An Architecture to Support Mission Orientated Wireless Sensor Network Surveillance Applications

D S Ghataoura†, J E Mitchell† and G Matich‡

† University College London, ‡ Selex Galileo, Basildon, Essex, U.K

Abstract: Sensor networks represent a powerful new data paradigm facilitating the development of new intelligent applications. In support of mission critical applications such as surveillance, sensors can be made to operate effectively in their deployed environments by adopting a "situation awareness" perspective. In this paper we present and adapt our VIGILANT "situation aware" system architecture to cater for mission orientation, in terms of the perceived surveillance threat and communication channel environment. By taking a joint context view, we envisage deployed sensors to self-organise efficiently into dynamic ad-hoc groups, based on a current threat "situation" with added tolerance to communication link disruption, thus maintaining mission objectives and quality of service reliability.

1. Introduction

With the advancement of autonomous, battery operated, wireless communication capable sensing platforms, multi-modal sensor based systems are becoming very powerful and flexible sources of information that support a wide collection of applications. Sensor networks are often deployed over an area of interest to gather information to aid some form of decision making, in support of these applications, such as surveillance. Surveillance applications however can be made to operate effectively in their deployed environments, by adopting a "situation awareness" perspective and methodology. Situation awareness increases the perception of environmental elements within dynamic and uncertain time and space constraints that are typical of such applications [1].

Deployed sensor networks which have an awareness of their current situation, can therefore provide command and control (c^2) systems a better informed view as to temporal unfolding of events and their understanding of the implications of those events. This further facilitates current ongoing improvements in both quality and timeliness of decision making for overall future mission planning [2].

1.1 Mission Orientated Sensor Network

For executing time-critical missions, sensor networks can be viewed as a distributed dynamic system within their physical operational environment. A mission orientated sensor network (MOSN) is such a dynamic system with additional high-level descriptions to support specific mission goals. MOSN nodes operate by accepting inputs from neighbouring nodes, to participate in either individual or ad-hoc group based dynamic adaption decision making, to satisfy mission goals and current changes in the physical environment, as shown in figure 1.

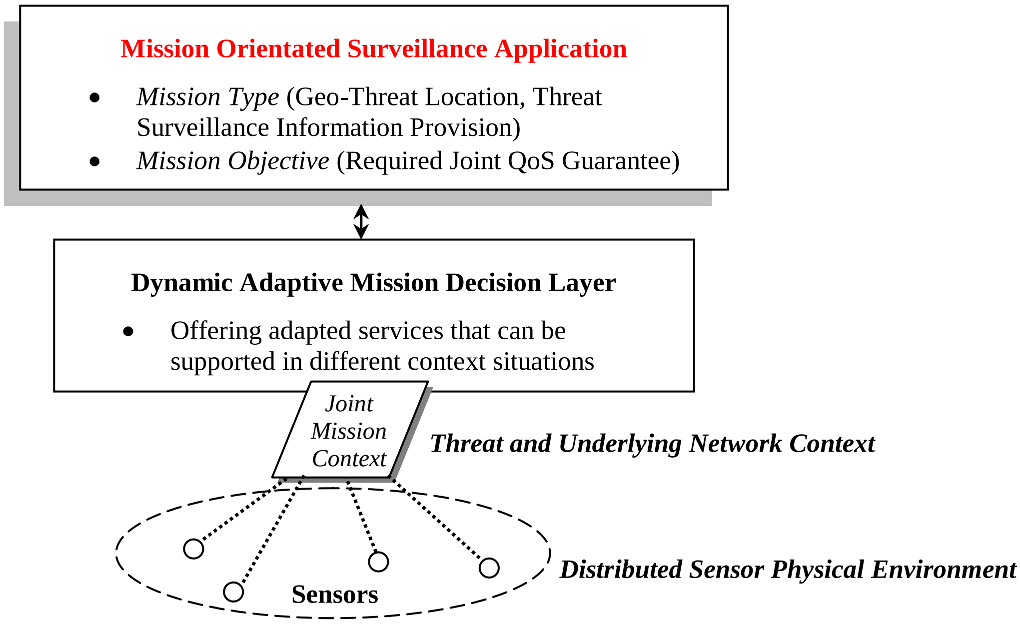

Figure 1. Mission Orientated Sensor Network Node Architecture

Utilising MOSN's can provide c^2 an adaptable infrastructure for dependable efficient "context aware" information collection, providing increased operational longevity required in real time surveillance applications. Utilising mission orientated service architectures, supports dynamic self-reconfigurable networks of sensor nodes, capable of jointly understanding mission objectives and adapting to the dynamics of difficult and uncertain physical environments.

We take a joint situation context view of the sensors operational physical environment, namely the perceived threat and the underlying changing network situation. As a result of unreliable wireless channel environments, dynamic network topologies are created, effecting overall mission quality of service (QoS) reliability. Applications require a minimum QoS, which the underlying network must maintain over a period of time. This presents new challenges for efficient and adaptive routing decisions and involves understanding the time evolution of the channel environment and their effect on mission execution.

In this paper we present a new architecture based and derived on our VIGILANT situation aware system, to cater for dynamic adaption to mission objectives. We take the view that providing an adaptable architecture with an integrated tolerance mechanism to communication link disruption, can therefore aid to preserve both mission orientation objectives and quality of service reliability constraints.

2. VIGILANT: "Situation Aware" Quality of Information Interest Groups

As can be seen from figure 2, VIGILANT [4] is a 3 level situation awareness system. VIGILANT takes inspiration from "conceptual integration" [3] inspired by and relating to the mammalian brains approach to fragmented sense making, namely conceptual recursive perception – Level 1, mental modelling – Level 2 and categorisation/framing – Level 3.

VIGILANT firstly establishes which neighbouring sensors share common "threat context" and subsequently based on this shared "context" to organize into "situation aware" groups to provide a better overall situation perspective of the surveillance environment, in terms of Quality of Information (QoI) [5]. Information is transmitted and shared, after an evaluated projection time, dependent on the level of shared context.

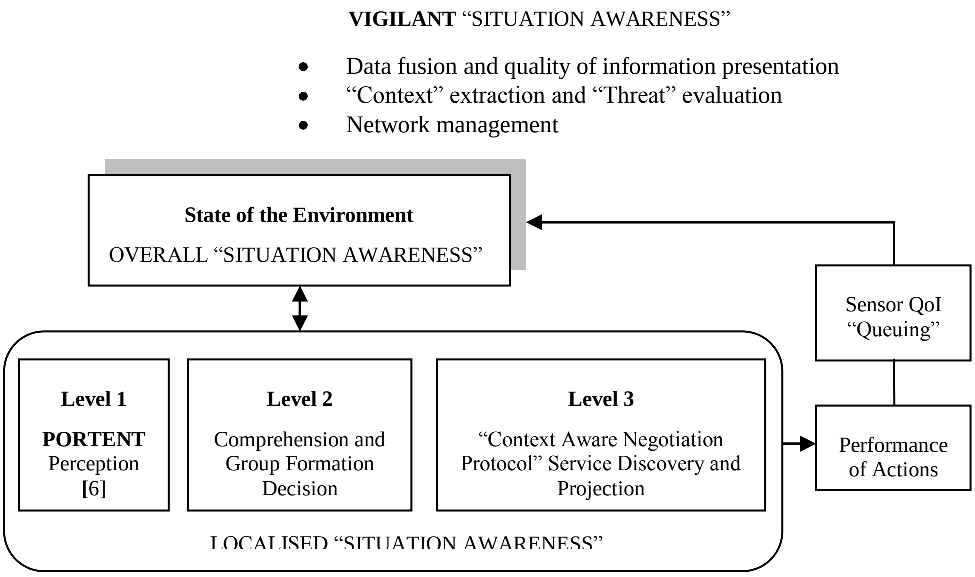

Figure 2. Overall combined VIGILANT "situation awareness" surveillance system architecture

3. Adapting VIGILANT to Mission Orientation

VIGILANT presently provides a framework for distributed sensors to self-organise into dynamic ad-hoc groups, without considering the underlying network, for robust formation, against possible communication link disruption. We envisage an architecture design to facilitate information collection, within wireless environments that are normally unreliable. The purpose of the platform is to abstract lower level functionality such as network connectivity and provide a higher level coordination interface. Often the combination of characteristics from the environment and application drive the design of the middleware system. VIGILANT middleware design, for mission orientation must encompass the following features:

- VIGILANT operation is essentially a **cooperative application** that shares available resources (e.g. channel bandwidth) and cooperates to achieve specific goals, depending on mission type (Threat geo-location, Threat QoI provision).
- VIGILANT, inherently has **constrained application QoS demands**, in the form of a QoI service provision time, dependent on the level of shared context. The service provision time determines when information needs to be transmitted to the designated group leader, for QoI fusion purposes. Furthermore, the required QoS and the means of meeting it can change over time, either as the state of the application or the availability of network sensors. This must be maintained over the period of the set value, to facilitate fault tolerant operation, critical for VIGILANT success.

Combining these features, it becomes imperative that VIGILANT middleware architecture for mission orientation must be proactive and adapt the network configuration, to meet QoS demands. For example specifying which sensors should send information, which sensors could act as routers to cater for link disruption mitigation in multihop networks and which sensors could provide the best possible solution to the current mission type. Figure 3, details our proposed VIGILANT mission orientated architecture.

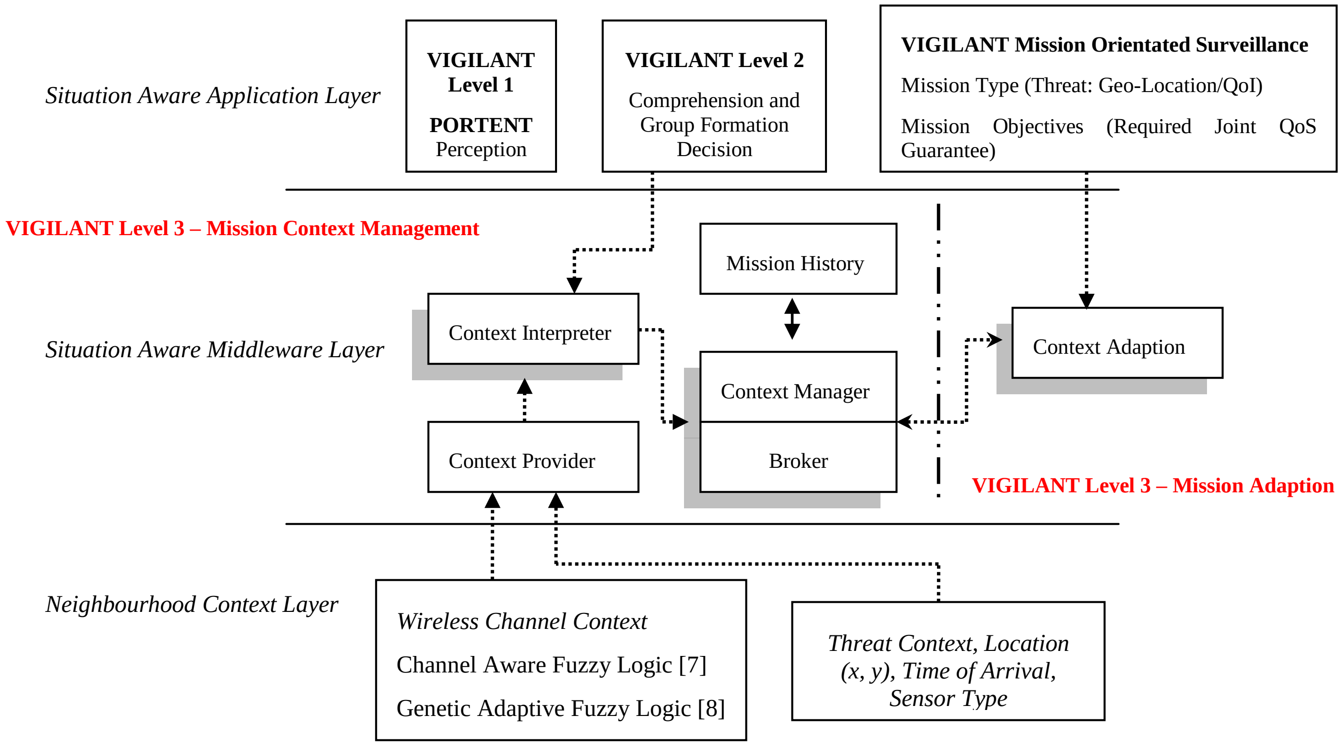

Figure 3. VIGILANT Surveillance Mission Orientated Architecture

As indicated in figure 3, VIGILANT middleware architecture consists of the following independent service components:

- ***Mission Context Management*** is highly dependent on the physical context properties of the environment. Context management is important in order to generate and provide the necessary knowledge, for decisions on actions required by the context adaption module.
  - *Context Providers* constitutes the distributed deployed sensor network. When group formation decisions are applied and enforced by the surveillance application, then this forms the local sensor neighbourhood. Providers provide low level context-sensing information for high-level context manipulation.
  - *Context Interpreter* is responsible for context processing using logical reasoning techniques, such as certainty factor model, Dempster-Shafer theory or Bayesian Belief Networks (BBN). Such techniques can be utilised to derive high-level context from low level contexts, for querying purposes, resolve conflicts and maintain consistency of relevant context knowledge.

- *Mission History* helps to keep a record of prior context for the purposes of network pattern analysis.
- *Context Manager/Broker* provides clear decoupling between the mission context management and the adaption system. Context managers detect the changes of the necessary context parameters and make the necessary operations to refresh the instances, in preparation of adaption requests. Context brokers act as the interface between the two relevant systems. Brokers provide pertinent context parameters to the adaption system, therefore providing a specialised context view for a required adaption service.

- ***Mission Adaption*** consists of the context adaption system, to allow scalable reconfigurable network operation, by proactively selecting the most suitable network sensors for meeting current mission objectives. This may restrict the set of sensors under consideration to particular locations or to those that can meet QoS requirements, for fault tolerant QoI provisioning. Selection and decision of sensors based on context information for adaptive operation, requires a preference model to trigger enabling actions to be invoked in response to changes in the current situation.

4. Conclusions

In this paper we present an architectural design framework for mission orientated sensor networks. Mission orientated sensor networks are dynamic systems with additional high-level descriptions of specific mission objectives. The architectural framework is based on our VIGILANT system and is redesigned to accommodate for tolerance against communication link disruption. Accommodating this is necessary, in order to preserve service guarantees required by the surveillance application, for threat QoI and geo-location provisioning.

Configuration/reconfiguration to network disruption (changing situation context) is carried out by the VIGILANT level 3 situation aware layer, containing both the mission context management and adaption sections. The purpose of adopting a situation aware layer is to provide transparency to the application layer without compromising the required QoS guarantees, with respect to the underlying highly dynamic sensor network. Overall, mission orientated service architectures enable dynamic self-reconfigurable networks of sensor nodes, capable of jointly understanding mission objectives and adapting to the dynamics of often harsh and uncertain physical environments.

Acknowledgments

This work is supported by Selex Galileo, Basildon, U.K under the “Networking and Application Interface Technology for Wireless Sensor Network Surveillance and Monitoring Applications” EngD program.

References

[1] Endsley M.R, “Toward a theory of situation awareness in dynamic systems”, Human Factors, 37(1), 1995, pp.32-64.
[2] Smart P.R, “Semantic technologies and enhanced situation awareness”, Annual Conference of U.S-U.K ITA, September 2007.
[3] Turner.M, “The way we think: conceptual blending and the minds hidden complexities”, New York: Basic Books, 2003.
[4] Ghataoura D.S, “VIGILANT: “Situation-Aware” Quality of Information Interest Groups for Wireless Sensor Network Surveillance Applications”, *European SPIE Security and Defence,* Toulouse, September 2010.
[5] Ghataoura D.S, “Quality of information and efficient delivery in military sensor networks”, *London Communications Symposium (LCS)*, University College London, September 2009.
[6] Ghataoura D.S, “PORTENT: Predator aware situation assessment for wireless sensor network surveillance applications”, *SPIE Defence, Security, Sensing*, Information systems and networks, Conference 7709A, Orlando, April 2010.
[7] Ghataoura D.S, “Channel Aware Fuzzy Logic Hop Selection for Wireless Sensor Networks”, *16th International Conference on Telecommunications*, 25th – 27th May 2009.
[8] Ghataoura D.S, “GAFO: Genetic Adaptive Fuzzy Hop Selection Scheme for Wireless Sensor Networks”, *IWCMC 2009 Wireless Sensor Networks Symposium*, 21st -24th June 2009.