VIGILANT^{+}: Mission Objective Interest Groups for Wireless Sensor Network Surveillance Applications

D.S.Ghataoura[1], J.E.Mitchell[1], G.E.Matich[2]

ABSTRACT

In this paper a system termed VIGILANT^{+} is outlined, which utilises situation awareness for the purposes of enabling distributed, autonomic, sensor management, so that savings on consumption of network resources can be achieved. VIGILANT^{+} is a novel proposition allowing deployed, unattended, wireless sensor nodes to self-organise into dynamic groups and self-manage their transmissions efficiently, according to a current common mission objective. Firstly, a distributed situation assessment system named PORTENT models, detects and characterises potential situations occurring within an uncertain environment, using the metric, quality of surveillance information (QoSI). Secondly, a Bayesian Belief Network (BBN) is utilised to understand and analyse the significance associated with the potential situation, primarily to enable deployed sensors to self-organise and assign themselves to mission objectives autonomously. Thirdly, a system is introduced for distributed autonomic transmission control, which enables the efficient management of sensor network resource consumption. Simulations have been undertaken to verify the integrated VIGILANT^{+} concepts and to demonstrate the effectiveness of the proposed approach in improving network efficiency, without compromising the presentation of mission surveillance utility.

1. INTRODUCTION

Continuing advances in sensor related technologies (battery and low power computation capabilities), including those in pervasive computing are opening opportunities for the deployment and operation of autonomous wireless sensor networks [1]. In addition, a highly distributed ad-hoc infrastructure can support fundamentally new ways of designing and implementing unattended ground sensor (UGS) networks for surveillance applications, in order to provide support in mission objective capabilities, such as threat presence detection, classification and geo-location. In this paper we focus on threat presence detection (mission objective 1) and geo-location (mission objective 2) capability.

The characteristic nature of UGS surveillance operations requires however dynamic, intelligent, sensor management decisions regarding efficient consumption of sensor resources without compromising the objectives of the mission. Efficient management of resource is a necessity since the nature of UGS deployment

can prevent devices being accessible for battery replenishment for long periods of time [2]. In this paper, a system named VIGILANT^{+} is outlined, which utilises a distributed sensor self-management approach to improve robustness to node failure and reduce communications load significantly over the more traditional centralised or task driven approaches [3].

1.1 Related Work

Clustering in ad-hoc sensor networks is an effective technique for achieving scalability and prolonged network lifetime [4-9]. A well-known clustering algorithm for continuous data centric application gathering sensor networks is the Low Energy Adaptive Clustering Hierarchy (LEACH) mechanism [5]. LEACH is a distributed single hop algorithm and includes inherent characteristics such as, self-configuration and localised data transmission control using Time Division Multiple Access (TDMA).

In surveillance scenarios, self-organisation to perform energy efficient threat geo-localisation is equally important, as detailed in [6 -9]. Dynamic clustering for acoustic target tracking (DCATT) [6], 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 single signal threshold.

In addition, the above mentioned schemes [5-9], offer disadvantages by incorporating task driven criteria for sensor management. In [5], CHs are rotated according to metrics such as, battery energy level, transmission power or network connectivity, while in [6] CH's with the greatest received energy are selected, according to the defined signal threshold. Such criteria offer drawbacks due to random rotation of cluster heads (CHs), by introducing considerable re-setup delay of the clusters, increasing communication overhead (energy consumption) and congestion (latency). This can also lead to degradation in surveillance performance by depleting network resources rapidly as in [5] or introducing higher target location errors, as in [6-9], in conditions where the sensing environment is corrupted with high levels of noise, leading to greater group instability.

In addition, [5-9] do not consider the potential resource benefit savings that can be achieved through networking according to the derived understanding of the external operating environment, from captured sensor data. Recent initiatives have begun to address the problem of organising nodes according to the level of understanding about their environment, so that further improvements in operational and network performance can be achieved [10-12], however this view is mostly taken towards the network and medium access control layers.

1.2 VIGILANT^{+} Distributed Autonomic Surveillance Networking

In this paper, VIGILANT^{+}, outlines a new approach towards self-organisation and management of network resource consumption for surveillance missions. This is achieved by taking a "situation awareness" perspective of the surveillance environment, which mainly addresses the drawbacks of existing systems highlighted in the previous section, by minimising on the task driven criteria required for sensor management. Situation awareness (*SA*) is an application-orientated approach, offering a different perspective to [10-12] and can be neatly described through expanding Endsley's "tripartite" model [13]:

- ***Level 1-Perception***-involves the correct identification of entity elements (e.g. type of threat) as well as their combined detection characteristics (e.g. accuracy, identity, certainty and timeliness), representing a measure of the detection information captured, by the distributed surveillance network [14].
- ***Level 2-Comprehension***-involves derivation of the significance associated with uncertain sensor data, enabling relevant decision making and confidence in mission objective understanding ("context").
- ***Level 3- Projection***-the ability to project future "context" of the mission objective environment based on potential association of the fragmented sensor data, within a temporal frame.

Through integrating levels 1 and 2, VIGILANT^{+} minimises random rotation of CHs, as currently with [5-9], by ensuring CHs are only self-nominated according to the neighbourhood sensor, which registers the highest change in monitored threat dynamics, further detailed in section 2. In addition, VIGILANT^{+} also caters against the effects of the noisy and false alarm surveillance environment, primarily through level 1 and 2 operations, which can compromise on mission objective utility and is something not actively considered in [5-9]. In this paper, we also improve on [6-9] by not considering a signal energy threshold mechanism for target localisation, but rather self-organise by considering locally derived threat awareness using Bayesian techniques and include an evaluation of the relative positions of deployed sensors to the current monitored threat, in terms of geometric dilution of precision (GDOP), for improved geo-location performance.

By also considering the confidence in mission objective "context" in level 2, VIGILANT^{+} can allow deployed UGS networks to conserve and self-manage their lower layer operational resources efficiently, such as communication energy (longevity) and bandwidth (latency) consumption, by minimising on the need for continuous updates, as currently done in [4-6]. In addition to our previous work [15], this paper also highlights the network resource efficiency benefits that can be achieved, by incorporating a distributed, mission objective, autonomic approach, as shown below, rather than the more traditional centralised approaches detailed in [5-9]:

- Derivation of confidence through expansion of level 2 “context”, allowing deployed sensors to assign themselves to a particular mission objective autonomously.
- A partial and fully observable Markov Decision Process enabling autonomic transmission control, so that further benefits can be achieved in conserving on network resource consumption.

As with current LEACH operation [5], utilising TDMA in periods of low surveillance activity, can introduce bandwidth inefficiencies by non-utilisation of time slots for packet transmission. Also the medium access control strategies used in [6-9] are primarily pure contention access protocols, which can result in packets being dropped during high surveillance activity. In this paper, we manage this dual scenario by proposing a contention-schedule channel access mechanism, through our autonomic transmission control methodology, detailed in section 3. This allows a duty-cycle approach towards localised sensor channel contention access, where access periods are defined according to the evaluated urgency concerning the monitored threat, to improve on bandwidth utilisation, but without compromising on mission objective surveillance utility. Access periods defined in this way become sensor unique and can assist to balance the surveillance reporting load appropriately across the deployed network. Figure 1, illustrates and summarises the novelty of our proposed method for improving on operational resource efficiencies, through adaptive networking according to the *SA* of the surveillance environment.

The remainder of this paper is structured as follows: Section 2 details VIGILANT^{+} self-organisation. Section 3 details the autonomic transmission control methodology, by utilising the underlying mission objective “context”. Section 4 details VIGILANT^{+} system performance and Section 5 concludes the paper.

2. VIGILANT^{+} SELF-ORGANISATION

VIGILANT^{+} self-organisation is primarily focused on sensors establishing their localised “context” of the present situation (e.g. awareness to a threat) in order to allow sensor self-assignment to a particular mission objective. Self-organisation based on a common “context” can facilitate operational effectiveness by:

- Providing robustness in the probability of detection to common perceived events of interest, which consequently increases surveillance provision utility, as detailed in section 2.1 and 2.2.
- Activating only those sensors currently providing a relevant sensing coverage to a security-sensitive area, thus propagating increased relevance in surveillance provision, as detailed in section 2.3. Non-active sensors therefore participate less in group communication, providing further network resource consumption efficiencies.

- Reducing the influence of sensors which share low common mission objective "context" (outliers) which can decrease surveillance provision utility, as detailed in section 2.3.

2.1 VIGILANT^{+} Level 1 – Perception

False alarms have a distinct impact on perception and mission performance since they relate to threat detection. A low false alarm rate, which is needed to avoid unnecessary responses, involves a larger sample set being collected for threat verification, implying greater sampling energy consumption and reduced timeliness. A system that has self-adjustable sensitivity to accommodate sensing environment uncertainties is therefore beneficial. Our evaluated situation assessment system, named PORTENT, comprises level 1 perception, accommodating the adjustable sensitivity requirement [16].

As shown in figure 2, PORTENT comprises a combined "fast" but less accurate and "slow" but more accurate validation system. "Fast" response is based on single sensory observations modelled using standard signal detection theory [17]. "Slow" response is modelled by integrating sensory samples over time, using the sequential probability ratio test (SPRT), in terms of the Neyman-Pearson (NP) lemma [18]. The SPRT tests two alternative hypotheses, representing the presence and absence of threat while updating the relative likelihood ratio of each as new sensory samples arrive. A decision in favour of a hypothesis is made by comparing the updated ratio against the NP detection sensitivity, which is designed to self-adjust in order to maximise the detection probability subject to the current false alarm. This assists in minimising on both false alarm detection and the need for extensive sampling.

For threat presence characterisation, PORTENT specifically uses detection accuracy (q_1), detection certainty (q_2) and timeliness (q_3) quality factors. A linear weighted fusion strategy is used by assigning normalized weights (W_b), to capture localised quality of surveillance information (*QoSI*), as shown in (1).

$$QoSI = \sum_{b=1}^{T} W_b * q_b \tag{1}$$

where T = Number of Quality Factors Used.

The PORTENT system provides strategies for efficiently combining both "fast" and "slow" response systems, to provide increased detection accuracy, certainty and timely situation assessment performance. The results of our evaluation studies indicate that incorporating PORTENT option 2 increases overall *QoSI* [16].

2.2 VIGILANT^{+} Level 2 – Mission Objective Surveillance Comprehension and Analysis

Situations occurring in an uncertain environment require a level of cognition to derive "context" of those situations. Level 2 utilises an action orientated design approach [19], in the form of a Bayesian Belief Network (BBN), as shown in figure 3. A BBN is a directed acyclic graph, using a collection of nodes denoting the random variables representing the situation domain. Corresponding links between nodes define the casual relationships between them, with conditional probability tables (CPTs) encoding the quantitative influence. Where no link exists between nodes, quantitative influence is given by marginal probabilities. Table 1 summarises the relevant probability derivations from figure 3, for making "context" based decisions at local sensors, concerning the current single threat situation for each mission objective.

2.3 VIGILANT^{+} "Context" Querying for Sensor Mission Objective Self-Assignment

Ad-hoc group self-organisation of single hop sensors can be enhanced through assigning sensors that share common "context" to a mission objective. Using "context" for self-organisation involves procedures which must support the following considerations:

- ***Dynamics:*** Groups must provide adaptability, depending on changes to "context", allowing sensors to leave and join at any time, during a mission.
- ***Group Initiator re-election:*** Dynamic re-election of new CHs is imperative to maintaining relevant surveillance report aggregation, while minimising communication overhead.

Bearing in mind these considerations, mission self-assignment can be restricted to querying about certainty in "context", where communication efficiency relies on mission objective specific "context" instead of traditional IP-style addressing. "Context" centricity enforces uncoupled coordination, where distributed sensors are modelled as a set of components interacting with each other through the sensor analysing and reacting to their "context" independently. This supports flexibility within dynamic UGS surveillance network scenarios.

The certainty factor (*CF*) model [20] can establish the degree of certainty which sensors have regarding a specific "context" of the mission objective. CF operates according to proportional measures in belief (*MB*) and measures in disbelief (*MD*) towards a certain hypothesis. The hypothesis stems from whether a distributed sensor should assign themselves to a specific mission objective, according to its current "context", as shown in (2), using table 2, derived from figure 3.

$$CF''Sensor'' = (MB - MD) \Big/ 1 - min(MB, MD) \tag{2}$$

Sensor self-assignment is initiated by the group initiator (*GI*) publish request, represented by the current sensor which perceives the highest current threat (*Threat-"High"*), calculated as detailed in table 1, entry 4 and shown in (3).

$$p(Threat-"High") > (1 - p(Threat-"High")) \tag{3}$$

A combined *CF "Mission Objective"* evaluation, as shown in (4), quantifies the degree of certainty that a *GI* and a sensor should form a partnership due to their respective current "context" in a mission objective. *CF "GI"* is calculated in the same way as (2).

Figure 4, illustrates the overall publish-subscribe "context" centric operation, for *GI* mission objective led sensor self-assignment and group self-organisation.

$$CF"Mission\ Objective" = \begin{cases} if\ CF"GI"\ and\ CF"Sensor" \geq 0 : CF"GI" + CF"Sensor"(1 - CF"GI") \\ if\ CF"GI"\ and\ CF"Sensor" < 0 : CF"GI" + CF"Sensor"(1 + CF"GI") \\ Otherwise \quad : \dfrac{(CF"GI" + CF"Sensor")}{1 - min(|CF"GI"|, |CF"Sensor"|)} \end{cases} \tag{4}$$

2.4 VIGILANT+ Group Initiator Re-Election

GI re-election is dynamically conducted in the process of a mission. Assigned sensors rely on the current *GI* mission objective "context" centric address (GI_{mocca}) sent in the initial publish request, to re-evaluate whether to initiate "new" *GI* status, as shown in (5).

$$if\ (Confidence\ in\ current\ mission\ objective"context") \geq (GI_{mocca}) \tag{5}$$

$$Then, Publish"New"\ GI\ Mission\ Objective\ Request\ Status$$

Upon the condition in (5) being satisfied, the new *GI* re-evaluates the distributed mission objective "context" certainty, as shown in figure 4.The resulting new self-organised group further facilitates maintaining relevant on-going aggregation in surveillance information utility.

3. VIGILANT$^+$ AUTONOMIC NETWORK CONTROL

Autonomic network control is orientated towards the management of network resources at infrastructure level, through applying feedback upon temporal environmental dynamics. Being efficient to network resource consumption implies a methodology, which provides projection capabilities (level 3) concerning the "context" to a current specific mission objective. This can be formalised using a random discrete time state representation, through either a Markov Decision Process (*MDP*) or Partially Observable *MDP* (*POMDP*) [21], detailed in

sections 3.1 and 3.2. Being in a particular state signifies an evaluation of the current shared "context" to a specific mission objective at that point in time, detailed in sections 3.3 and 3.4. This enables us to make necessary transmission control decisions (selection, scheduling and prioritisation), detailed in sections 3.5 to 3.7.

3.1 MDP Formulation for Transmission Control

A *MDP* representation stipulates that a belief probability towards the current state environment is conditionally independent of all previous states and actions taken due to the Markov property exhibiting memory-less operation [21]. This property implies current actions regarding transmission decision making are dependent only on the current state, as shown in figures 5(a) and (b). Evaluating a current belief state (BS_{k+i}) to facilitate transition to the next state ($STATE_{k+i}$), where i=0 at initialisation, is based only on the conditional joint probability of current observation z_{k+i} (A_1) and current action taken a_{k+i} (A_3), as shown in (6).

$$BS_{k+i} = p(STATE_{k+i} \mid A_1, A_3) \tag{6}$$

From figure 5(a), further GI updates are utilised, to deduce the current observable shared state environment. A consequence of utilising further GI updates is consumption of more network communication energy and bandwidth. We seek to explore this, with a view to considering the increase in surveillance information utility if any, due to an informed perspective about the current shared state environment, at the expense of more network resource consumption.

3.2 POMDP Formulation for Transmission Control

A *POMDP* implementation models the decision making process in which it is assumed that the system dynamics are determined by an *MDP*, but the decision maker (UGS) has an incomplete perspective regarding the shared state environment. Operating within a partial observable state environment requires feedback control of previous actions and observations [21]. The essential task for *POMDP* transmission feedback-control implementation is belief state estimation (*BSE*), as shown in figure 6(a) and (b). *BSE* represents the most probable view of the current shared state, given past experiences. Evaluating a current *BSE* (BSE_{k+i}) , to facilitate transition to the next state ($STATE_{k+i}$), where i=1 at initialisation, is based on the conditional joint probability of the current observation z_{k+i} (A_1), previous action a_{k-i} (A_3) and previous BSE_{k-i} (A_4), given in (7).

$$BSE_{k+i} = p(STATE_{k+i} \mid A_1, A_3, A_4) \tag{7}$$

From figure 6(a), we represent partial observable operation, through not relying on further *GI* updates, to substantiate whether this will provide improved network longevity and bandwidth efficiency savings at the expense of any degradation in reported surveillance information utility.

3.3 Determination of Shared Mission Objective 1 "Context"

For mission objective 1 the joint probability for shared non-common threat awareness "context" between the *GI* and its corresponding group member is a random variable, *U*, with probability density function (PDF_1) and cumulative distribution function (CDF_1), $U\sim N(\mu , \sigma^2)$. Additionally the joint probability in shared common threat awareness "context" is a random variable, *T*, with a PDF_2 and CDF_2 , $T\sim N(\mu , \sigma^2)$.

Determining the level of common "context" is based on the threshold ***S***, chosen as the intersection point of the two respective PDF's, as to minimise the sum of probabilities for incorrect determination of common "context" being made. The probability of correct detection in common threat awareness "context" (P_1) forms the basis for eventual BS_{k+i} or BSE_{k+i} evaluation, given in (8).

$$BS_{k+i} = p(STATE_{k+i} | P_1 , A_3) \text{ And } BSE_{k+i} = p(STATE_{k+i} | P_1, A_3 , A_4) \tag{8}$$

where, $P_1 = 1 - CDF_2 (S)$

3.4 Determination of Shared Mission Objective 2 "Context"

We assume sensors have the ability to obtain current threat position (x_{Threat}, y_{Threat}) using techniques such as time difference of arrival, to calculate current geometric dilution of precision ($GDOP_k$), with respect to the *GI*. $GDOP_k$ measures accuracy in shared geo-location "context", quantifying the mapping of measurement errors into position errors, magnified by the geometric relation of sensors to threat geometry [22]. The geometry matrix $\mathbf{H^T H}$, at each time instant, for *N* active sensors, is expressed in (9). In all cases we assume, *GI* (x_{GI}, y_{GI}) and active sensor (x_i, y_i) positions are known.

$$H^T H = \begin{bmatrix} \sum_{i=1}^{N-1} (a_{xi} - a_{xr})^2 & \sum_{i=1}^{N-1} (a_{xi} - a_{xr})^2 (a_{yi} - a_{yr}) \\ \sum_{i=1}^{N-1} (a_{xi} - a_{xr})^2 (a_{yi} - a_{yr}) & \sum_{i=1}^{N-1} (a_{yi} - a_{yr})^2 \end{bmatrix} \tag{9}$$

Where, $a_{xi} = (x_{Threat} - x_i) \Big/ \sqrt{(x_{Threat} - x_i)^2 + (y_{Threat} - y_i)^2}$, $a_{xr} = (x_{Threat} - x_{GI}) \Big/ \sqrt{(x_{Threat} - x_{GI})^2 + (y_{Threat} - y_{GI})^2}$

$a_{yi} = (y_{Threat} - y_i) \Big/ \sqrt{(x_{Threat} - x_i)^2 + (y_{Threat} - y_i)^2}$ and $a_{xi} = (x_{Threat} - x_i) \Big/ \sqrt{(x_{Threat} - x_i)^2 + (y_{Threat} - y_i)^2}$.

Since the matrix $\mathbf{(H^T H)}$ is symmetric and positive definite, all eigenvalues λ_1, λ_2 are real and positive. The trace of the matrix $\mathbf{(H^T H)}$ is then equal to the sum of the eigenvalues given in (10).

$$trace(H^T H) = \lambda_1 + \lambda_2 = \sum_{i=1}^{N-1} [(a_{xi} - a_{xr})^2 + (a_{yi} - a_{yr})^2] \tag{10}$$

$GDOP_k$ is therefore given as shown in (11).

$$GDOP_k = \sqrt{trace(H^T H)^{-1}} \tag{11}$$

Utilising the $GDOP_k$ measure to serve as an approximation of the current threat location (CTL) , in terms of circular error probable (CEP) [23], we can obtain a likelihood measure for common "context" (Q_1), forming the basis for eventual BS_{k+i} or BSE_{k+i} evaluation, given in (12).

$$BS_{k+i} = p(STATE_{k+i} \mid Q_1, A_3) \text{ And } BSE_{k+i} = p(STATE_{k+i} \mid Q_1, A_3, A_4) \tag{12}$$

where, $Q_1 = p(CTL \mid GDOP) = \exp(-\frac{(GDOP_{MAX} - GDOP_k)^2}{2\sigma^2_{Range\,Error}} \Big/ \sqrt{2\pi}\sigma_{Range\,Error}$

3.5 Mission Objective Transmission Control: Selection

Selection for transmission, at each decision epoch, can be formulated in terms of state information gain using information discrimination techniques such as Rényi divergence, also known as α-divergence [24]. Utilising a state information gain approach forms a direct measure on the quality for sensor transmission selection, this being either to select transmission or not, with an expected utility calculated for each. The calculation of information gain between two probability densities p_1 and p_0 using Rényi divergence denoted by, $(p_1 \,||\, p_0)$, is given in (13), where the α parameter is used to adjust how heavily one emphasises the tail of the two distributions p_1 and p_0.

$$D_\alpha(p_1 \,||\, p_0) = \frac{1}{1-\alpha} \ln \int p_1^\alpha(x) p_0^{1-\alpha}(x)\, dx \tag{13}$$

In the limiting case of $\alpha \rightarrow 1$ the Rényi divergence becomes the commonly used Kullback-Leibler (KL) discrimination, given in (14).

$$\lim_{\alpha \to 1} D_\alpha(p_1 \,||\, p_0) = \int p_0(x) \ln \frac{p_0(x)}{p_1(x)} \tag{14}$$

If probability state representations are taken from a normal distribution, $p_1 \sim N(\mu_1, \sigma_1^2)$ and $p_0 \sim N(\mu_0, \sigma_0^2)$ the KL discrimination (D_{KL}) is shown in (15).

$$D_{KL} = \lim_{\alpha \to 1} D_\alpha(p_1 \,||\, p_0) = \frac{(\mu_1 - \mu_0)^2}{2\sigma_0^2} + \frac{1}{2}\left(\frac{\sigma_1^2}{\sigma_0^2} - 1 - \ln\left(\frac{\sigma_1^2}{\sigma_0^2}\right)\right) \tag{15}$$

For mission objective 1 (M1) operation, the requirement is to have as much divergence between p_1 (non-common threat awareness) and p_0 (common threat awareness) to increase information gain. Expected Utility (EU) in (16) illustrates how risk attitudes are managed according to current uncertainty towards high threat presence awareness.

$$EU_{M1-Yes-TX} = \frac{1}{1+e^{(\beta - D_{KL})}} * (BS_{k+i} \; or \; BSE_{k+i}) \qquad (\beta = 2/D_{KL-MAX}) \tag{16}$$

For mission objective 2 (M2) operation, the requirement is to have as much convergence between p_1 ($GDOP_{MAX}$) and p_0 ($GDOP_k$) to increase information gain. Risk attitudes are modelled by (17) on $GDOP_k$, this being a direct approximation on the current CEP, a measure for geo-location accuracy.

$$EU_{M2-Yes-TX} = \frac{1}{1+e^{(D_{KL} - \beta)}} * (BS_{k+i} \; or \; BSE_{k+i}) \qquad (\beta = D_{KL-MAX}/2) \tag{17}$$

Transmission is selected by ensuring that the current expected utility for "yes" transmission is greater than or equal to the expected utility of selecting "no" transmission, as given in (16) and (17) but with complementary weighting.

3.6 Mission Objective Transmission Control: Scheduling

Scheduling can be made according to BS_{k+i} or BSE_{k+i} which represents a belief transition probability from the current to future state environments. Figures 5(b) and 6(b), illustrate the decision for selecting transmission scheduling, with both conditions derived to provide group stability, for situations where no state "contextual" discrepancy occurs. In mission objective 1 this constitutes non-scheduling as long as the BS_{k+i} or BSE_{k+i} adds to an increasing level in shared threat awareness "context" as evaluated in (8). In mission objective 2 this constitutes scheduling as long as the BS_{k+i} or BSE_{k+i} increases the level in shared geo-location "context" representing improved $GDOP_k$ from the previous state, which is a direct approximation of the current improvement in CEP, as shown in (12).

3.7 Mission Objective Transmission Control: Prioritisation

In order to ensure reliable surveillance report delivery and promote network longevity and bandwidth efficiency, sensors which are scheduled for transmission determine a service priority time, based on BS_{k+i} or BSE_{k+i}. The service priority time (M) is evaluated in terms of a shared state environment which continues for a total H time steps (seconds), as shown in (18).

$$M \sim Binomial(H, Mission\ Objective\ Specific\ BS_{k+i}\ or\ BSE_{k+i})$$
$$p(M = H) \sim (Mission\ Objective\ Specific\ BS_{k+i}\ or\ BSE_{k+i})^{H} \quad (18)$$

Derived M is dependent on the degrees of shared "context" present, with respect to the current GI. A higher belief state transition probability implies a higher M (lower urgency) since the uncertainty in the shared state environment is low. This allows unique sensor provisioning, through individual schedule channel access periods, promoting bandwidth efficiency and minimal congestion for group surveillance reporting. Figure 7, details the service priority time algorithm. Figure 8 illustrates the integrated process for VIGILANT^{+} distributed sensor management, for the purposes of self-assignment and self-managed transmission control.

4. VIGILANT^{+} SYSTEM PERFORMANCE

System performance is evaluated using the OMNeT++ simulation platform [25]. We deploy a static grid network within a 1000 × 1000 m^2 region, using a total of 9 sensors. We assume an intruder will be approaching the region in the near future and subsequently sensing operations are active [26]. Surveillance monitoring concerns a mobile target moving with constant velocity, v m/s, in a diagonal trajectory. Simulations are based on a sampling rate of 100 samples/sec, sensing range of 1000m, no packet loss and 500m transmission range, with the IEEE 802.11, distributed coordination function in basic access mode, for medium access control. Surveillance performance is measured either against level-1 threat detection certainty (*TDC*), through varying the mean separation in yes threat, no threat probability occurrence distributions or velocity of the mobile target, v m/s.

For energy consumption performance the model of [5] is used, with an arbitrary packet size of 500 bits. From figure 5(a), updates are only sent when the *GI* confirms a positive PORTENT detection, (section 2.1, fig.2), named, *MDP-Option 1* or when the *GI* condition for confidence in current threat, as shown in table 1, entry 6, is less than the previous confidence named, *MDP-Option 2*. Geo-location accuracy is measured in terms of *CEP-50%*, defined as the radius of the circle that has its centre at the true position, containing half the realisation uncertainties of the random vector. Figures 9-12, give performance results for a realistic joint mission objective surveillance operation.

4.1 Surveillance Utility Performance

The results of figures 9 and 10 (a) and (b) show that surveillance utility for threat presence detection (*QoSI*) and geo-location (*CEP-50%*) is jointly improved by incorporating a joint threat presence and geo-location "context" methodology, as highlighted in section 2. Figure 9 shows that continuous updates utilising all one hop

neighbours (LEACH), without consideration of shared threat presence detection "context" decreases *QoSI*, especially within low certainty surveillance environments, by approximately 13%. Figure 9, also highlights that reduction in influence of outliers within the network, using the operation outlined in figure 4, increases robustness in *QoSI* utility. Figures 10 (a) and (b) indicate distributed geo-location performance (VIGILANT^{+}) is comparable to a centralised operation utilising all one hop neighbours (LEACH), with only approximately a 7% loss in accuracy. As expected, geo-location operation can never be truly distributed, as shown through the LEACH results and should be kept central to the *GI* for improved performance. Figures 10 (a) and (b) also illustrate non-integration of geo-location "context" [15] in terms of *GDOP*, or reliance on received energy corrupted with noise from the sensing environment (DACTT), can result in geo-location performance shortfalls. As shown in figures 9 and 10, utilising derived mission objective "context", primarily through level 2 Bayesian Belief Network operation, can assist in filtering uncertainty towards a current threat situation, in order to improve on surveillance utility performance.

4.2 Communication Energy Consumption Performance

Figures 11 (a) and (b) show managing transmissions according to mission objective "context" can minimise on non-essential communication, which ultimately improves network longevity and prevents surveillance utility performance degradation, as shown in figures 9 and 10. Network communication energy consumption for operational longevity is improved through distributed self-managed transmission control, as highlighted in section 3, by making self-adaptive transmission control decisions according to shared "context" in a specific mission objective. A Centralised approach for surveillance updating as in our previous work [15], or continuous updating as in LEACH, do not promote this and as a result increase energy consumption. Being able to make self-adaptive transmission control decisions is imperative since, sensor nodes are typically restricted in their energy resources, therefore non –essential communication and overhead should be kept to a minimum, in order to prolong network lifetime, which VIGILANT^{+} operation clearly promotes.

4.3 Bandwidth Efficiency Performance

Results in figure 12 (a) and (b) indicate that utilising a surveillance service priority scheduling algorithm, figure 7, coupled with a *POMDP* methodology, allows a duty cycle benefit approach for individual sensor channel contention access, to improve on bandwidth efficiency. Figures 12 (a) and (b) show that a contention-schedule medium access control, where access periods vary according to shared mission objective "context" , offers better efficiency as compared to purely schedule based (LEACH) operation, through TDMA control, which was

found in our simulation studies to have an average 250 msec latency delay. In addition, bandwidth efficiency is increased, without degradation in mission objective surveillance utility, as shown in figures 9 and 10.

5. CONCLUSION

Efficient UGS surveillance operations require systems that can manage mission objective priorities autonomically in a distributed manner, within environmental (false alarm) and network resource consumption constraints. VIGILANT^{+} adopts a distributed "situation aware" design approach for sensor network self-management, in order to provide an improvement in operational effectiveness. Such an approach firstly allows for autonomic organisation of sensor groups to meet the needs of a specific mission objective, within environmental constraints. Secondly, we utilise a *MDP* or *POMDP* methodology for autonomic network control, in order to enable efficient management of network resource consumption, without compromising on mission objective surveillance utility. Results indicate that VIGILANT^{+} can improve on network resource consumption by adapting according to the "situation awareness" perspective of the surveillance environment, primarily through level 3 operation, as illustrated in figures 1 and 8.

We also conclude that a *POMDP* implementation offers improved overall network efficiency performance, compared with a fully observable *MDP* approach, primarily due to a reduction in use of further *GI* observation updates, with only a small decrease in geo-location utility performance resulting. Further work is required however to extend the *POMDP* operation for adapting decision epochs, figure 6(b), matched to the characteristics of the surveillance threat and experimentation for VIGILANT^{+} performance within an unreliable channel communication environment.

6. REFERENCES

[1] Akyildiz I, Su W, Cayirci E, "A survey on sensor networks", IEEE Communications Magazine, 2002, 40, (8), pp.102-114.

[2] Onur E, Ersoy C, Delic H and Akarun L, "Surveillance wireless sensor networks: deployment quality analysis", IEEE Network, 2007, 21, (6), pp. 48 -53.

[3] Bevington J.E, "Distributed sensor management and target tracking for unattended ground sensor networks", Proc. SPIE Security and Defence, Battlespace digitization and network centric systems IV, vol.5441, 2004, pp.25-35.

[4] Singh S.K, "Routing protocols in wireless sensor networks – a survey", International Journal of Computer Science and Engineering Survey (IJCSES), 2010, 1, (2), pp.63-83.

[5] Heinzelman W, "An application specific protocol architecture for wireless micro sensor networks", IEEE Transactions on Wireless Communications, 2002, 1, (4), pp.660-670.

[6] Chen W.P, Hou J.C, Sha L, "Dynamic clustering for acoustic target tracking in wireless sensor networks", IEEE Transactions on Mobile Computing, 2004, 3, (3), pp.258-271.

[7] 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.

[8] Biswas P.K, Phoha S, "Self-organising sensor networks for integrated target surveillance", IEEE Transactions on Computers, 2006, 55, (8), pp.1033 – 1047.

[9] Roelant D, Yen K, Hao Z, " Self organisation of unattended wireless acoustic sensor networks for ground target tracking", Elsevier Journal of Pervasive and Mobile Computing, 2009, 5 , (2), pp.148 -164.
[10] Guang-Yao J, "CAC: Context adaptive clustering for efficient data aggregation in wireless sensor networks", Lecture notes in computer science, 2006, 3976, pp.1132-1137.
[11] Preece A, "Reasoning and resource allocation for sensor-mission assignment in a coalition context," Proc. IEEE MILCOM, San Diego, USA, November 2008.
[12] Garcia-Luna-Aceves J.J, Mosko M, "Context-aware protocol engines for ad hoc networks", IEEE Communications Magazine, 2009, 47, (2), pp.142-149.
[13] Endsley M.R, "Toward a theory of situation awareness in dynamic systems", Human Factors, 1995, 37, (1), pp.32-64.
[14] Bisdikian C, "On sensor sampling and quality of information: a starting point", Proc. of the 5th annual IEEE PerComW, White Plains, New York, USA, March 2007, pp.279-284.
[15] Ghataoura D.S, Mitchell J.E, Matich G.E, "VIGILANT: "Situation-Aware" Quality of Information Interest Groups for Wireless Sensor Network Surveillance Applications", Proc. European SPIE Security and Defence, Unmanned/Unattended Sensors and Sensor Networks VII, vol.7833, Toulouse, September 2010.
[16] Ghataoura D.S, Mitchell J.E, Matich G.E, "PORTENT: Predator aware situation assessment for wireless sensor network surveillance applications", Proc. SPIE: Defence, Security and Sensing, Information systems and networks, vol. 7709, Orlando, April 2010.
[17] Egan J.P, "Signal Detection Theory and ROC Analysis", New York, Academic Press, pp 16-18.
[18] Onur E, Ersoy C, Delic H, "How many sensors for an acceptable breach probability level?, Computer Communications, 2006, 29, (2) , January 2006, pp.172-82.
[19] Jakobson G, Buford J, Lewis L, "A framework of cognitive situation modelling and recognition", IEEE MILCOM, Washington, USA, October 2006, pp. 1-7.
[20] Krause P, "Representing uncertain knowledge", Intellect Books, 1st Edition, pp. 52-66, 1993.
[21] Lerma O.H, "Adaptive Markov control processes", Springer-Verlag, New York, 2001.
[22] Kadar I, "Optimum geometry selection for sensor fusion", SPIE: Defence, Security and Sensing, Conference on Signal processing, Sensor fusion and Target recognition VII, 1998, 3374, pp.96-107.
[23] Torrieri D.J, "Statistical theory of passive location systems", IEEE Transactions on Aerospace and Electronic Systems, 1984, AES-20, (2), pp.183-198.
[24] Kreucher C.M, "An information-based approach to sensor management in large dynamic networks", Proceedings of the IEEE, 2007, 95, (5), pp.978 – 999.
[25] Varga A, "Software tools for networking: OMNeT++", IEEE Network Interactive, 2002, 16, (4).
[26] Ghataoura D.S, Mitchell J.E, Matich G.E, "Swarm intelligent odour based routing for geographic wireless sensor network applications", Proc. IEEE MILCOM, Boston, USA, October 2009.

Authors Affiliations
[1]Department of Electrical and Electronic Engineering, University College London, Torrington Place, London, WC1E 7JE; E-mail:dghataou@ee.ucl.ac.uk
[2]Selex Galileo Ltd, Christopher Martin Road, Basildon, Essex, SS14 3EL, U.K;
Email:george.matich@selexgalileo.com

Probability Expression	Probability Derivation from figure 3 using CPT Analysis
1. p(Yes Intruder Present – "True" (C))	P(C | Threat Presence True) * P(r) + P(C| Threat Presence False)* (1 – P(r))
2. p(No Intruder Present – "True" (D))	P(D | Threat Presence True) * P(r) + P(D | Threat Presence False)* (1 – P(r))
3. p(Current Threat Level – "High" (F))	[P(F| C,D) * P(C) * P(D)] + [P(F | ~C,D) * P(~C) * P(D)] + [P(F|C,~D) * P(C) * P(~D)] + [P(F | ~C,~D) * P(~C) * P(~D)]
*4.**Group Formation** p(Threat-High)*	P(Yes-"Form"| F)* P(F) + P(Yes-"Form"| ~F)*P(~F)
5.p(Local Awareness to Current Threat – "High" (L))	[P(L | C,F) * P(C) * P(F)] + [P(L | ~C,F) * P(~C) * P(F)] + [P(L | C,~F) * P(C) * P(~F)] + [P(L | ~C,~D) * P(~C) * P(~F)]
*6. **Mission Objective 1** p(Confidence in Current Threat – "High" (Q))*	P(Q | L) * P(L) + P(Q| ~L)* P(~L)
7. p(L and Position Observation Estimate (POE) – "High" (E))	[P(E | L,POE) * P(L) * P(POE)] + [P(E | ~L,POE) * P(~L) * P(POE)] + [P(E | L,~POE) * P(L) * P(~POE)] + [P(E | ~L,~POE) * P(~L) * P(~POE)]
*8. **Mission Objective 2** p(Confidence in Geo-Location – "High" (S))*	P (S | E) * P(E) + P(S | ~E)* P(~E)

Table1. *Probability derivations for the purposes of initiating group formation and making "context" informed decisions regarding a specific mission objective*

	Mission Objective 1 – Threat Presence	Mission Objective 2 – Threat Geo-Location
Increased Belief (MB) Expression	$\frac{p(\text{Awareness to Threat} \mid L) - p(L)}{1 - p(L)}$	$\frac{p(\text{Geo} - \text{Location Awareness} \mid E) - p(E)}{1 - p(E)}$
Increased Disbelief (MD) Expression	$\frac{p(L) - p(\text{Awareness to Threat} \mid L)}{p(L)}$	$\frac{p(E) - p(\text{Geo} - \text{Location Awareness} \mid E)}{p(E)}$

Table2. *MB and MD expressions for local UGS mission objective CF evaluation, using table 1*

Figure Captions:

Figure 1. VIGILANT^{+} approach to *SA* informed autonomic networking

Figure 2. PORTENT situation assessment architecture

Figure 3. VIGILANT^{+} BBN for localised single threat mission objective situation analysis

Figure 4. "Context" centric publish-subscribe querying for mission objective self-assignment. Feedback is used for non- subscribers to re-evaluate their position if "contextual" changes occur

Figure 5. (a) *MDP* representation of the underlying shared state environment, **(b)** Projection of the decision chain to future states is driven by BS_k. Temporal decision epoch frequencies for scheduling, depends on the variation of received GI updates

Figure 6. (a) *POMDP* representation of the underlying shared state environment, **(b)** Projection of the decision chain to future states is driven by BSE_{k+i}. Temporal decision epoch frequencies for scheduling, depends on the variation in localised sensor observations

Figure 7. Service priority time algorithm governed by the complementary BS_{k+i} or BSE_{k+i} transition probability

Figure 8. VIGILANT^{+} distributed autonomic sensor management

Figure 9. Mission objective 1 performance, *QoSI* with level-1 *TDC*, v = 5m/s

Figure 10. Mission objective 2 performance CEP-50% with v (m/s) (a) *TDC* = 0.01 (b) *TDC* = 0.9

Figure 11. Communication energy consumption performance (a) *TDC* = 0.01 (b) *TDC* = 0.9

Figure 12. Surveillance report update quality of service (latency) (a) *TDC* = 0.01 (b) *TDC* = 0.9

Figure 1

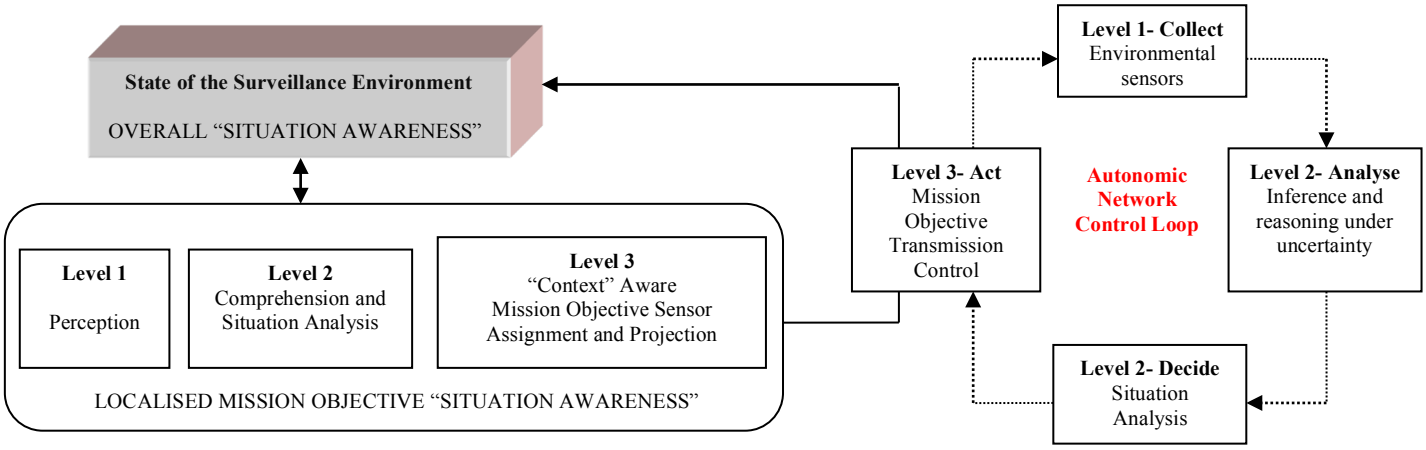


Figure 2

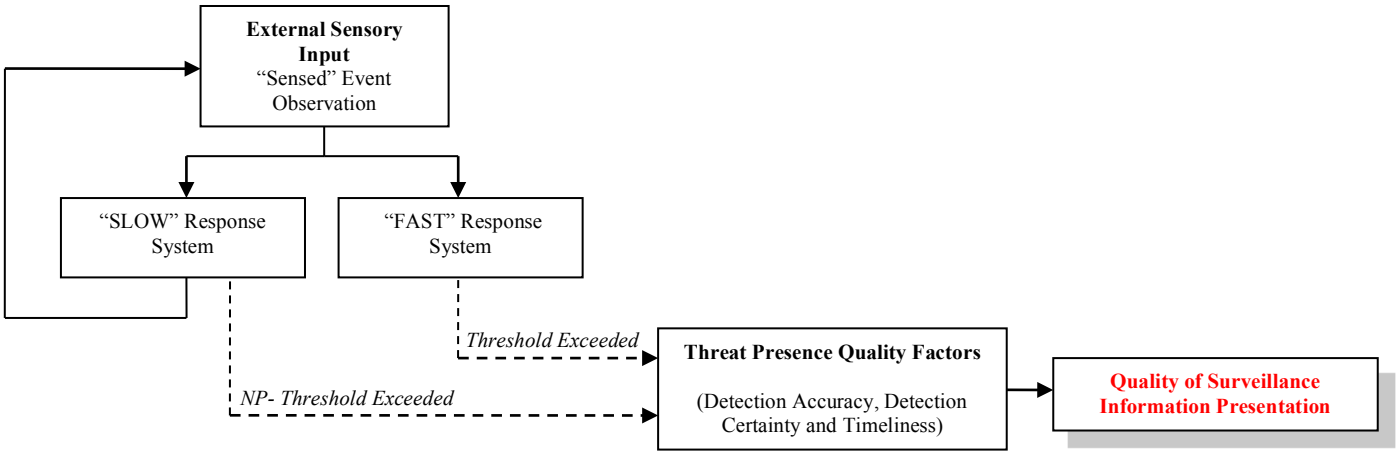


Figure 3

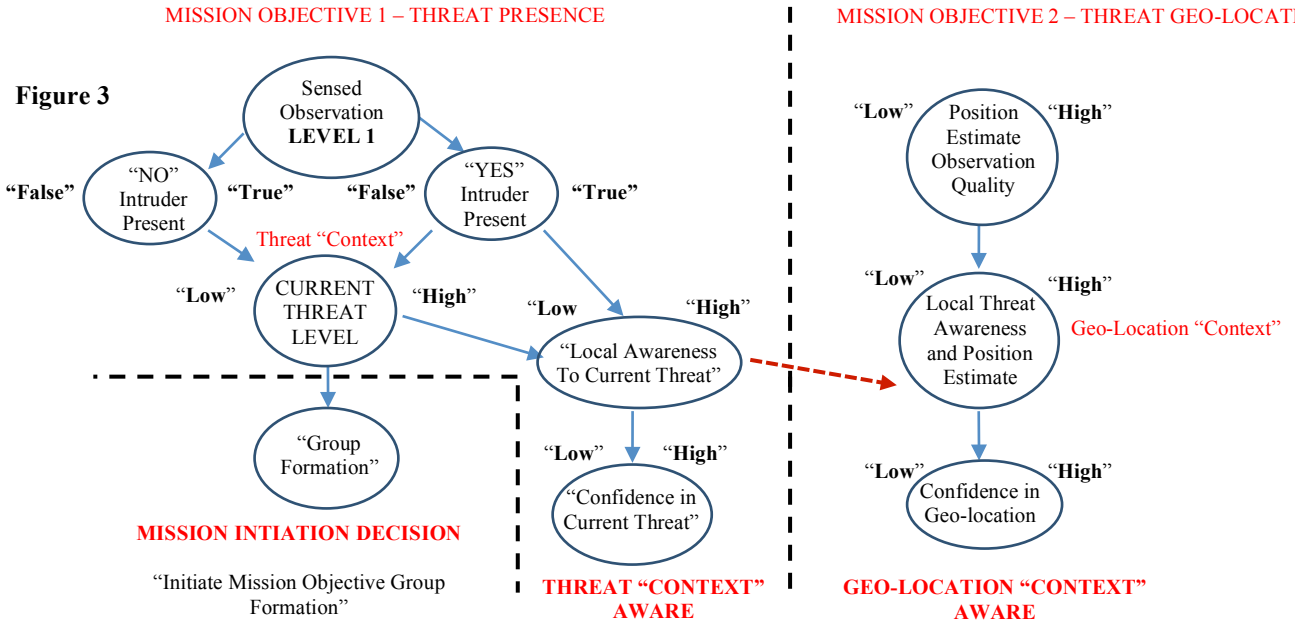


Figure 4

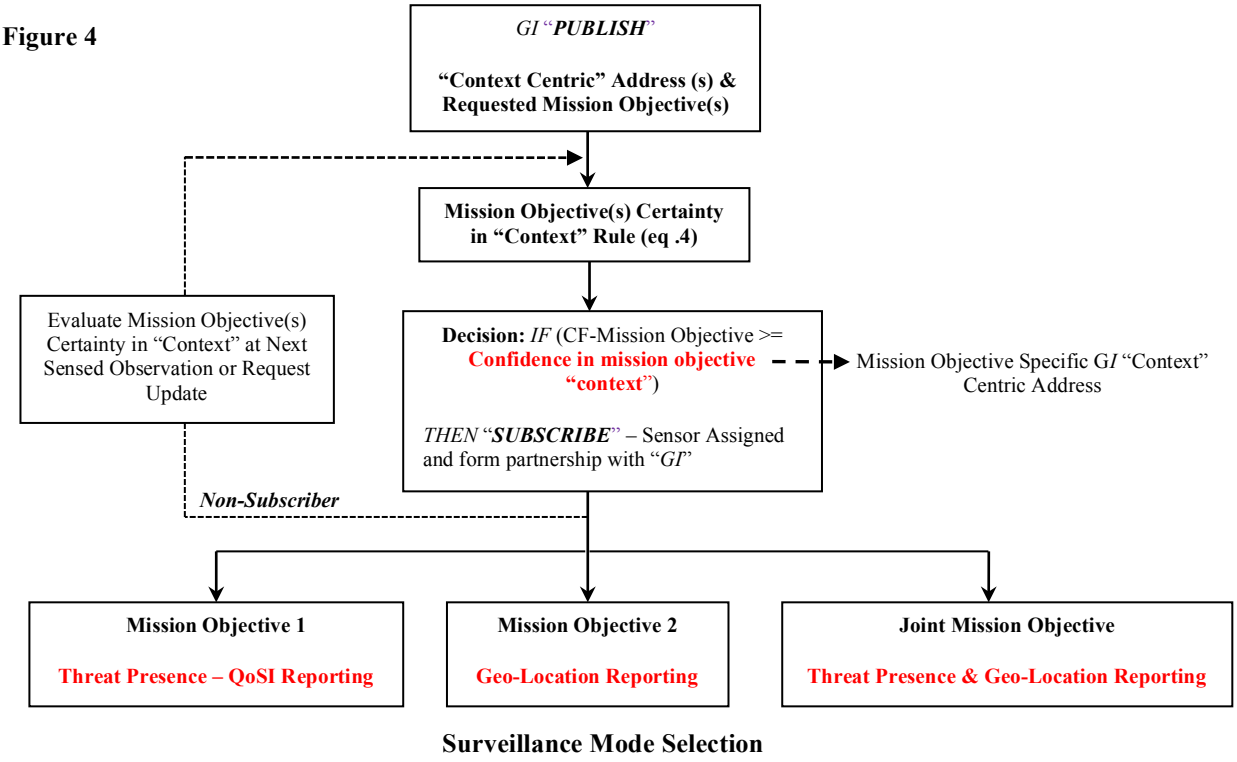


Figure 5(a)

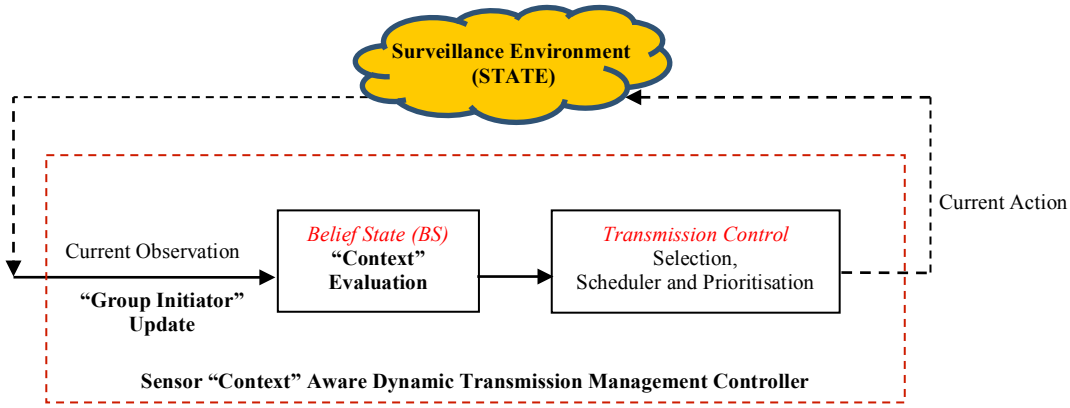


Figure 5(b)

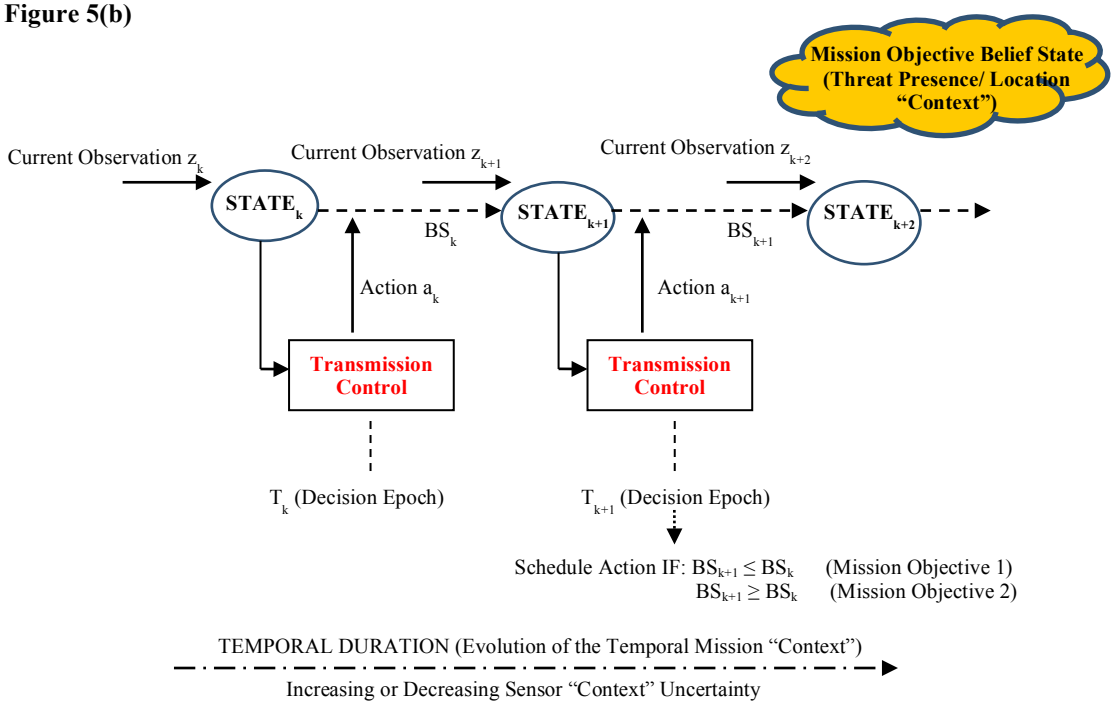


Figure 6(a)

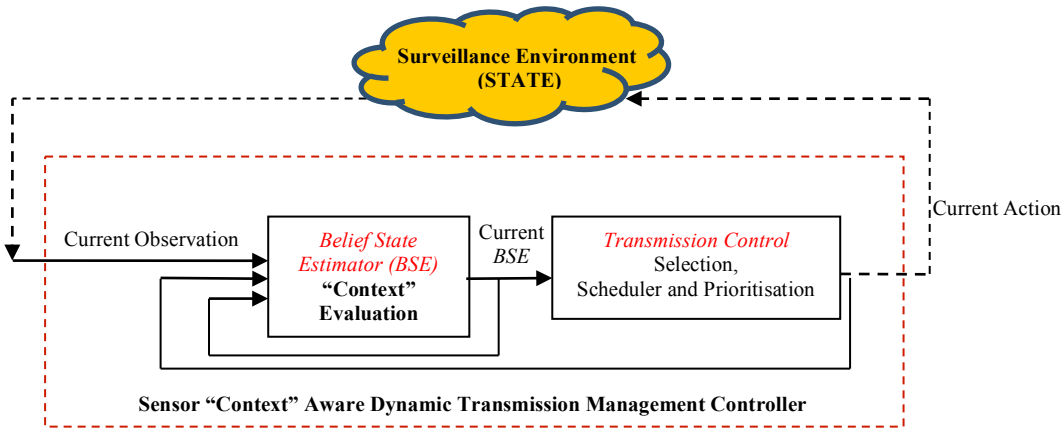


Figure 6(b)

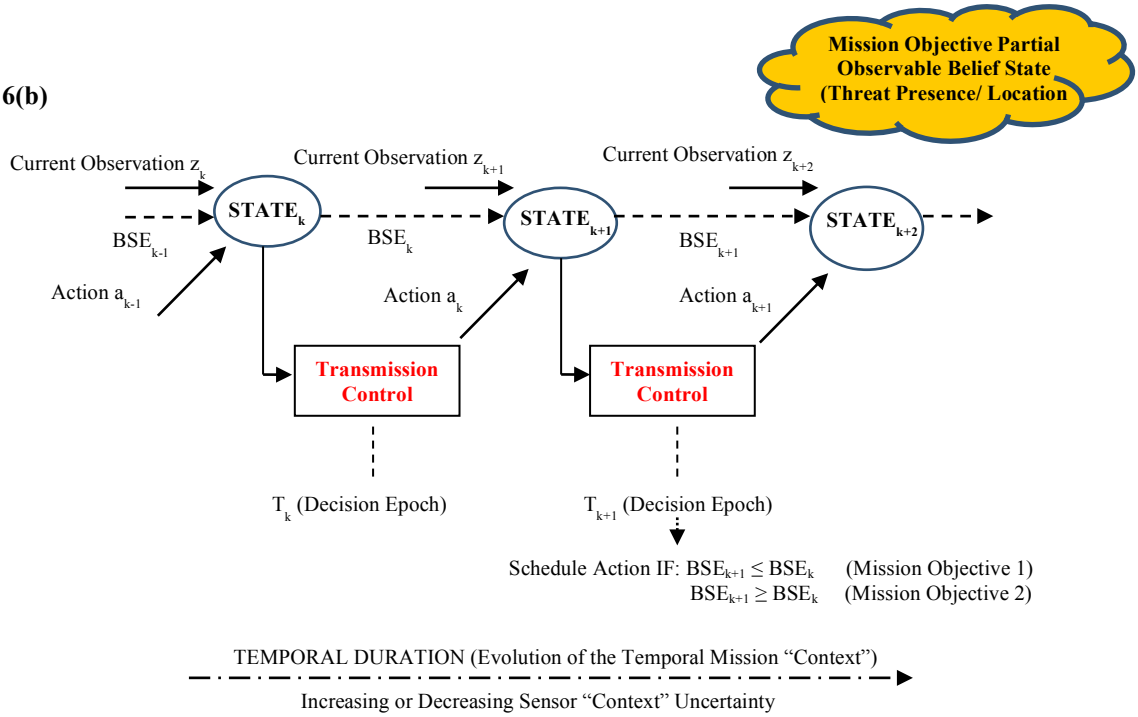


Figure 7

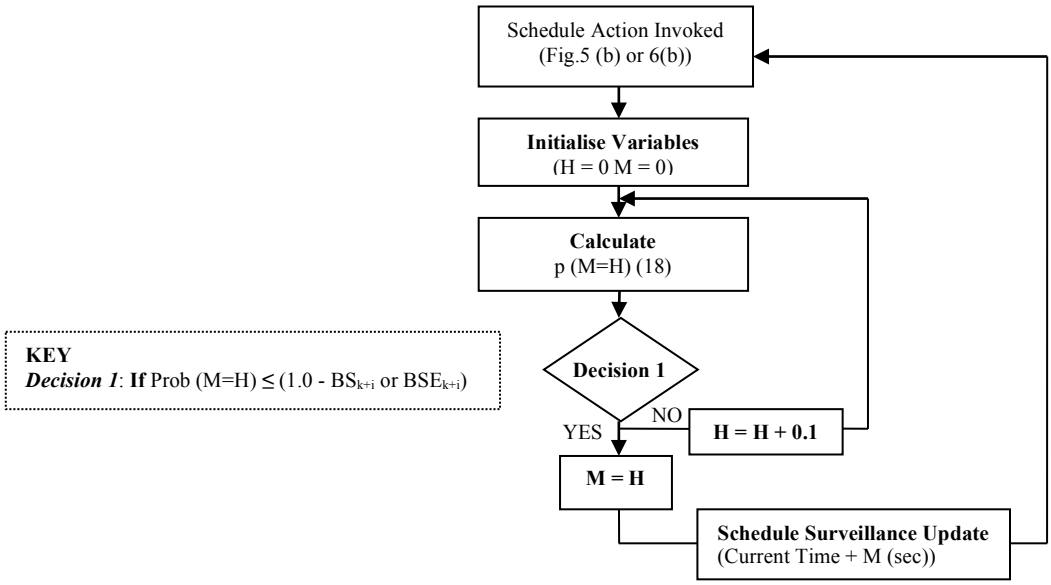


Figure 8

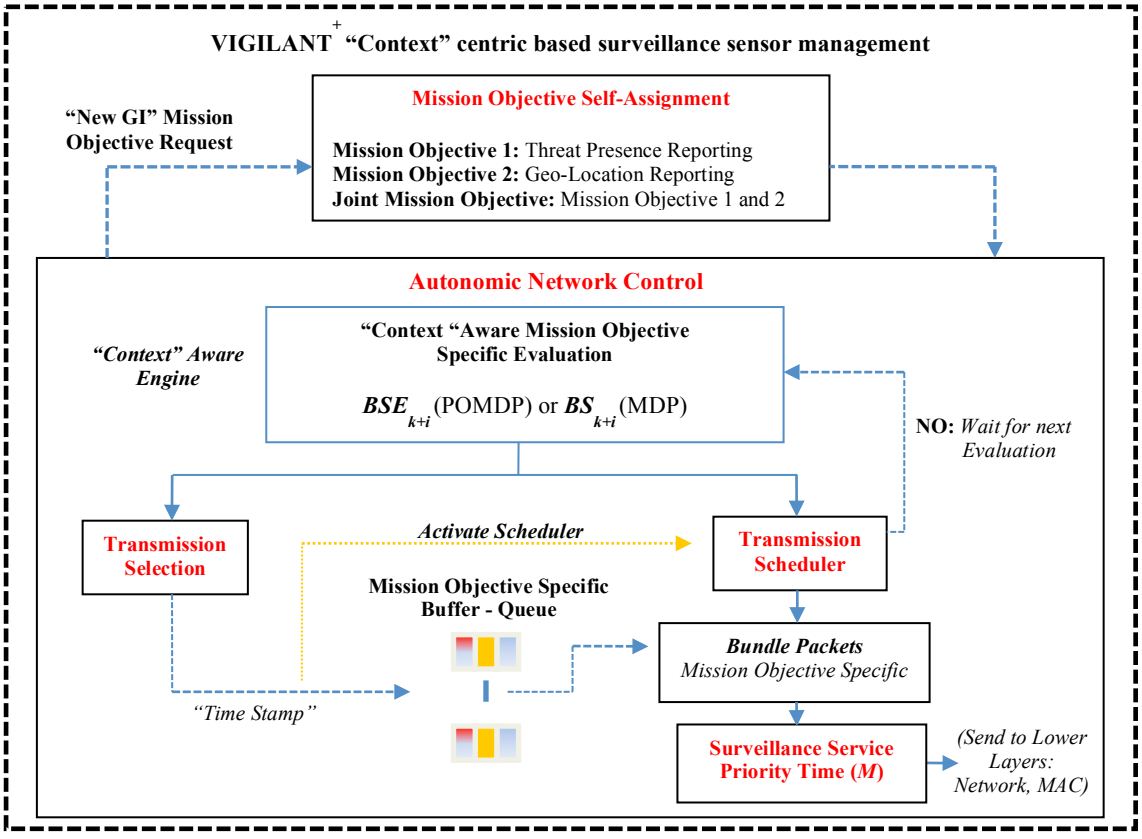


Figure 9

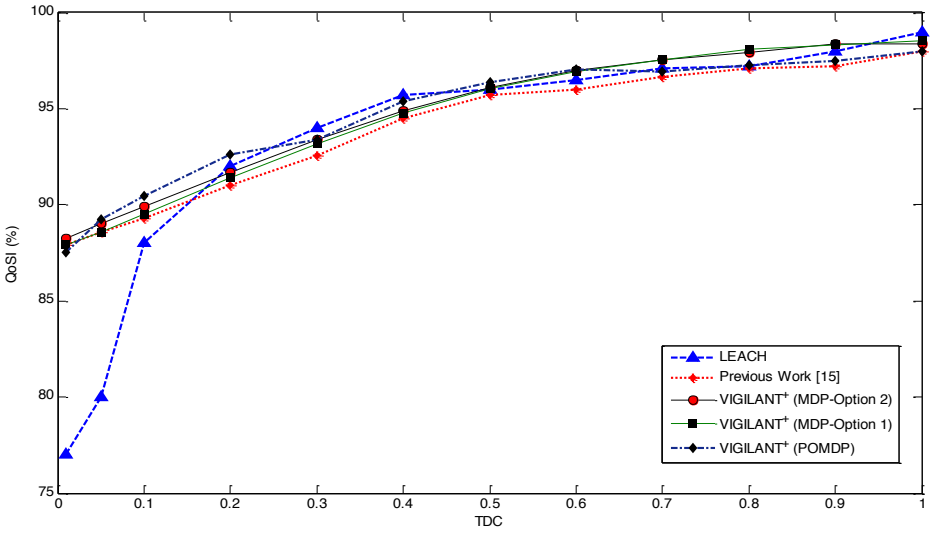


Figure 10(a)

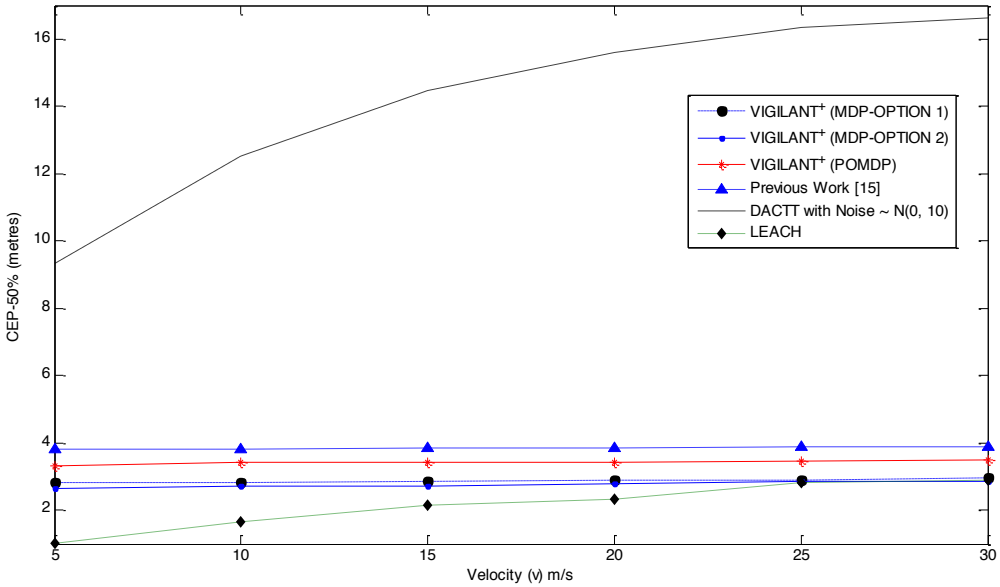


Figure 10(b)

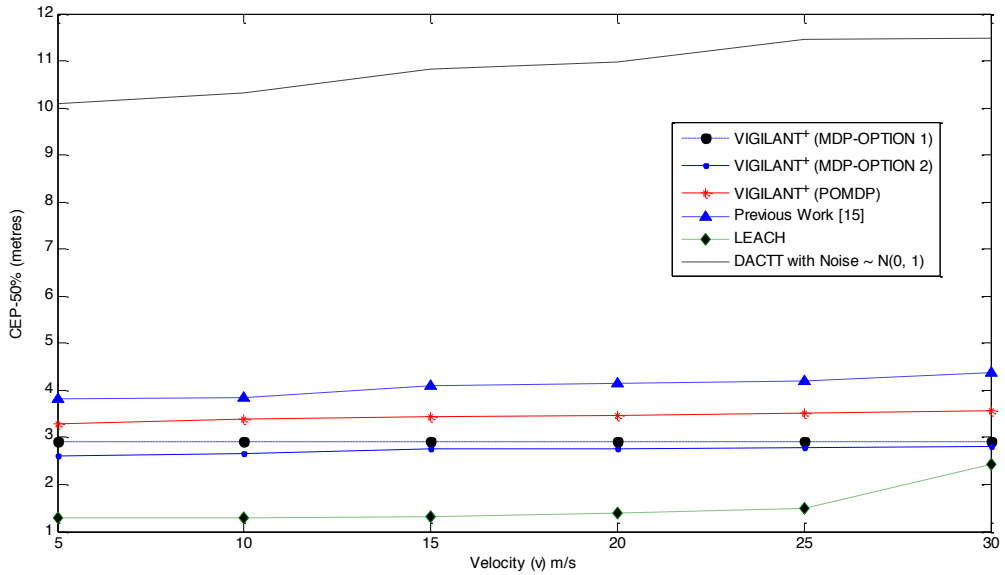


Figure 11(a)

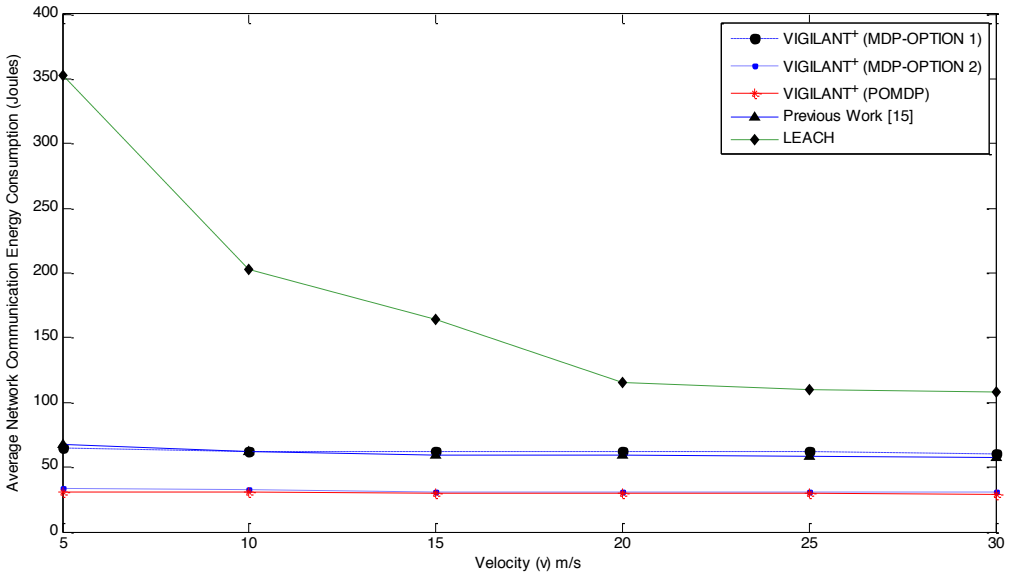


Figure 11(b)

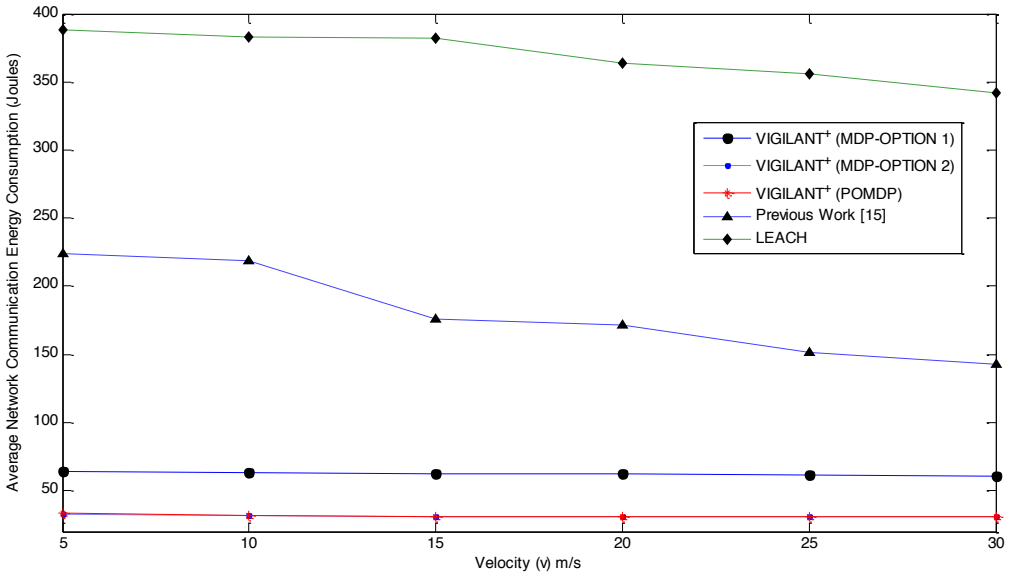


Figure 12(a)

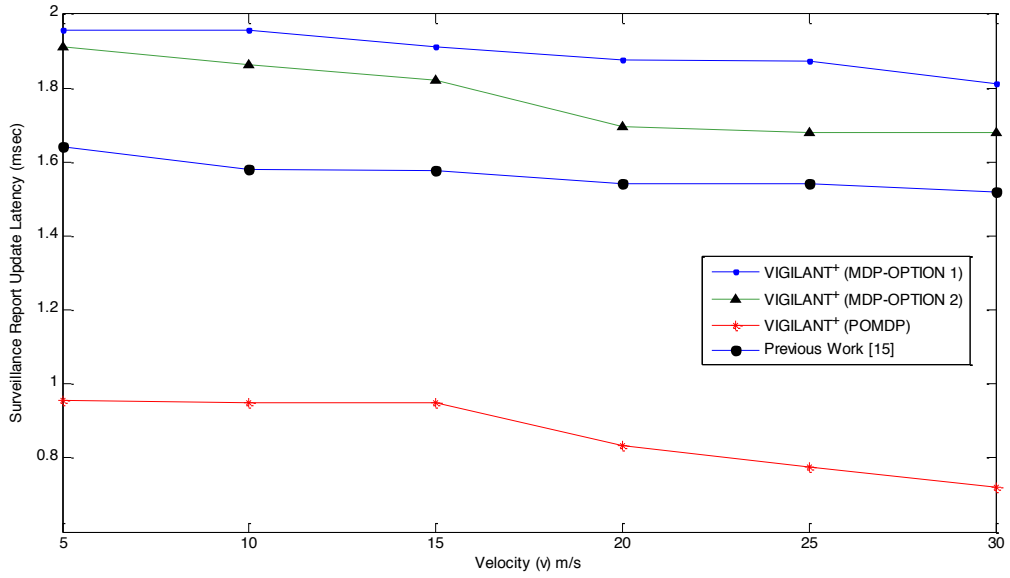
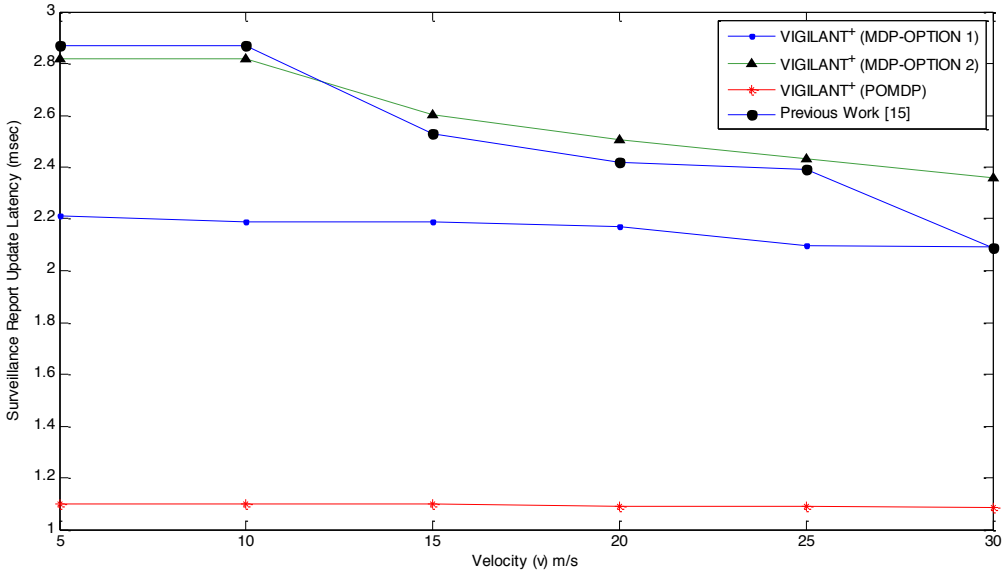


Figure 12(b)


VIGILANT+ (MDP-OPTION 1)
VIGILANT+ (MDP-OPTION 2)
VIGILANT+ (POMDP)
Previous Work [15]
Surveillance Report Update Latency (msec)
Velocity (v) m/s
3
2.8
2.6
2.4
2.2
2
1.8
1.6
1.4
1.2
1
5
10
15
20
25
30