexibility when planning appropriate counter measures.

The LFE uses well-developed, current technologies (XML and Semantic Web ontologies) to allow for future extensibility and to encourage interoperability with existing platforms. Information sharing and data fusion is a critical component in today's Homeland Security and MAJIIC initiatives [4] [5]. Authorized users and systems are given secure access to each sensor's data stream, current and/or historical, as well as data fusion capabilities.

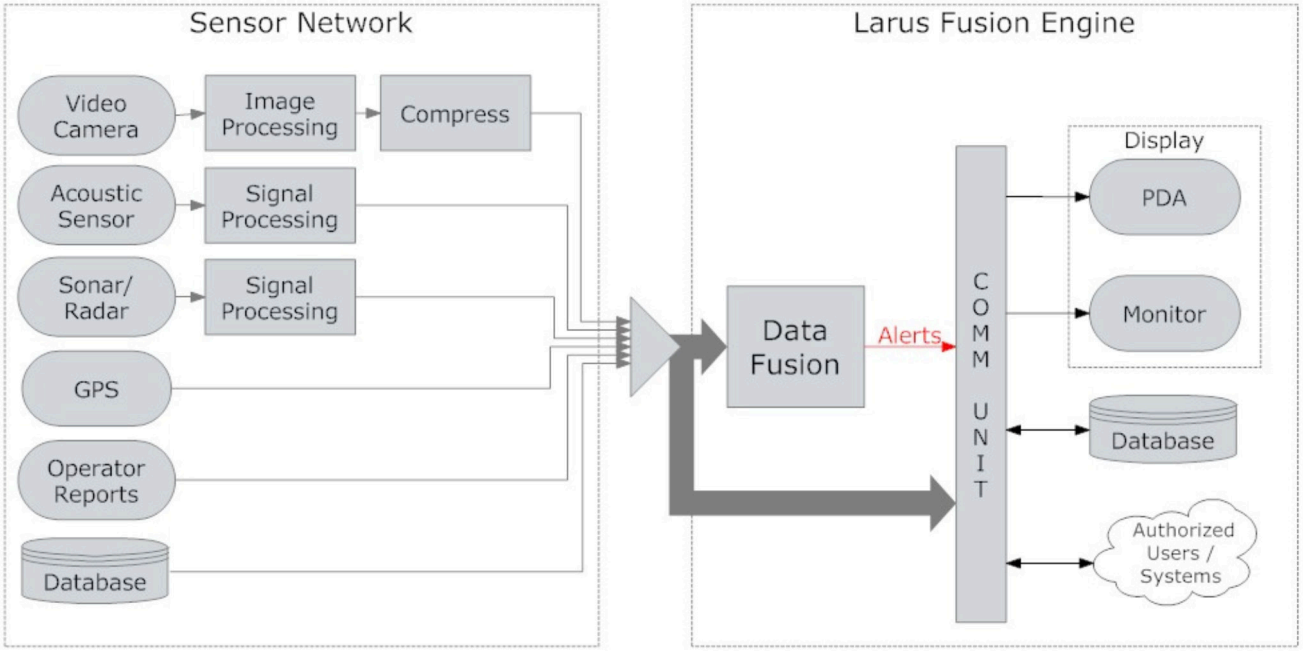

Figure 2. Data flow of proposed system.

The initial reference platform, shown in Figure 3, would consist of an unmanned ground vehicle (UGV) equipped with a data fusion payload that consists of a single- board computer (SBC), an integrated and deployable video compression system and an acoustic data capture system, running an intelligent data analytics software for the purpose of

territorial security. The LFE runs a closed-loop decision-support system that takes in the data source inputs, extracts the required information from their raw data streams and, according to the user's decision, proceeds to perform a plan of action through effectuation of the environment. As the latter has now changed, the data consumption phase starts another run through the DSS loop.

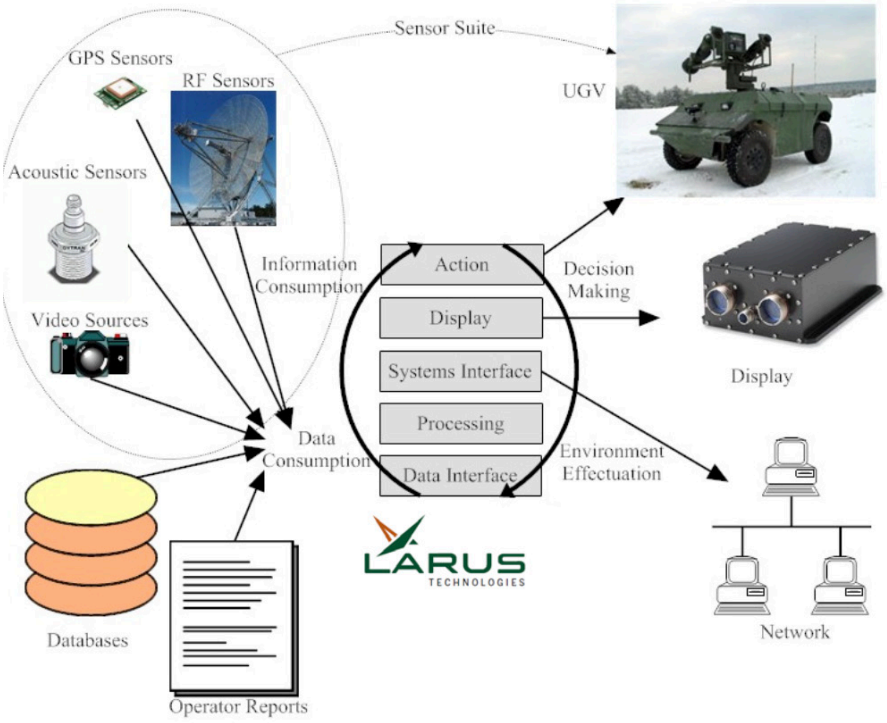

Figure 3. Initial reference platform.

Conclusions

Sensor networks and data fusion are poised to improve the state-of-the-art in territorial security systems. Larus' product-line and expertise areas provide an ideal foundation to solve this task. Our intended solution offers deployment flexibility, eases operator overload, and offers interoperability/data sharing capabilities.

References

[1] USBX Advisory Services, “HSIC 2006; The State of Play in Homeland Security: Critical Infrastructure – The Next Frontier.” 2006.

[2] Rami Abielmona and George Dinardo, “Networking: The Growing Role for Advanced Sensors.” Vanguard, March/April 2007, pp. 23.

[3] Simon Collins, “VPX: Architecture of Choice for Situational Awareness.” COTS Journal, September 2007, pp. 34-43.

[4] Imperial Capital LLC, “HSIC 2007; Thinking Through the Homeland Security Landscape: A Guide Through the HLS Market Segments and Technologies.” 2007.

[5] Lars Nesse, “MAJIIC: Multi-sensor Aerospace-ground Joint ISR Interoperability Coalition.” October 2006.

About Larus

Through our culture of innovation and research, Larus Technologies has developed the next generation of embedded technology for developers of mission-critical C4ISR Systems and Security Systems.

With a solid foundation pioneering high level information fusion (HLIF) for the ever-changing defense and security industries, Larus is perfectly positioned to help Original Equipment Manufacturers (OEMs) make a world of difference. Working at the higher levels of the US Department of Defense’s Joint Director of Laboratories (JDL) information fusion model, our technology not only delivers more knowledge, its adaptive learning algorithms deliver more accurate and more predictive information—faster.

170 Laurier Ave West, Suite 310
Ottawa, Ontario K1P 5V5
Canada

Phone +1 (613) 244-8916
Fax +1 (613) 244-9941

www.larus.com