VIGILANT: "Situation-Aware" Quality of Information Interest Groups for Wireless Sensor Network Surveillance Applications

D.S.Ghataoura[1], J.E.Mitchell[1], G.E.Matich[2]
[1]University College London, Gower Street, Torrington Place, London, WC1E 7JE;
dghataou@ee.ucl.ac.uk
[2]Selex Galileo Ltd, Christopher Martin Road, Basildon, Essex, SS14 3EL, U.K;
george.matich@selexgalileo.com

ABSTRACT

Effective situation awareness is a critical element for decision support in a wide range of military and para-military operational surveillance scenarios. Effective situation awareness in a surveillance scenario can greatly increase operational effectiveness, by improving the quality and timeliness of decisions. In this paper we outline a three level integrated design approach to promote situation awareness. Our approach allows deployed wireless sensor nodes to efficiently self-organise into dynamic clusters, based on a current common perceived threat situation (context). Firstly our distributed predator aware situation assessment system (PORTENT) models, detects and presents, in terms of quality of information (QoI), potential situations occurring within an uncertain environment. Secondly, we utilise a Bayesian belief network to understand the significance associated with the potential situation. Finally in order to obtain a better shared awareness we have developed a "context aware" service protocol that supports group formation and efficient management of sensor network assets. By combining this three level approach, we present our VIGILANT "situation aware" QoI interest group system. Extensive simulations have been undertaken to verify the VIGILANT concept, to demonstrate the effectiveness of our approach, in improving performance for network management efficiency, through utilisation of a shared "context" service provision time and QoI surveillance presentation.

Keywords: Wireless sensor networks, Quality of information, Context aware applications, Network management, Distributed situation awareness, Bayesian belief networks, Certainty factor model, Surveillance, Geo-localisation

1. INTRODUCTION

Sensor networks are often deployed over an area of interest to gather data and extract information to support operational timely and effective decision making in missions such as surveillance. Adopting a "situation awareness" perspective and methodology enables effective surveillance operation within their deployed environments. Situation awareness is the perception of environmental elements within a dynamic and uncertain volume of time and space, the comprehension of their meaning and the projection of their status in the near future[1]. A useful representation of situation awareness is provided in Endsley's "tripartite" model[1], describing three levels which contribute towards overall current situation awareness:

- ***Level 1-Perception***-involves the perception of different elements (e.g. Presence and type of target) in the environment as well as their combined characteristics (e.g. detection accuracy, certainty and timeliness), in terms of Quality of Information (QoI).
- ***Level 2-Comprehension***-understanding of the significance associated with sensor data that could be fragmented within an uncertain environment.
- ***Level 3- Projection***-the ability to evaluate and project future states of the environment based on the potential association of fragmented sensor data.

In VIGILANT deployed sensors have an awareness of their current "situation" (Threat Presence) and are able to self-organise into dynamic ad-hoc groups based on a current shared "situation" understanding (context). A self-organisation perspective therefore provides command and control (c^2) systems a better informed view as to unfolding events based on

fragmented sensor data and their implications. Our VIGILANT approach to group formation, takes active and adaptive decisions which are relevant to the current "context" within the surveillance environment. Using VIGILANT, we seek to highlight within a surveillance mission setting, the advantages offered in networking according to "context" of the sensing environment. The approach also facilitates current ongoing improvements in both quality and timeliness of decision making, essential for future mission planning[2].

1.1 VIGILANT Biological Inspiration – Conceptual Integration

Mammals commonly have to deal with ambiguous sensory information to determine whether predators are present or not[3]. The amygdala within the mammalian brain plays a central role in the processing of threat related sensory information and activation of defensive responses. Mammalian species have evolved at least two distinct neural pathways for detecting and responding to signals of threat, via sensory inputs. Fear related visual stimuli research in mammal's show that shorter sub cortical pathways appear to provide the amygdale with coarse but rapid sensory information, without waiting for further information, while longer cortical pathways provide more detailed information extraction over a longer time period[4]. In mammals, almost all sensory data gets routed via the thalamus to the amygdala for a "fast" inspection, for threat indication purposes and separately to the higher cortex "slow", but accurate processing function for more detailed examination. This provides inspiration to assume that the mammalian brain comprises of decision making components, which are able to process and integrate fragmented sensory data in different ways, in a variety of contexts and at different speeds[5].

VIGILANT situation awareness system, takes inspiration from the mammalian brains ability to make decisions in uncertainty scenarios, "conceptual integration"[6]. According to conceptual integration, which is assumed to be ubiquitous to everyday thought and language, elements and vital relations from diverse scenarios are "blended" in a subconscious process, namely through conceptual recursive perception – level 1, mental modelling – level 2 and categorisation/framing – level 3. In VIGILANT an integration approach ensures that sensed elements from the current changing situation are integrated (levels 1 and 2) effectively, in relation to the mammalian brains approach to fragmented sense making. This initiates new situation awareness meaning, through further establishing relevant decision making outcomes for sensor network self-organisation (level 3), in support of mission critical applications such as surveillance. Using this finding we present our VIGILANT situation awareness system, shown in figure 1.

2. VIGILANT SITUATION AWARENESS SYSTEM

VIGILANT operation is primarily focused on the analysis (level 1) and derivation of context information from the surveillance environment (level 2, 3). VIGILANT sensors firstly establish their own localised view of the "situation" and whether to invoke their decision for group formation (level 2). Upon the decision for formation by the group initiator, requested "context" information from neighbouring sensors is evaluated, to determine the degree of confidence in "context" (level 3, part a). VIGILANT sensors subsequently then self-organize into "situation aware" groups and report their QoI values after an evaluated service time bound, based on the level in shared "context" (level 3, part b). This facilitates a better and informed view of the overall situation perspective about the presence of threat, in terms of QoI. A "context aware" group perspective about the pervading situation, in terms of QoI, increases operational effectiveness since:

- QoI about the surveillance environment represents the capability and characterisation measure for sensor derived information flowing through the sensor network[14]. Utilising a QoI framework effectively describes the salient features of situations of interest[17].
- Group formation according to a high level of shared "context" propagates increased QoI provision, therefore allowing surveillance missions to perform their tasks effectively within uncertain environments. A higher group aggregated QoI value, indicates better urgency and utility for effective c^2 decision making.
- Maintaining group formation according to high level of shared "context" promotes better network management since:
    - Reduces the influence of QoI contributed by outliers in the network that would otherwise produce a lower overall aggregated QoI output. Outliers represent neighbouring sensors which are distant in terms of "context" when compared with the rest of the contributing group.

- Non-common "context" group members can therefore communicate less, until they become active in terms of "context", providing improved bandwidth efficiency and transmission energy consumption benefits.

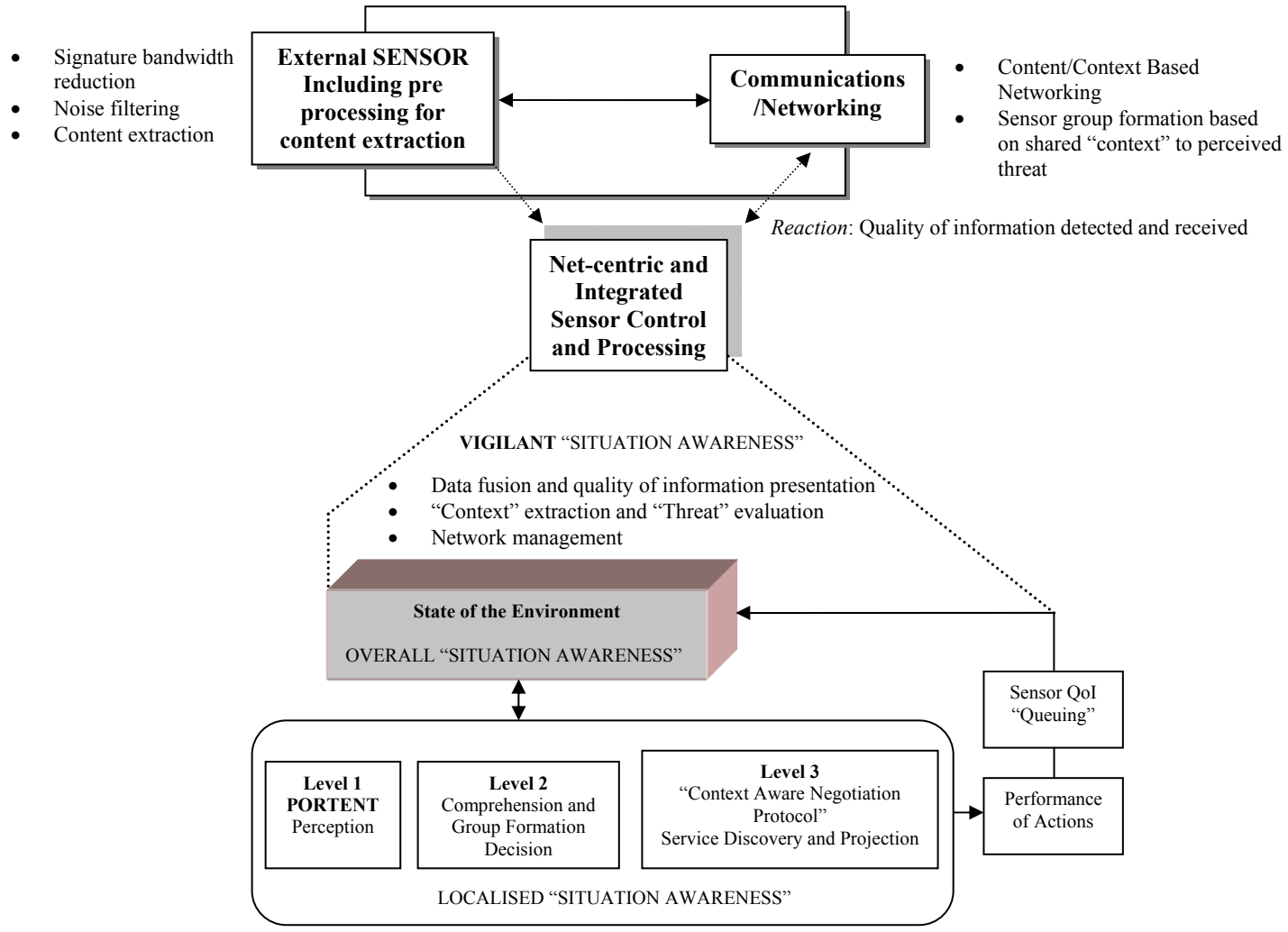


Figure 1. Overall combined VIGILANT "situation awareness" architecture derived from Endsley's "tripartite" model and inspired by "conceptual integration" with its functionality mapping to a real sensor system implementation

Sensors deployed in adverse unpredictable environments for surveillance purposes, have tendencies for elevated false-alarm rates due to the nature of operation and deployment. Providing a high level group "context" perspective can therefore help to minimise the likelihood in missing events of interest, increasing QoI robustness and preventing unnecessary or costly c^2 actions being undertaken.

2.1 VIGILANT Level 1 - PORTENT Perception

The focus of surveillance missions is to efficiently detect, acquire and verify information about potential threats and targets, within a specified region of interest. False alarm rates however have a distinct impact on surveillance performance and mission success especially, as it relates to target detection. Therefore enforcing a low false alarm rate to

avoid unnecessary response costs implies a larger data set (samples collected) and hence greater sampling energy consumption, by the deployed network. In mission critical scenarios a high degree of sensitivity is desired to capture all potential targets, especially where larger standoff ranges are desired. A sensing system that has self-adjustable sensitivity to accommodate different kinds of sensing environments and security requirements is therefore ideal.

2.1.1 PORTENT Operation

Our evaluated and presented predator aware situation assessment system[15], PORTENT, compromises VIGILANT level 1 perception. The PORTENT situation assessment system design emulates the mammalian amygdala threat detection response mechanism, as discussed in section 1.1.

As shown in figure 2, PORTENT comprises of a "fast" but less accurate decision making system, based on a single sensory event observation, representing broad situation assessment. The second is a "slow" but more accurate validation system of the perceived event that integrates sensory data over time, until an ideal threshold is met, representing extensive situation assessment. The threshold itself is designed to self-adapt and adjust optimally to the current uncertainty (false alarm) present in the sensed observation environment, thus minimizing on both false alarm detection and the need for full extensive sampling.

PORTENT represents the faster system using standard signal detection theory[16]. The slower more accurate extensive situation assessment system and response mechanism is framed in terms of the sequential probability ratio test (SPRT). The SPRT tests between two alternative hypotheses, updating the relative likelihood of each as new sensory data arrives, until deciding in favour of one of the hypotheses.

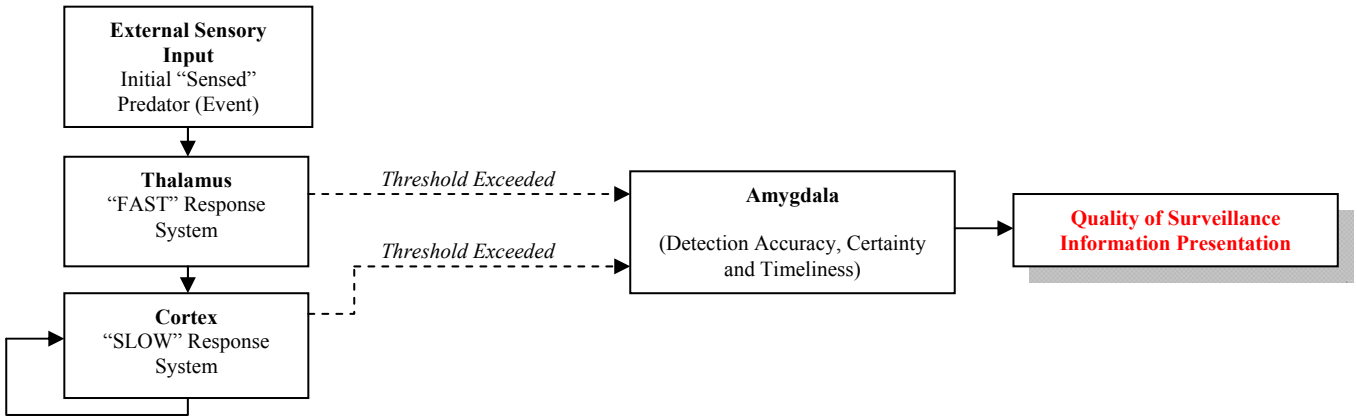


Figure 2. PORTENT situation assessment system architecture inspired by the mammalian amygdala recursive threat detection mechanism

The PORTENT system provides information relevancy within uncertainty, by implementing strategies for efficiently combining both "fast" and "slow" response systems, to provide increased detection accuracy, certainty and timely situation assessment performance[15]. The system promotes scalability in allowing distributed event detection and optimal sampling operation, without relying on the assistance of a base station or other means of central coordination.

Sensors deployed within a field of interest, represent the probability of a predator (event) being present P_R , prior to the initial sensed event, as a function of the maximum sensing range S_{RMAX} and the Euclidean distance to the sensed event $|d(s,p)|$, as shown in equation 1. We assume one possible predator being present, prior to the initial sensed event. Therefore the probability of there being no predator is (1- P_R).

$$P_R = \left(1 + e^{b_1\left(\frac{\left(\frac{S_{RMAX}}{2} - |d(s,p)|\right)}{\frac{S_{RMAX}}{2}}\right)}\right) * \frac{1}{1 + e^{b_1}} \quad \left(\text{if } 0 \geq |d(s,p)| \leq {}^{S_{RMAX}}/_{2}\right) \text{ and } b1 = \ln 3$$

$$P_R = \left(e^{-b2\left(\left(\frac{2*|d(s,p)|}{S_{RMAX}}\right)-1\right)} \right) * 0.5 \qquad \left(\text{if } {S_{RMAX}}/{2} > |d(s,p)| \leq S_{RMAX}\right) \text{and } b2 = 3.91 \tag{1}$$

From the results of our evaluation studies[15], we use PORTENT option 2 in our VIGILANT design, for increased QoI provision. PORTENT specifically uses detection accuracy, certainty, timeliness quality factors and a linear weighted fusion strategy by assigning normalized weights (W_b), to calculate localised QoI surveillance captured[17], shown in equation 2.

$$QoI_{Surveillance} = \sum_{b=1}^{k} W_b * q_b \tag{2}$$

2.2 VIGILANT Level 2 - Comprehension and Group Formation Decision

In the case of surveillance applications, searching and comprehending the environment for potential intruders can be argued as the most critical part of the mission requirement, since this reduces the chance of relevant events remaining undetected. VIGILANT, level 2 involves the comprehending the significance associated with the sensor data occurring within a fragmented and uncertain environment.

Real situations that occur in a real uncertain environment require the need for a mental representation, to derive "context" (meaning) of those situations. This is facilitated with a vital relation sketch that promotes a concise structure, representing the view of the current perceived situation. In general there exist two approaches to the modelling of situations within environments of interest[18]:

- *State orientated* approaches look on situations as aggregated state entities of the world.
- *Action orientated* approaches consider situations as sequences of actions and viewpoints originating from some declared initial world state.

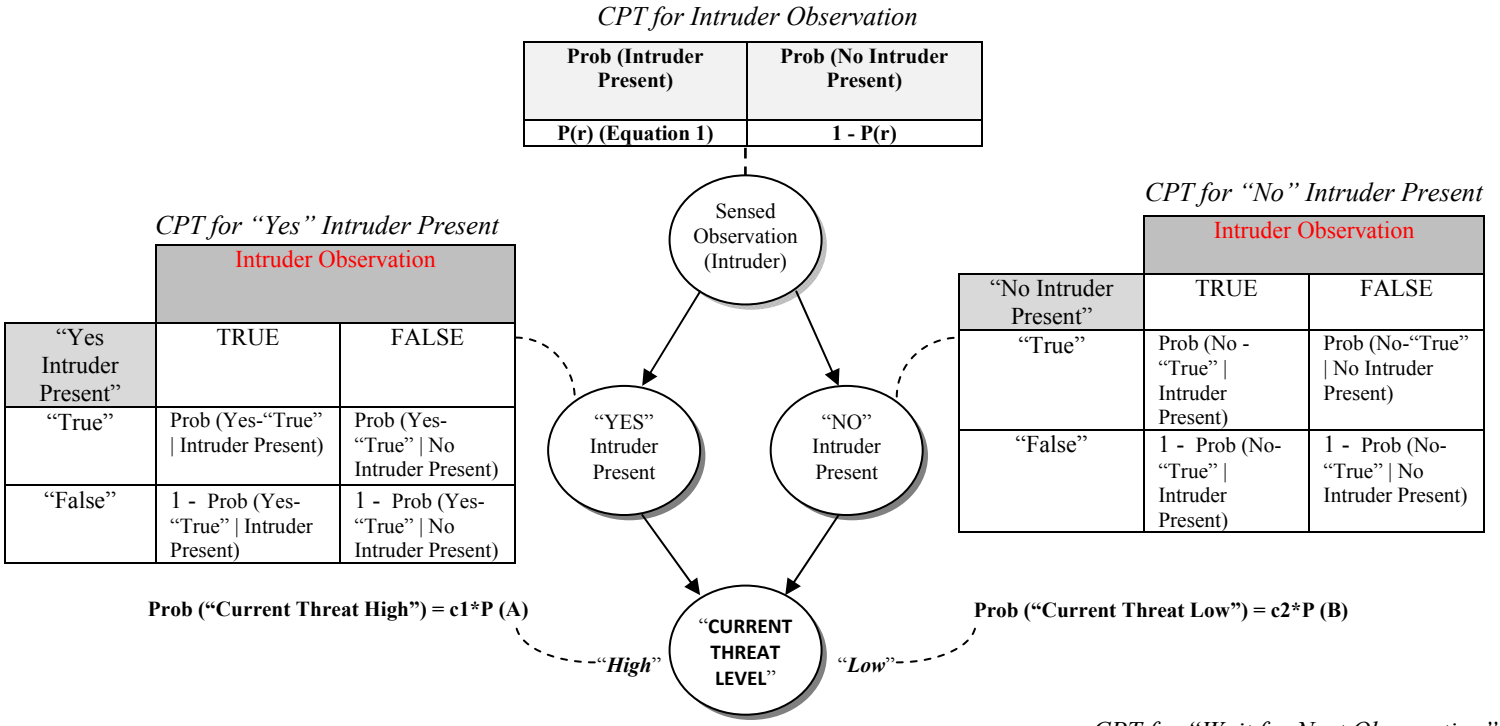
For this purpose we utilise an action orientated design approach, in the form of a Bayesian belief network (BBN). BBN techniques have proved very useful and effective in a variety of decision aiding domains, especially in dealing with issues concerning inference, within an uncertain environment[19]. Practical advantages offered by BBN techniques include:

- Valuable in any area where there is the requirement for finding out about unknown variables through the utilisation of formal structural relationships and data.
- If exact forms of the relationships between the variables of interest are not known it does not matter, because the uncertainty can be represented probabilistically, through Bayes theorem.
- BBNs can be used to help identify key factors that most influence some outcome of interest, to help prioritize the decision making process.

A BBN is a graphical, probabilistic knowledge representation, of a collection of variables describing a "situation" domain. Nodes of the belief network denote the variables representing concepts. The corresponding links define the casual relationships between them. The overall topology of the network encodes the qualitative knowledge about the situation. Conditional probability tables (CPTs) encode the quantitative details (strengths and influence) of the casual relationships. Figure 3 details the VIGILANT BBN, with corresponding CPTs and decision rule for "situation aware" group formation.

The belief network of figure 3, encodes the relationship over a simple "situation" domain modelling threat surveillance comprehension, consisting of six binary variables. *Sensed observation*, *"yes" intruder present*, *"no" intruder present*, *"current threat level"*, *"form situation awareness group"* and "*wait for next observation*". The belief network topology captures the common sense knowledge that:

1. Sensed observation influences *"yes" intruder present*.
2. Sensed observation influences *"no" intruder present*.
3. Both *"yes and no" intruder presence* have direct casual effects on the level of understanding concerning the current threat level.
4. The *"current threat level"* influences the decision to *form situation awareness group*.
5. The *"current threat level"* influences the decision to *wait for next observation*.



Decision: "Initiate Service Discovery"
IF Prob ("Yes Form Situation Awareness Group") >= Prob ("Yes Wait for Next Observation")

Figure 3. VIGILANT level 2 localised "situation aware" BBN

As shown in figure 3, the CPT specifies the probability of each possible child variable value conditioned on each possible combination of parent values. Table 1 details the probability expressions derived from our VIGILANT level 2 BBN, based on the CPT's, to facilitate "context" (meaning) of those situations and aid final decision making for initiating group formation.

Probability Expression	Probability Derivation from VIGILANT BBN using CPT Analysis
1. $Prob(Yes\ Intruder\ Present - True)$	P(A) = Prob (True – Yes Intruder Present | Intruder Present True) * P(r) + Prob(True – Yes Intruder Present | Intruder Present False)* (1 – P(r))
2. $Prob(No\ Intruder\ Present - True)$	P(B) = Prob (True – No Intruder Present | Intruder Present True) * P(r) + Prob(True – No Intruder Present | Intruder Present False)* (1 – P(r))
3. $Prob(Current\ Threat\ Level - High)$	C1 * P(A) (C1 = 1 – ($\|d(s,p)\| / S_{RMAX}$))
4. $Prob(Current\ Threat\ Level - Low)$	C2 * P(B) (C2 = 1 – C1)
5. $Prob(Form\ Situation\ Awareness\ Group)$	Prob (Yes-"Form"|Current Threat High)* Prob (Current Threat High) + Prob (Yes-"Form"| Current Threat Low)*Prob (Current Threat Low)
6. $Prob(Wait\ for\ Next\ Observation)$	Prob (Yes-"Wait"|Current Threat High)* Prob (Current Threat High) + Prob (Yes-"Wait"| Current Threat Low)*Prob (Current Threat Low)

Table 1. Probability derivations from VIGILANT BBN for the purposes of "Situation" decision making

2.3 VIGILANT Level 3 - Quality of Information Surveillance Network Management

VIGILANT level 3 is driven by the group initiator, representing the sensor which perceives the highest current threat, established in level 2. Initiation of a "context aware" service discovery is primarily for the need to collect additional information concerning the present situation. This involves utilising the deployed distributed sensor network, by grouping single hop sensors that share common "context" about the pervading situation, in order to further satisfy the mission objective in providing high QoI surveillance (Overall "situation awareness").

A special challenge in using context information for clustering is dealing with the procedure for providing accuracy in both the degree of confidence and the evaluated shared level in context. The confidence value in evaluated context between two nodes can vary in time, which may cause undesirable fluctuations of the clustering structure. The VIGILANT grouping algorithm therefore needs to be designed with regard to the following requirements:

- ***Dynamics:*** Groups must provide adaptability, depending on changes to the pervading situation "context", allowing nodes to leave and join at any time.
- ***Stability:*** In order to provide an accurate basis for QoI surveillance processing, the group structure has to provide a level of stability, in cases where there are no contextual changes. For this purpose the decision to enter and provide QoI surveillance updates is based on the level in sharing a common "context".
- ***Group Initiator re-election:*** A leader, for QoI surveillance aggregation is dynamically re-elected in the process of a mission, to facilitate maintaining QoI and geo-location accuracy while minimising on communication overhead required for group re-setup phase.
- ***System energy-efficiency:*** Sensor nodes are typically restricted in their energy resources, therefore non – essential communication and overhead should be kept to a minimum to prolong network lifetime.

Bearing these requirements in mind, VIGILANT level 3 is broken into two parts. Part A focusing on "context aware" service discovery. Part B, once shared "context" has been established, involves calculation of a QoI surveillance service provision time bound, for "situation aware" partnership stability between matched sensors.

2.3.1 VIGILANT Level 3- Part A

Part A involves establishing which sensors in the neighbourhood can provide the same level of confidence in "context", using the certainty factor model[20]. Certainty factor (CF) provides a framework to evaluate and measure the confidence between two random entities ("Context" in present threat). CF operates according to proportional measures of increased

belief (MB) and disbelief (MD) about a certain hypothesis. For VIGILANT, the hypothesis stems from the degree of certainty in MB and MD that an individual sensor should join to form a partnership, according to its current situation "context", as shown in equation 5.

$$MB = \frac{Prob(\text{Yes Form Situation Awareness Group} | \text{Current threat level "High"}) - Prob(\text{Current threat level "High"})}{1 - Prob(\text{Current threat level "High"})} \quad (3)$$

$$MD = \frac{Prob(\text{Current threat level "High"}) - Prob(\text{Yes Form Situation Awareness Group} | \text{Current threat level "High"})}{Prob(\text{Current threat level "High"})} \quad (4)$$

$$CF\ \text{"Sensor"} = {}^{(MB - MD)}\Big/_{1 - \min(MB, MD)} \quad (5)$$

Upon receiving a REQUEST broadcast notification, from the group initiator, sensors within the single hop neighbourhood reply with their corresponding *CF "Sensor"* values. Group initiators then seek to evaluate the current level of shared confidence in "context" by combining their own *CF "Group Initiator"*, calculated in the same form as equation 5, with *CF "Sensor"* on a per sensor basis, by utilising the "**confidence evaluation in context**" rule, shown in equation 6. The combined CF evaluation seeks to measure the degree of confidence that both sensors should form a partnership, due to their respective current perceived situation "context".

"Confidence evaluation in context" $rule:$ (6)

$$IF\ CF\ \text{"}Group\ Initiator\text{"}, Current\ Threat\ Level\ \ AND\ \ CF\ \text{"}Sensor\text{"}, Current\ Threat\ Level$$

$$THEN\ \ Confidence\ in\ Current\ Threat\ Level, CF\ \text{"}Situation\ Context\text{"}$$

$$CF\ \text{"Situation Context"} = \begin{cases} If\ \ CF\ \text{"Group Initiator" and CF "Sensor"} \geq 0: & CF\ \text{"Group Initiator"} + CF\ \text{"Sensor"}(1 - CF\ \text{"Group Initiator"}) \\ If\ \ CF\ \text{"Group Initiator" and CF "Sensor"} < 0: & CF\ \text{"Group Initiator"} + CF\ \text{"Sensor"}(1 + CF\ \text{"Group Initiator"}) \\ \text{Otherwise}: & \frac{(CF\ \text{"Group Initiator"} + CF\ \text{"Sensor"})}{1 - \min(|CF\ \text{"Group Initiator"}|, |CF\ \text{"Sensor"}|)} \end{cases}$$

Establishing "active" sensor members in terms of "context" provides efficient network management, by minimising on outlier member contribution, which allows a higher quality of surveillance information relevancy to be achieved. Figure 4, illustrates the overall VIGILANT level 3 part A operation.

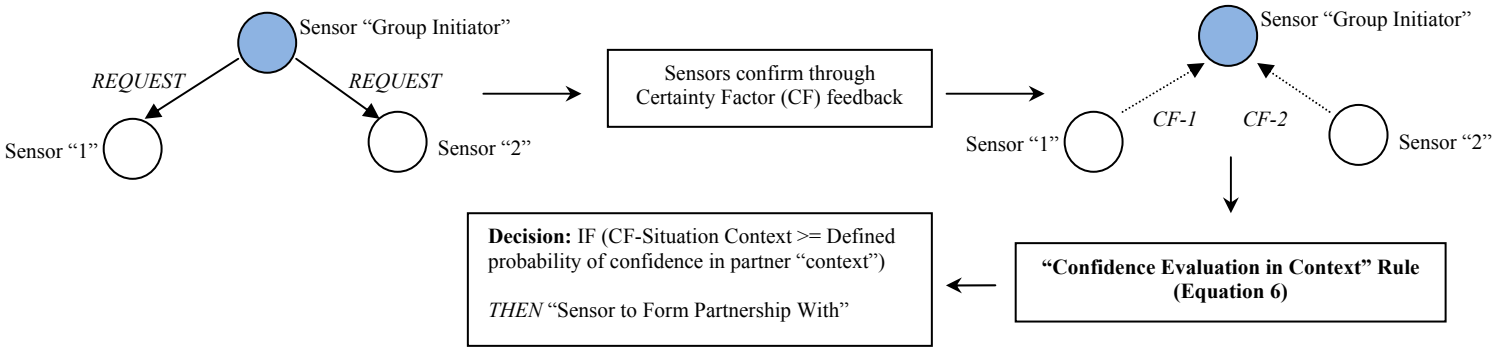


Figure 4. VIGILANT level 3 part A group initiator "context aware" service discovery with corresponding partnership decision

2.3.2 VIGILANT Level 3- Part B

Part B determines a lower QoI service provision time bound that VIGILANT can provide, based on a shared level of common "context" within the interest group, once matched partnership sensors have been identified. The service provision time placed is dependent and varies on a per partner basis, due to the changes in different degrees of shared "context" present. A shorter service provision time implies the risk of sharing same level "context" will change frequently (high uncertainty present), hence the need for communicating more often to maintain the mission objective, in providing accurate levels of QoI and vice versa for longer provision times. The advantage of a service provision time according to a shared level of common "context" serves as a network management mechanism in two ways:

- Allowing "active" group sensor members to communicate at defined bounded time slot periods.
- Defined periods minimises on congestion, collision and latency issues (bandwidth efficiency) for partner QoI reporting, when utilising a random medium access control scheme, within the interest group.

2.3.2.1 Determination of Common Shared "Context" – Partnership Stability

In order to provide an accurate basis for QoI surveillance aggregation, the group structure has to provide a measure in level of stability, for cases where there are no contextual changes. We model the joint probability confidence in shared low threat "context" between the group initiator and its corresponding partner as a random variable, U, with probability density function (PDF_1) and cumulative distribution function (CDF_1), $U \sim N(\mu_{\text{common low threat "context"}}, \sigma^2_{\text{common low threat "context"}})$. Additionally the joint probability confidence in shared high threat "context" as a random variable, T, with a PDF_2 and CDF_2 , $T \sim N(\mu_{\text{common high threat "context"}}, \sigma^2_{\text{common high threat "context"}})$.

The group initiator determines the probability in partnership stability, by determining the level of common shared "context", based on a threshold $\boldsymbol{S}$, chosen as the intersection point of the two respective PDF's. The intersection point is chosen as to minimise the sum of probabilities of an incorrect determination in common "context" being made.

We denote P_1 as the probability of correct detection of non-common high threat "context" and Q_1 as the probability in correct detection of common low threat "context", as shown in equations 7 and 8. Equation 9 shows the probability of partnership stability in the form of a ratio measure indication. Clearly probabilities P_1 and Q_1 should be as low as possible; in order to represent the view in shared confidence that a partnership has a high level of awareness to the current situation "context". The degree of confidence in partnership stability will of course vary accordingly to the characteristics of the underlying joint probability distributions, PDF_1 and PDF_2, which are dictated by the present changing situation and level of uncertainty within the sensing environment.

$$P_1 = Prob(Correct\ detection\ of\ non\ common\ high\ \text{context} \mid Share\ common\ high\ threat\ "context") = CDF_2(S) \tag{7}$$

$$Q_1 = Prob(Correct\ detection\ of common\ low\ \text{context} \mid Share\ common\ low\ threat\ "context") = CDF_1(S) \tag{8}$$

$$Partnership\ Stability = {}^{P_1}/_{Q_1} \tag{9}$$

2.3.2.2 QoI Surveillance Service Provision Time Bound

In order to ensure timely and reliable delivery of QoI surveillance updates (minimal latency and collision) and promote sensor network operational longevity, the group initiator determines a service provision lower time bound limit, based on the current level of partnership stability. The service provision time bound (M) is evaluated in terms that a partnership shares a common stability for a minimum time history H_{min} out of a total H time steps, given as the CDF of a binomial distribution shown in equation 10. Figure 5, illustrates the overall VIGILANT level 3 part B operation.

$$M \sim Binomial(H, Partnership\ Stability)$$

$$Prob(Partnership\ Stability \leq H_{min}) = \sum_{k=H_{min}}^{H} \binom{H}{k} Partnership\ Stability^k\ (1 - Partnership\ Stability)^{H-k}$$

$$Expected\ QoI\ Service\ Provision\ Time = E(M) = Partnership\ Stability * H \tag{10}$$

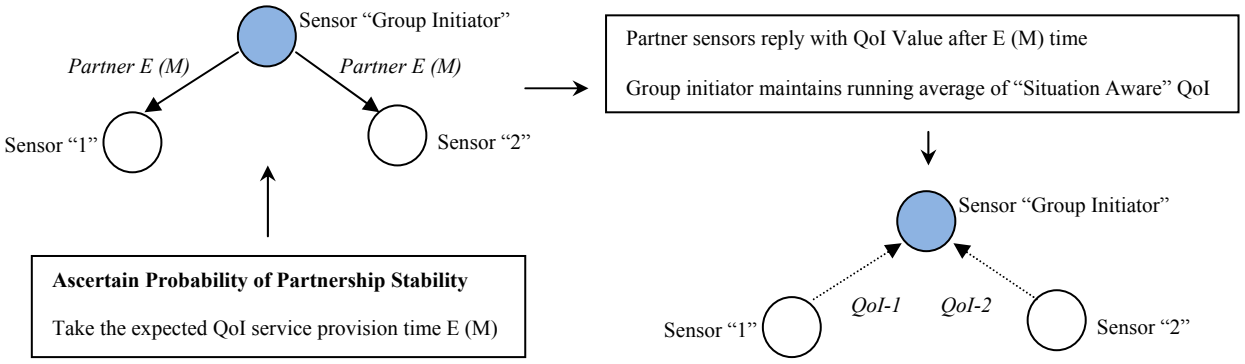


Figure 5. VIGILANT level 3 part B "context aware" partnership stability for QoI surveillance service provision

2.3.3 VIGILANT Group Initiator Re-Election

To facilitate maintaining relevant QoI surveillance aggregation and minimising on communication overhead, commonly required in group re-setup phases, group initiator re-election is dynamically conducted in the process of a mission. VIGILANT group initiators rely on the QoI surveillance updates from sensor partners to re-evaluate their current group status, using a relative QoI ratio metric, shown in equation 11.

$$QoI_{Relative\ Ratio} = \frac{QoI_{Group\ Initiator}}{QoI_{Partner\ Sensor}} \tag{11}$$

Group initiators invoke the process of passing on group initiator status, to a partner sensor if the $QoI_{Relative\ Ratio} \leq 1$. Notification of new group initiator status is broadcast to the identified partner sensor, as shown in figure 6, which then re-initialises the group as detailed in section 2.3.1 and 2.3.2.

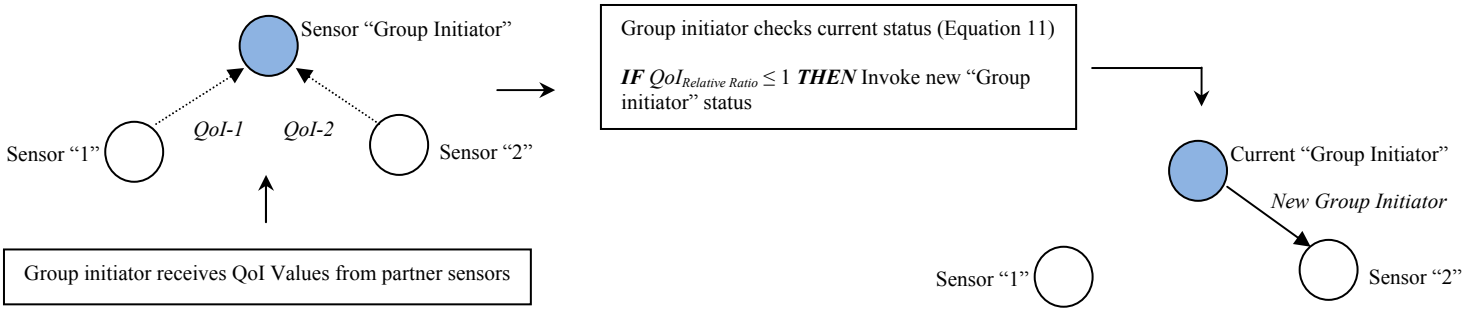


Figure 6. VIGILANT group initiator re-election operation

Group initiator operations' describing the combined overall VIGILANT situation awareness system is shown in figure 7. Figure 7 outlines the VIGILANT concept, based around the clustering of sensor nodes into groups that share common "context", where this context is expressed in terms of the level and presence of a threat (situation). This supports the primary mission objective for higher QoI surveillance (aggregated detection certainty, accuracy and timeliness) provision, about the presence of a threat.

For more complex mission objectives (e.g. optimal geo-location threat estimate, estimated track of threat migration), transferring level 3 operation from "group initiator" onto the network sensor side is required, to support these mission specific "contexts". This will aid sensors to self-schedule themselves accordingly to "context", in order to better quantify the utility for specific information provision requests, as required by the command and control function. Transferring scheduling for surveillance provision (e.g. QoI, geo-location estimate) also prevents centralised control as currently with VIGILANT. This can further improve on network performance, such as reducing communication overhead and promoting true self-autonomous operation, important within disruptive communication environments.

3. RELATED WORK

In hierarchical approaches, sensors are grouped into a number of clusters, each of which has a local point of access, the cluster head (CH). Member sensor nodes send sensed information to the CH for aggregation purposes, which then forward aggregated information onwards to a central control station. Clustering in ad-hoc and sensor networks is an effective technique for achieving scalability and prolonged network lifetime[7, 8, 9]. Typically parameters such as node degree, transmission power, battery energy level and network connectivity, serve as metrics for choosing the optimal clustering structure.

The Low Energy Adaptive Clustering Hierarchy (LEACH) mechanism[7] is a distributed single hop algorithm for sensor networks in which the sensors elect themselves as CHs with some probability and broadcast their decisions. LEACH has inherent characteristics such as, self configuration, localised control of data transmission using Time Division Multiple Access (TDMA) and data aggregation capability. One of the drawbacks of LEACH is in applying probabilistic values to select CHs, which may result in a selection of CHs from a smaller geographic region.

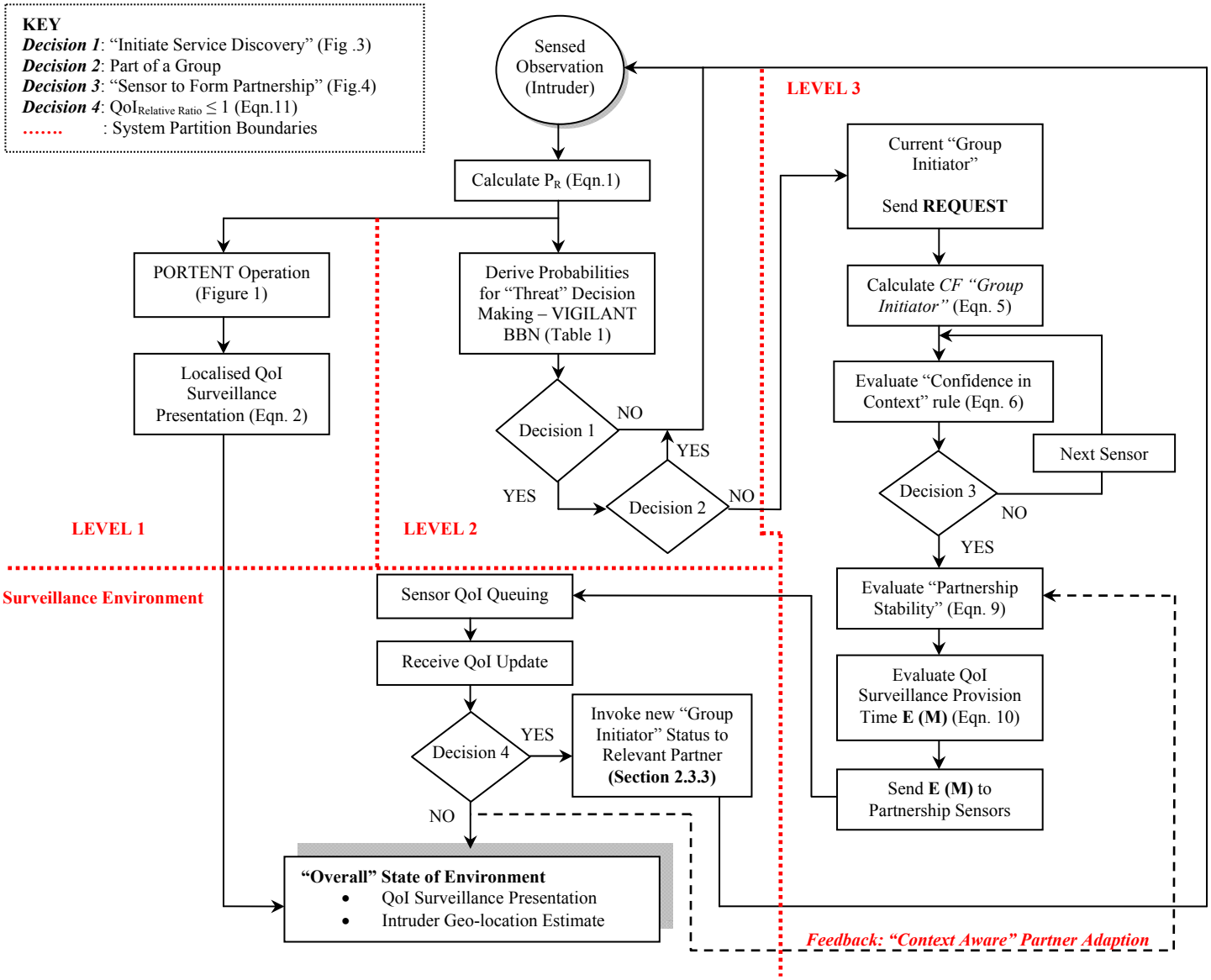


Figure 7. VIGILANT group initiator situation awareness operation flow chart, showing an integrated level 1, 2, 3 process for surveillance updating. Feedback from the surveillance environment during an ongoing mission is used to make "context aware" adaption decisions in terms of re-evaluating "partnership stability" to provide further relevant QoI service provision times

In a surveillance operation, self-organisation to form groups that can perform energy efficient target geo-localisation and provide tracking information is important[10, 11]. Dynamic clustering for acoustic target tracking in wireless sensor networks[10], proposes a simple physical based localisation view, based on estimated distances derived from received signal energy levels, from the sensing field. The locus of a potential target is dependent on the level of shared signal energy between two sensors, characterised by a defined signal threshold. CHs are elected accordingly to the sensor with the greatest received energy and are rotated when a change in energy levels is detected accordingly, in the neighbourhood. This can lead to certain inaccuracies arising, especially if the sensing environment is effected by high levels of noise, leading to greater uncertainties, group instability and degradation in performance.

The above mentioned schemes also introduce considerable latency involved in the set up of the clusters and overhead messages in the schemes due to random rotation of the CHs. Most of the schemes do not take into account the message losses due to collisions and congestion at the sensor nodes.

Until recently recent initiatives have begun to address the problem of grouping based on "context" attributes of the sensing environment, to provide application specific services, for improved network management performance[12, 13]. Grouping according to "context" offers an obvious advantage in extended relevant sensing coverage over isolated nodes, important in situation awareness and surveillance applications.

Our VIGILANT approach is different, in that we utilise a situation aware approach to group formation, taking active and adaptive decisions which are relevant to the current "context" within the surveillance environment, rather than physical or sensor device centric means. Using VIGILANT, we seek to highlight within a surveillance mission setting, the advantages offered in networking according to "context" of the sensing environment.

4. VIGILANT SYSTEM PERFORMANCE

VIGILANT performance is determined through the OMNeT++ simulation platform[21]. We utilise a fixed known 20 node static *acoustic* and *seismic* sensor network deployed deterministically to a grid coordinate system, in a 1km by 1km region of interest. An equal number of acoustic and seismic sensors are used with maximum sensing ranges (S_{RMAX}) for seismic type sensors set to 250 meters and 1000 meters for acoustic types. We assume that higher level application algorithms are present on each sensor for target intruder classification purposes. All simulations are based on a single full sampling rate of 100 samples/second. Sensor transmission range is set to 500 metres and the IEEE802.11 protocol, based on the distributed coordination function (DCF), in basic access mode, is utilised for medium access control.

Surveillance for intruder monitoring is based on a mobile target moving at a constant velocity of 5m/s, within the region of interest in a diagonal direction. We assume a command centre has just received intelligence that an intruder will be approaching the region in the near future and subsequently activates sensing operation, within the specified region of interest[22].

4.1 VIGILANT Performance - Surveillance Network Management

A special challenge in using context information for group formation and management is dealing with the procedure for providing accuracy in both the degree of confidence and the evaluated level, of context being shared. VIGILANT network management is provided through:

- Establishing which sensors in the neighbourhood can provide the same level of confidence in "context", using the certainty factor model. The number of sensors included in the group is set by a lower defined bound, probability of confidence in partner "context", as shown in figure 4. The higher the bound set inherently provides efficient network management, by further minimising on outlier contribution, to satisfy mission objectives in higher QoI surveillance provision.
- VIGILANT promotes efficient network management by employing a QoI surveillance service provision time. Service provision time is based on the level of common shared "context" and the maximum set time allocated (H), calculated in equation 10, within the interest group on a per partner basis.

4.1.1 Geo-Location Accuracy

VIGILANT primary operation is based on networking nodes into groups that share common "context" in order to provide improved QoI surveillance about the threat. Geo-location accuracy could therefore potentially be affected by not

utilising all available nodes (non-common "context" nodes) within a neighbourhood communication range cluster. VIGILANT is compared with LEACH[7] using our designed PORTENT mechanism for initial CH election purposes and a physical received sensing energy approach[10], as discussed in section 3. LEACH acts as our benchmark since the protocol utilises all available nodes for grouping. This will aid comparison to establish the trade off in geo-location accuracy incurred when compared with VIGILANT, which networks according to only common "context".

Geo-location accuracy is measured in terms of the circular error probable (CEP) metric. E (CEP) provides a measure of the search area within which the true target location can be expected to be found, with a lower value indicating better geo-location accuracy. E (CEP -50%) is the radius of a circle about the (x, y) estimate which has an expected 50% probability of containing the target. Performance for intruder geo-location is undertaken for a single track of the mobile target (mission), using time difference of arrival (TDOA), on every QoI update received from partner sensors. Figure 8, shows VIGILANT geo-location performance during a mission cycle.

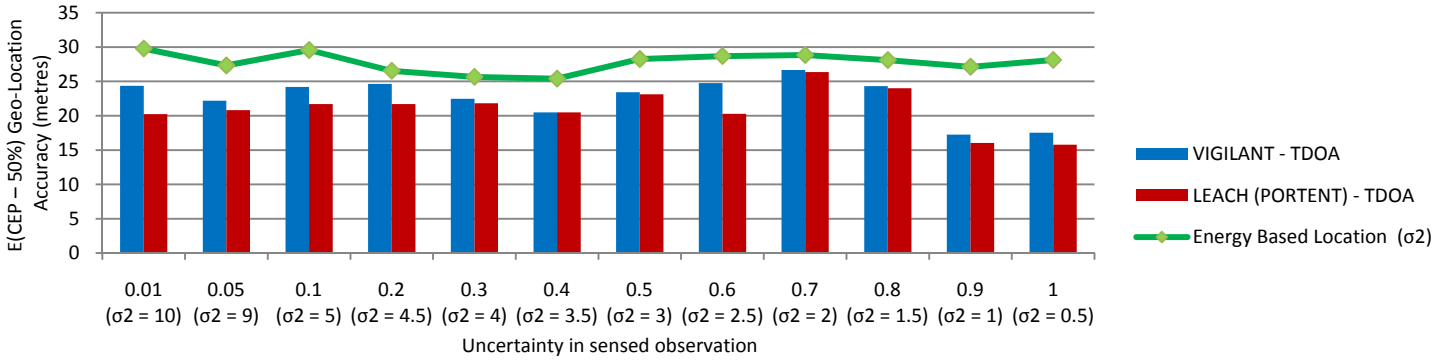


Figure 8. VIGILANT geo-location accuracy as uncertainty in observation (level 1) measured as the degree of overlap in predator, no predator probability distributions, partner confidence in "context" = 0.9 . Energy based location uncertainty is varied according to the noise present ~ N (0, σ^2) in the sensing environment.

4.1.2 Minimising on Outlier Contribution

VIGILANT inherently reduces the influence of QoI contributed by outliers in the network that would otherwise produce a lower overall aggregated QoI surveillance output. Outliers represent neighbouring sensors which are distant in terms of "context" when compared with the rest of the contributing group. The degree of outlier contribution is dictated by the set probability of confidence in partner "context" and uncertainty present in the sensing environment, as shown in figure 9.

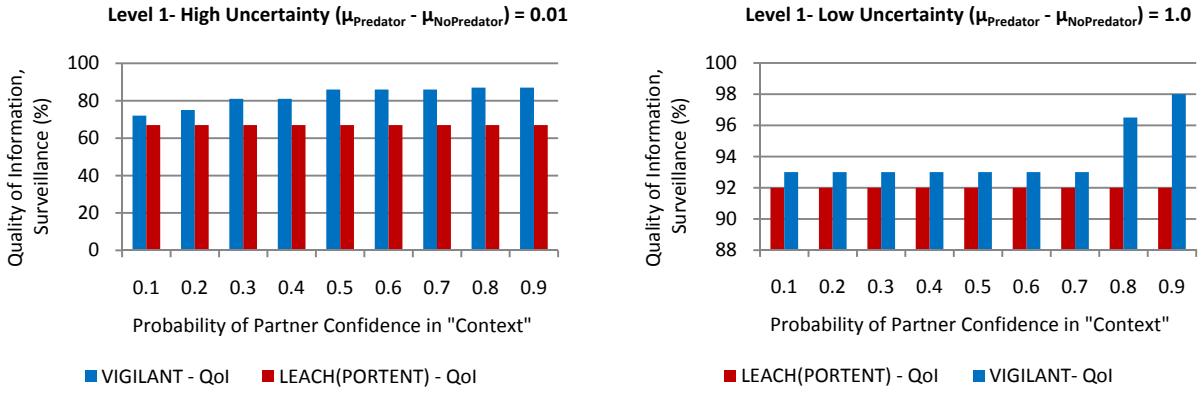


Figure 9. Setting a higher probability of partner confidence in "context" minimises on outlier contribution for improved QoI surveillance performance in both low and high uncertainty conditions

Setting a high probability of confidence in partner "context", however leads to a trade-off being incurred against geo-location accuracy and QoI surveillance provision, as shown in figure 10.

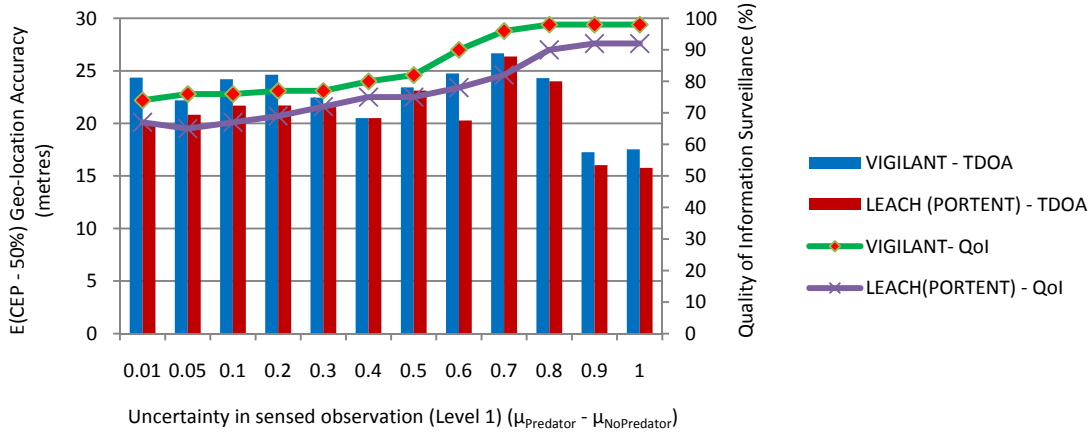
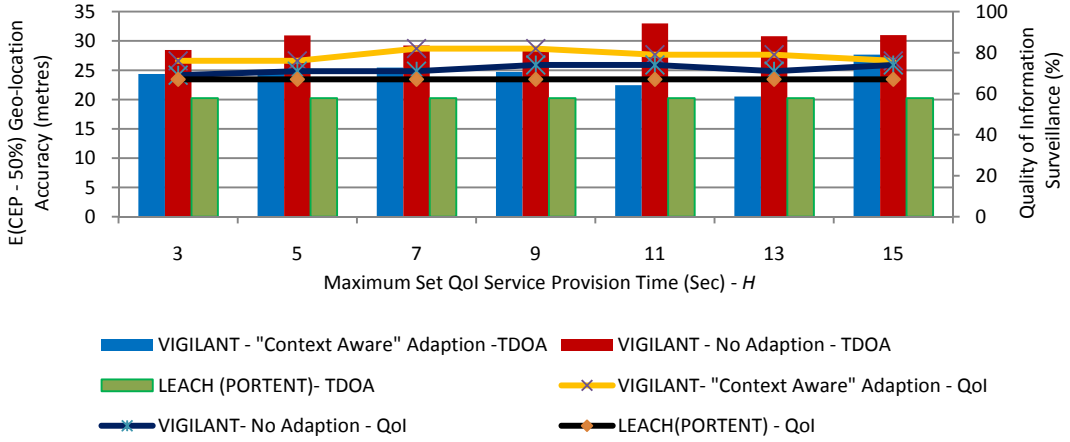


Figure 10. VIGILANT reduces the influence contributed by outliers in the network for improved mission objective QoI surveillance performance, probability of confidence in partner "context" = 0.9, *H* = 5 Sec. With the reduction in group outliers a trade-off however is incurred in terms of geo-location accuracy

4.1.3 "Context Aware" Partner QoI Service Provision Time Adaption

As shown in figure 7, VIGILANT uses feedback from the surveillance environment, on a per QoI update to make "context aware" adaption decisions to cater for changes in situation "context". Adaption is made in terms of re-evaluating "partnership stability" to provide relevant QoI service provision times, thus maintaining an accurate overall state of the surveillance environment. As shown in figure 11, group formation according to a high level of confidence in shared "context" with "context aware" adaption propagates increased QoI provision, allowing surveillance missions to perform their tasks effectively, within uncertain sensing environments.

(a)



(b)

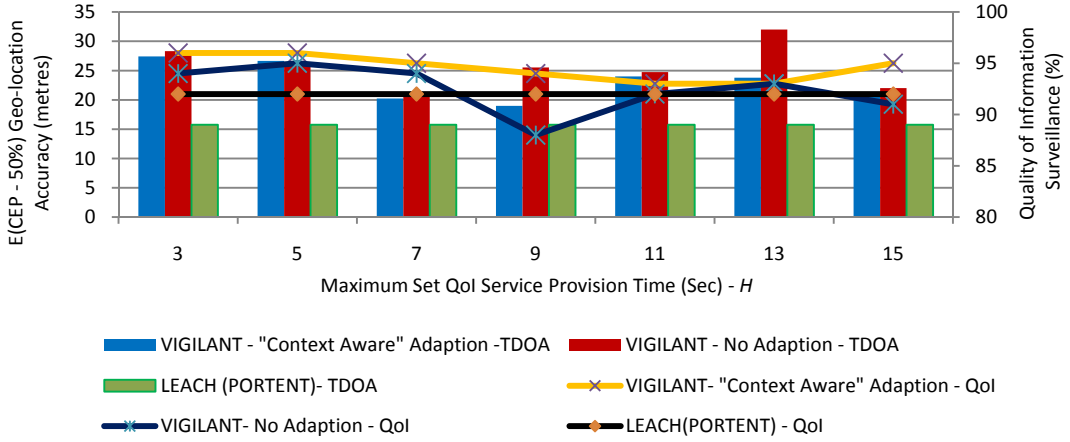


Figure 11. VIGILANT "Context Aware" Adaption (a) High Uncertainty ($\mu_{Predator} - \mu_{NoPredator}$) = 0.01 (b) Low Uncertainty ($\mu_{Predator} - \mu_{NoPredator}$) = 1.0, probability of confidence in partner "context" = 0.9. Adaption allows improved QoI surveillance and geo-location estimate performance therefore providing an accurate relevant state of the surveillance environment

4.1.4 Latency and Communication Energy Performance

VIGILANT provides partnership sensors unique defined time slot periods, for mission QoI transmission reliability, to mitigate on collisions occurring within the neighbourhood and improve on latency (bandwidth efficiency).

Latency performance is dependent on the probability of confidence in partner "context" set, which determines the intended breadth of the group size structure, according to the desired level of confidence in "context" required within the group. Figure 12, shows VIGILANT latency performance, during a mission cycle, for QoI surveillance updating.

QoI surveillance service time provisioning inherently has the advantage, in allowing sensors that are "active" in partnership to only communicate at defined bounded time slot periods, utilising communication when required and promoting energy –efficient operation. Non-active partner members can also communicate less, until they become active in terms of "context" providing further transmission energy consumption and latency benefits, as shown in figures 13 and 14.

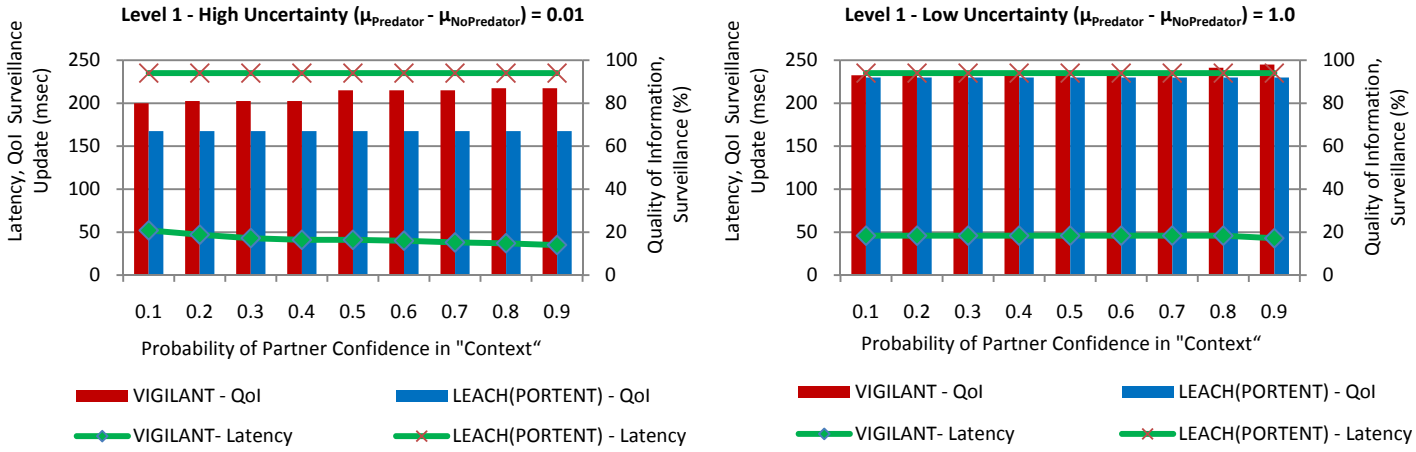


Figure 12. VIGILANT Latency performance, with *H = 5 sec*. Setting a probability of confidence in partner "context" improves on latency without degradation in QoI surveillance performance

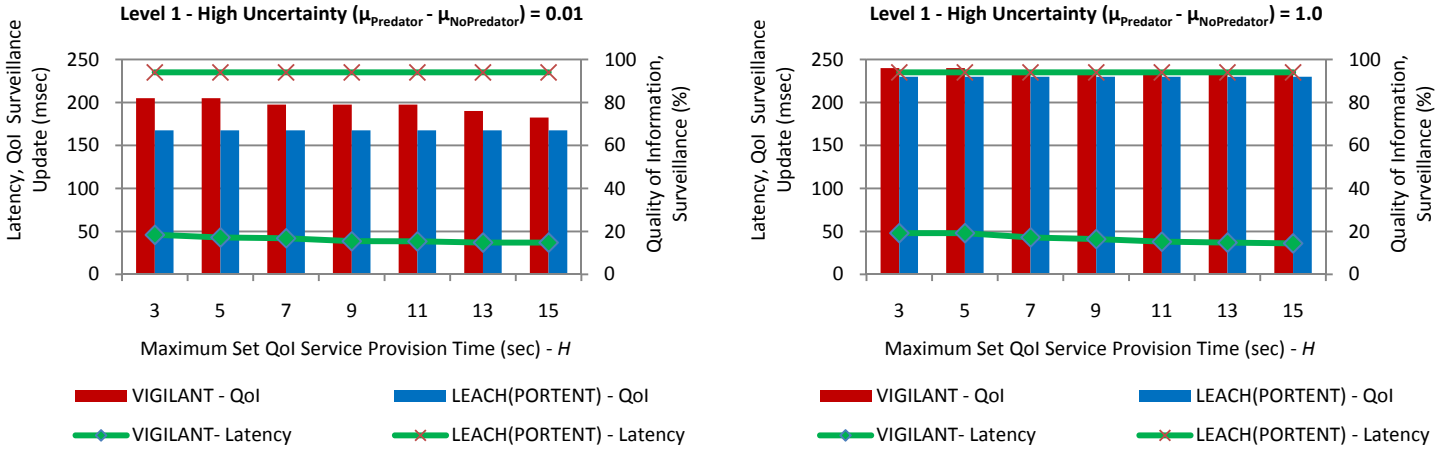


Figure 13. VIGILANT latency performance, with probability of confidence in partner "context" = 0.9. Increasing *H* reduces the level of QoI surveillance contribution but improves on latency

The same energy consumption model is used as in[7]. Frequency in communication for QoI surveillance updating, is only dependent on the level of shared common "context" present, which is influenced by both the uncertainty present in the

sensing environment and *H*, from equation 10. Figure 14 shows VIGILANT communication resource management performance, during a mission cycle for QoI surveillance updating.

Providing an increasing maximum set QoI service provision time can improve on energy consumption by reducing the frequency in communication for QoI surveillance updating, but this has an effect on geo-location accuracy performance as shown in figure 15.

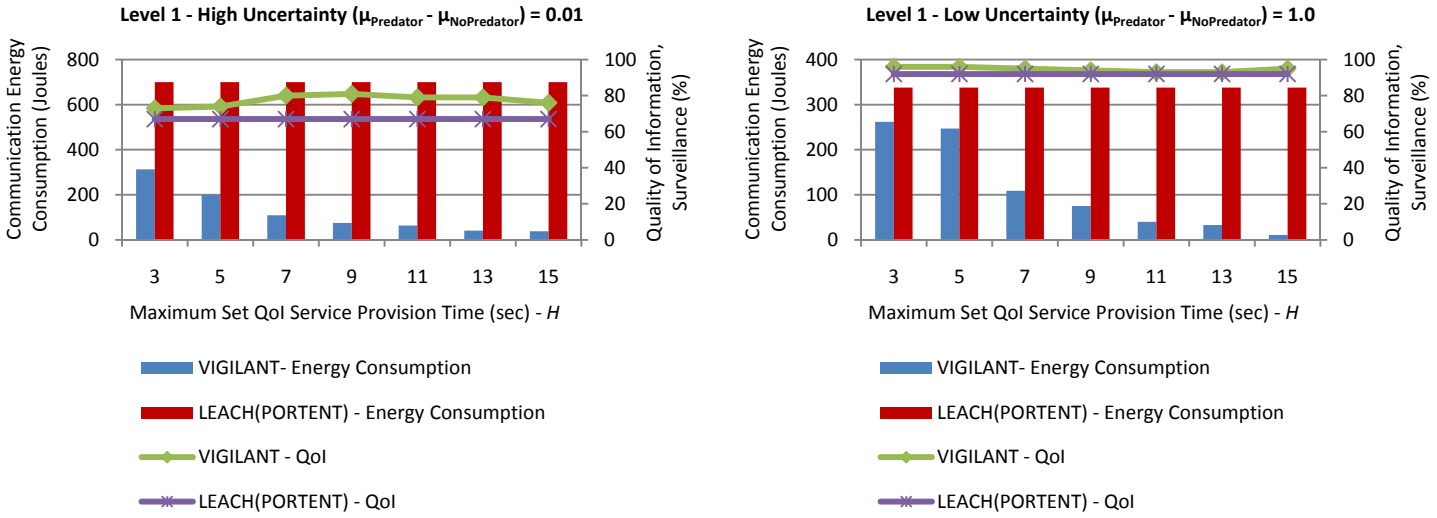


Figure 14. VIGILANT communication energy consumption performance, with probability of partner confidence in "context" = 0.9. The effect of providing a QoI service provision time matched to the level of shared "context" improves on energy consumption, without degradation in QoI surveillance performance

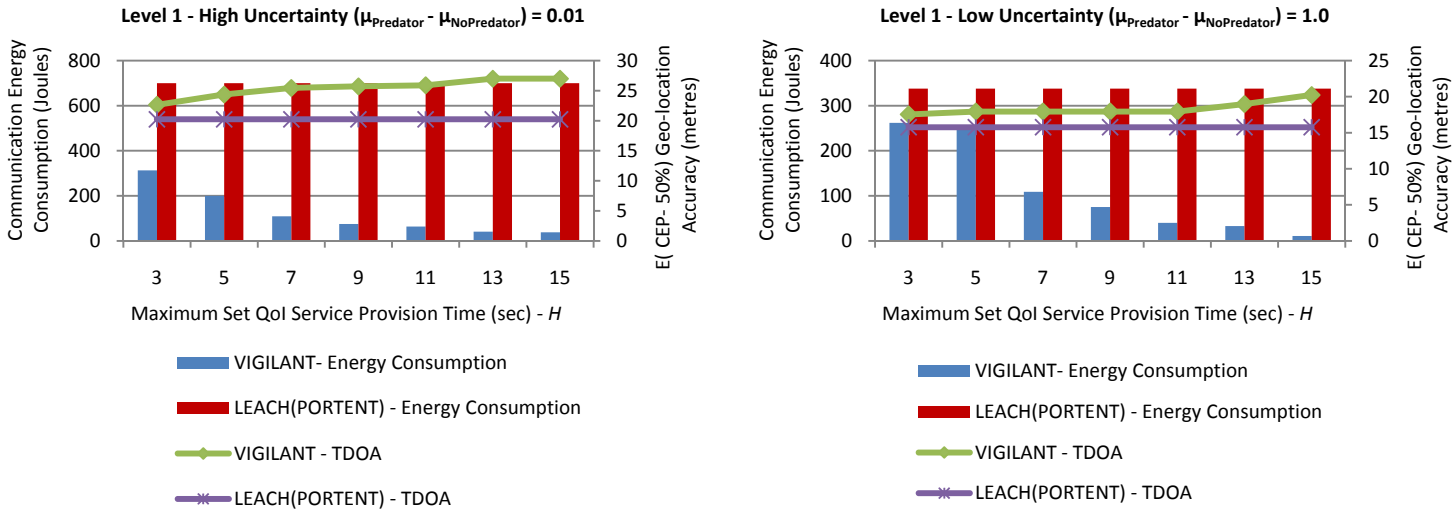


Figure 15. VIGILANT geo-location, energy consumption trade off performance, with probability of partner confidence in "context" = 0.9. Increasing maximum set QoI service provision time improves on energy consumption but since the frequency in QoI surveillance updating decreases this introduces a loss in geo-location accuracy especially in high uncertainty conditions

5. CONCLUSIONS

The focus of surveillance missions is to efficiently detect, verify and acquire information about the capabilities or position of targets, within a specified region of interest. For efficient operation of wireless sensor network surveillance applications, providing a relevant mission specific sensing coverage to a security-sensitive area, while minimising on both energy consumption and outlier contribution of deployed sensor nodes, is important. This helps to promote operational effectiveness, both on operational network longevity and quality of information (QoI) for c^2 decision support making. An effective approach for obeying this requirement is grouping sensors according to common shared situation "context". This offers obvious advantages in extending relevant sensing coverage over outlier nodes and maintaining accurate mission objective levels in threat QoI, important in surveillance applications. For this exact purpose we present our VIGILANT "situation aware" quality of information QoI interest group system. VIGILANT is an integrated 3 level design approach, adopting a "situation awareness" perspective and methodology, to increase operational effectiveness. VIGILANT increases surveillance operational effectiveness through:

1. **Minimising on false alarm rates** which has a distinct impact on surveillance performance and intruder target detection, through utilising our designed, evaluated and presented, level 1 PORTENT system[15]. PORTENT optimally self-adjusts sensitivity levels to the current uncertainty (false alarm) present in the sensed observation environment.
2. **Increased QoI surveillance presentation**, for c^2 decision support. PORTENT through optimal self-adjustable sensitivity and the efficient combination of a broad and extensive threat response system[15] (fig.2) provides increased detection accuracy, certainty and timeliness situation assessment performance.
3. **Effective comprehension of the uncertain surveillance environment**. VIGILANT level 2 utilises a Bayesian belief network to derive relevant "context" of the pervading uncertain surveillance situation, for localised active decision making.
4. **Efficient QoI surveillance network Management**. VIGILANT level 3 promotes network management to maintain the mission objective in providing accurate levels in QoI surveillance. This is undertaken in two ways:
    - Networking with sensors with a high probability of confidence in partner "context". This provides advantages in:
        - ***Minimising on outlier contribution*** as indicated in figure 9. Outliers represent neighbouring sensors which are distant in terms of "context" when compared with the rest of the contributing group. Figure 8 illustrates that networking according to a high confidence in partner "context" can propagate increased QoI surveillance provision and robustness. A higher QoI surveillance value indicates better urgency and utility for effective c^2 decision making.
        - ***Improving bandwidth efficiency*** as indicated in figure 12. QoI surveillance updates form sensor partners are typically time sensitive. Figure 11 illustrates that setting a confidence measure on partner "context" promotes reception of QoI surveillance in a timely manner.
    - Employing a QoI surveillance service provision time based on the level of common shared partner "context". This provides advantages in:
        - ***Maintaining accurate levels in QoI surveillance provision through "context aware" adaption*** as indicated in figure 11. Re-evaluating QoI service times to cater for changes in situation "context" propagates increased QoI provision, allowing surveillance applications to perform their tasks effectively.
        - ***Improving on bandwidth efficiency*** as indicated in figure 13. Figure 13 illustrates that setting a high confidence measure on partner "context" and increasing service provision time promotes reception of QoI surveillance in a timely manner.
        - ***Improved operational longevity***, through better communication energy management performance as indicated in figure 14.
5. **Effective intruder geo-location accuracy** as illustrated in figure 8. Figure 8 shows that networking according to threat "context" introduces much lower tracking geo-location error ~18% (High Uncertainty) and ~38% (Low

Uncertainty) when compared with physical energy means. Since VIGILANT operation is primarily geared towards networking according to high confidence in partner "context" to minimise on outlier contribution, this leads to a trade-off being incurred against geo-location accuracy and QoI surveillance provision, as indicated in figure 9. Results indicate for the simulated scenario that trading for improvement on geo-location accuracy (LEACH all nodes) we reduce our QoI surveillance provision by ~10% (High Uncertainty) and by ~6% (Low Uncertainty) and increase our communication energy consumption by ~75% (High Uncertainty) and by ~27% (Low Uncertainty), as shown in figure 15.

Future work will also be undertaken to explore grouping strategies for further optimisation in threat geo-location accuracy and how the VIGILANT concept performs within unreliable communication environments. For this we envisage adapting the VIGILANT system architecture to cater for mission orientation operation, with added tolerance to communication link disruption. Investigation of performance gains, to a real world surveillance scenario with variable observation and communication environment uncertainties, will be conducted.

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] Marshall J.A.R, "*On optimal decision making in brains and social insects*", Journal of the Royal Society, pp. 1-10, January 2009.

[4] Vuilleumier P, "*Distinct spatial frequency sensitivities for processing faces and emotional expressions*", Nat. Neuroscience, 6, pp. 624-631, 2003.

[5] Trimmer P.C, "*Mammalian Choices*", Proceedings of the Royal Society, pp. 2353-2361, July 2008.

[6] Turner M, "*The way we think: conceptual blending and the minds hidden complexities*", New York: Basic Books, 2003.

[7] Heinzelman W, "*An application specific protocol architecture for wireless micro sensor networks",* IEEE Transactions on Wireless Communications, vol.1, no.4, October 2002.

[8] Lindsey S, "*PEGASIS: Power efficient gathering in sensor information systems"*, IEEE Aerospace Proceedings, vol.3, pp.1125-1130, 2002.

[9] Ibriq J, "*Cluster based routing in wireless sensor networks: Issues and challenges"*, SPECTS, pp.759-766, 2004.

[10] Chen W.P, Hou J.C, Sha L, "*Dynamic clustering for acoustic target tracking in wireless sensor networks",* IEEE Transactions on Mobile Computing, vol.3, 2004.

[11] Yang.H, Sidikar.B, "*A protocol for tracking mobile targets using sensor networks"*, Proc. IEEE Workshop Sensor Network Protocols and Applications at IEEE ICC, 2003.

[12] Guang-Yao J, "*CAC: Context adaptive clustering for efficient data aggregation in wireless sensor networks"*, Lecture notes in computer science, vol. 3976, 2006.

[13] Zhou. H, "*CIVIC: A Power and context-aware routing protocol for wireless sensor networks"*, WiCom, pp.2771-2774, 2007.

[14] Bisdikian C, Zahedi S, "*A computational framework for quality of information analysis for detection orientated sensor networks"*, IEEE MILCOM, November, 2008.

[15] Ghataoura D.S, "*PORTENT: Predator aware situation assessment for wireless sensor network surveillance applications*", SPIE: Defence, Security, Sensing, Information systems and networks, Vol.7709, April 2010.

[16] Egan J.P, "*Signal Detection Theory and ROC Analysis*", pp 16-18, New York, Academic Press.

[17] Ghataoura D.S, "*Quality of information and efficient delivery in military sensor networks*", London Communications Symposium (LCS), University College London, September 2009.

[18] Jakobson G, Buford J, Lewis L, "*A framework of cognitive situation modelling and recognition"*, IEEE MILCOM, 2006.

[19] Finn V. Jensen, "*Introduction to Bayesian Networks*", Springer; 1st Edition, 1997.

[20] Krause P, "*Representing Uncertain Knowledge"*, Intellect Books, 1st Edition, pp. 52-66, 1993.

[21] Varga A, "*Software tools for networking: OMNeT++*", IEEE Network Interactive, vol.16, no.4, 2002.

[22] Ghataoura D.S, "*Swarm intelligent odour based routing for geographic wireless sensor network applications*", IEEE Military Communications Conference (Milcom), 2009.