

Networking and Application Interface Technology for Wireless Sensor Network Surveillance and Monitoring

D.S.Ghataoura and J.E.Mitchell, University College London
G.E.Matich, Selex Galileo Ltd

ABSTRACT

Distributed unattended ground sensor (UGS) networks used in battlefield surveillance and monitoring missions, have proven to be valuable in providing a tactical information advantage required for command and control, intelligence, surveillance and reconnaissance planning. Operational effectiveness for surveillance missions can be enhanced further through network centric capability (NCC), where distributed UGS networks have the ability to perform surveillance operations autonomously. NCC operation can be enhanced through networked UGSs having the ability to evaluate their awareness of the current joint surveillance environment, in order to provide the necessary adaption to dynamic changes. NCC can also provide an advantage for UGS networks to self-manage their limited operational resources efficiently, according to mission objective priority. In this article, we present a cross-layer approach and highlight techniques, which have potential to enable NCC operation within a mission-orientated UGS surveillance setting.

INTRODUCTION

Deployments of wireless unattended ground sensor (UGS) networks are primarily used to support mission objective surveillance capabilities such as threat presence detection, classification and geo-location, within a security-sensitive region. The information they generate can enhance decision making abilities for command and control, intelligence, surveillance and reconnaissance (C2ISR) tactical mission planning. From a region of interest (ROI) surveillance perspective, this creates tremendous strategic and tactical advantages for C2ISR operations, through providing a relevant, timely and concise net-centric view, regarding threat monitored activities.

UGS surveillance in para-military mission scenarios present challenges for application and protocol developers because of their dynamic network operating environment. Such environments are characterised by their ad-hoc nature, unstable wireless communication links with limited bandwidth, coupled with a changing threat situation. UGS devices are also inherently limited by their sensing, computation and communication capabilities, which are dictated by their battery energy reserves. Consumption of energy therefore becomes crucial in extending the operational longevity of the overall UGS network field, since deployment of UGS devices may be conducted in

a covert manner, which can prevent devices being accessible for manned battery replenishment for long periods of time [1]. Continuing advances in battery, renewable energy sources and low power computation technologies are however, opening up opportunities for the deployment of autonomous wireless sensor networks [2].

Network Centric Capability for Efficient UGS Surveillance Networking

For a typical UGS surveillance scenario, as shown in figure 1, deployed UGS nodes are required to detect an imminent approaching mobile threat and be able to self-organise, in order to provide timely, relevant and specific mission objective information (e.g. current threat location), as the threat traverses the surveillance field. Information concerning the threat is typically relayed back to a gateway node located within the far-field region of the network and so UGS nodes must also be capable of providing the required routing functionality. Development of protocols and systems to support efficient UGS surveillance network operations, as shown in figure 1, must also be robust within a dynamic and network resource constrained environment, without reliance on any pre-existing centralised infrastructure. Such operations can be assisted by integrating cross-layer self-managing features within deployed UGS networks, which have an ability to perform *agile* decision making in a distributed manner. In essence, UGS nodes which incorporate a distributed *agile* mode of operation exhibit Network Centric Capability (NCC) and can assist to achieve the necessary savings in consumption of network resources, through providing controlled adjustments, in response to dynamic environmental changes, promoting operational longevity [3]. Identifying techniques to support NCC, can, as a result, provide the advantages to support *agile* decision making, while ensuring reliable and timely mission objective information levels are maintained for C2ISR tactical planning purposes.

The main objective of this article is, therefore, to present a potential cross-layer approach to enable UGS NCC surveillance operations, within a dynamic mission-orientated environment, whilst also ensuring the efficient management of operational network resources, as illustrated in figure 2. We initially begin by highlighting the key features that account for cross-layer functionality, within a dynamic surveillance environment, as shown in table 1, which summarises the key features identified during our research activity, in order to achieve UGS NCC operation. This exercise is crucial since it allows the necessary application interface and networking technology research developments to be identified, in support of facilitating and enabling UGS NCC operation, as shown in figure 2. From table 1, requirements 2-4 are further expanded in this article, which details our application interface development, while requirements 5-6 are detailed further, to highlight the networking technologies developed to support routing functionality and adaptability towards an unreliable wireless channel environment, within the UGS network field.

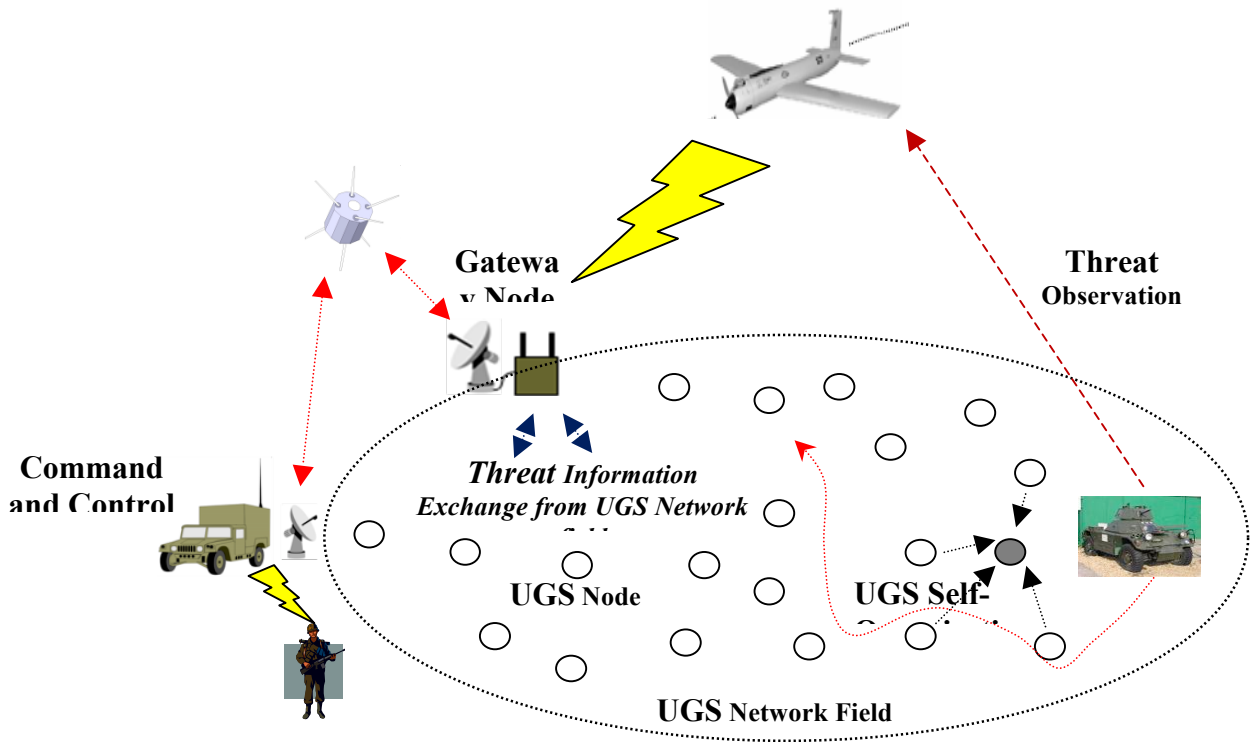


Figure 1. UGS surveillance scenario with links to the wider tactical networking environment

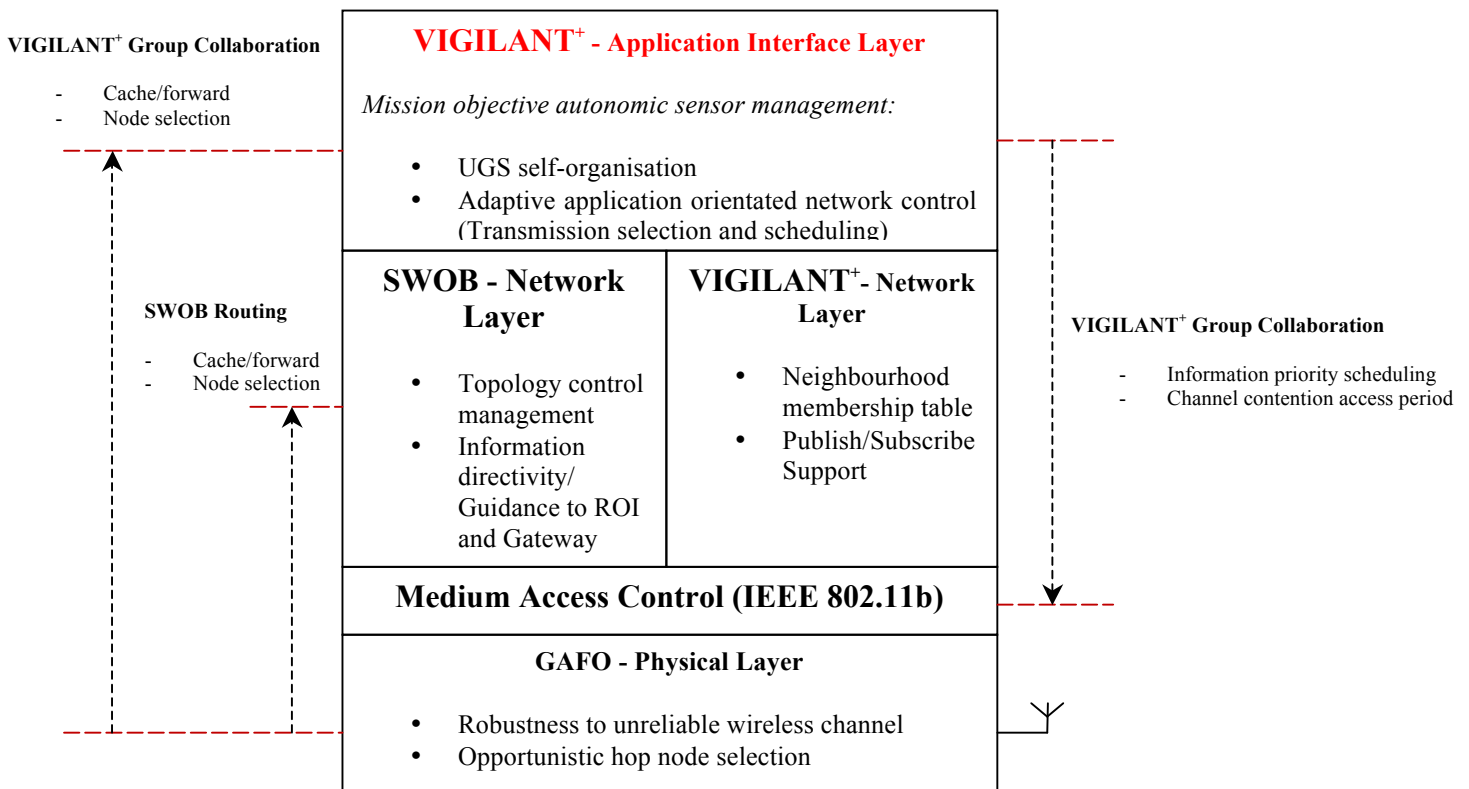


Figure 2. Proposed cross-layer design approach for geographic UGS NCC surveillance operations

Requirement	Key Features
1. Distributed UGS Operation	<ul style="list-style-type: none"> To provide a robust and scalable network infrastructure to significantly improve the reach of information gain for C2ISR tactical planning. Minimising centralised points of failure and performance bottle necks.
2. Threat Perception Quality (<i>Application Interface</i>)	<ul style="list-style-type: none"> Determining sensor data quality, in the presence of ambiguity. The UGS network must ensure that the right information is gathered which meets the needs of a respective mission objective.
3. Information Robustness (<i>Application Interface</i>)	<ul style="list-style-type: none"> Analysing the uncertainty and ambiguity in sensed measurements to convert sensed data into useful relevant mission objective understanding (“<i>context</i>”). Preventing the dissemination of irrelevant surveillance information.
4. Autonomous Surveillance and Tracking (<i>Application Interface</i>)	<ul style="list-style-type: none"> UGS’s supporting a “problem driven collection” approach (e.g. forming groups that can best meet the objectives of a mission such as threat presence and/or geo-location at a particular point in time), based on agile decisions derived from the shared surveillance environment. Self-supporting adaptive network control for mission objective surveillance provision, within network resource constraints.
5. Geographic Routing (<i>Networking</i>)	<ul style="list-style-type: none"> Employing efficient topology control whilst ensuring that information is migrated reliably from the ROI to command and control and vice versa. Information delivery is driven by mission needs, within network environment constraints.
6. Disruption tolerance for surveillance information provision (<i>Networking</i>)	<ul style="list-style-type: none"> Making optimal choices for robust packet transmission. Providing a channel aware decision making capability, to support reliable node selection for information forwarding.

Table 1. Requirement and key feature analysis for UGS NCC operation as shown in figure 2, for a typical surveillance scenario depicted in figure 1

Sections in this article are accordingly presented to expand on figure 2 and supplement the analysis made in table 1. Section 2 of this article reviews the general distributed nature of UGS operation. Section 3 presents an approach for allowing UGS self-management, according to a dynamic mission objective surveillance situation. Section 4 presents a bio-inspired geographic routing protocol to support migration of surveillance information, within the UGS network field. Section 5 presents a technique to facilitate reliable node selection for information forwarding, within an unreliable communication link environment. The final section concludes the article and draws attention to the cross-layer approach proposed, for efficient UGS NCC surveillance operation.

DISTRIBUTED UGS SURVEILLANCE OPERATION

In this section, we introduce the necessary steps towards enhancing distributed UGS NCC operation as detailed by requirement 1, in table 1, suitable to the surveillance scenario illustrated in figure 1.

The inherent dynamic nature of surveillance missions does not allow time for manual system configuration, especially within an unreliable, bandwidth-limited communication environment. Distributed systems can address this concern through minimising the burden for centralised architecture and points of failure, including the reduction in communication overhead. A distributed architecture allowing for UGS self-management, whilst maintaining the mission objective surveillance capabilities necessary for C2ISR tactical planning, is therefore essential.

Distributed Situation Awareness

Situation awareness (SA) is an integrated approach involving the perception of environmental entities within an uncertain, dynamic volume of time and space, the comprehension of their meaning and lastly, the projection of their status in the near future. SA is an effective methodology to fulfil the critical NCC application interface elements, required for *agile* decision making in operational military surveillance scenarios, as shown in figure 2.

A useful representation describing three levels, which can contribute towards awareness of a current surveillance situation, is provided through Endsley's "tripartite" model [4]:

- **Level 1-Perception-**
involves the correct identification of the environmental entity (e.g. type and mode of threat) as well as their combined characteristics (e.g. detection accuracy, certainty and timeliness). This represents an aggregated measure regarding the current threat detection characteristics captured from the surveillance environment, by the distributed UGS network.

- **Level 2-Comprehension**-involves derivation of the significance associated with fragmented sensor data and confidence in understanding (“*context*”) about the uncertain surveillance environment, to enable relevant decision making outcomes (e.g. Initiating UGS group self-organisation).
- **Level 3- Projection**-the ability to project future “context” of the surveillance environment based on the association of fragmented sensor data within a temporal frame.

Deployed UGS’s employing distributed SA perspective, with the ability to self-organise into dynamic ad-hoc groups after evaluating their common “context” (e.g. evaluating the level of common threat presence awareness within the UGS field) , can subsequently provide C2ISR a relevant, informed view as to unfolding events. This facilitates operational effectiveness, by improving the quality of C2ISR decision making through increased information relevancy and utility, while minimising on transmission of redundant and unreliable information.

Unmanned Vehicle Operations to Support Surveillance Capability

Unmanned ground and air vehicles are becoming increasingly common in military operations. With the use of unmanned assets increasing, the importance of their use in supporting distributed UGS surveillance operations increases as well. This is illustrated in figure 1, where unmanned air vehicles have the potential to perform airborne surveillance and to notify deployed UGSs within a relevant geographic ROI to initiate sensing operations, due to an incoming threat. This prevents continuous sensing operations being conducted across the deployed UGS network field, saving on sampling energy consumption. An additional benefit of using this approach is that only those UGSs relevant to the ROI are utilised enabling relevant sensing coverage, to verify airborne threat observations and fulfil current mission objectives. Additionally, such capability focuses further research efforts in developing collaborative behaviours, where multiple deployed unmanned assets cooperate, in order to accomplish required mission objectives.

Geographic Directed Queries

In typical military surveillance scenarios, as shown in figure 1, possible threats, which are identified using airborne reconnaissance are usually constrained to a specific geographic region. Generation and migration of information queries from command and control can therefore be restricted to where information is most geographically pertinent at that specific time. UGS nodes that are aware of their geographic position within the surveillance field, can accordingly facilitate routing protocol development in support of this activity by using publish/subscribe mechanisms, relevant to the specific geographic information request (e.g. current coordinates

of where a threat might be approaching within the UGS network field). Geographic driven queries offers better network management through geographic partitioning since:

- This focuses C2ISR efforts for surveillance provision needs concerning a current threat (e.g. classification, current location and future track of threat) to a specific identified geographic ROI, therefore increasing the utility in information received for C2ISR tactical planning purposes.
- Deployed UGS nodes, which are distant concerning the current threat in terms of geography can therefore conserve on sampling energy consumption, since they are more likely to decrease overall required information relevancy.

VIGILANT⁺: MISSION OBJECTIVE AUTONOMIC SENSOR MANAGEMENT

UGS NCC surveillance operations require systems that can self-manage mission-objective priorities in a distributed manner, within network resource consumption constraints. In this section, we present our developed VIGILANT⁺ system [5] derived from our previous work [6], which adopts a distributed SA approach to allow UGS self-management, as shown in figure 2. The performance evaluation scenario conducted in [6] to support our current VIGILANT⁺ work concerns monitoring a single mobile threat moving at a constant velocity, v m/s, with a diagonal trajectory. VIGILANT⁺ mission objective capabilities supported are for threat presence detection and threat geo-location. Geo-location performance is measured in terms of *Circular Error Probable-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. The evaluated scenario is based on using a total of 10 UGS nodes deployed randomly, within a 1km by 1km ROI, using a sampling rate of 100 Sa/sec, sensing range of 1000m, transmission range of 500m and IEEE 802.11b in basic access mode, for medium access control.

In figure 3, VIGILANT⁺ illustrates how utilising a distributed SA methodology can provide a control mechanism towards managing transmission resource consumption, through adaptive networking according to the mission objective environment. Accordingly, by ensuring UGS nodes can first create their own awareness (level 1 and 2) towards a current mission objective priority and share this awareness with their neighbourhood, decisions can be made as to when information should be scheduled for transmission, concerning the monitored threat. As shown in figure 3, our VIGILANT⁺ system firstly allows for self-organisation of UGS nodes to form groups, which can meet the needs of a current and specific mission surveillance capability, within environmental sensing constraints (false alarms). Secondly, we incorporate a methodology to enable autonomic network

control for efficient management of communication resource consumption, without compromising on mission objective utility.

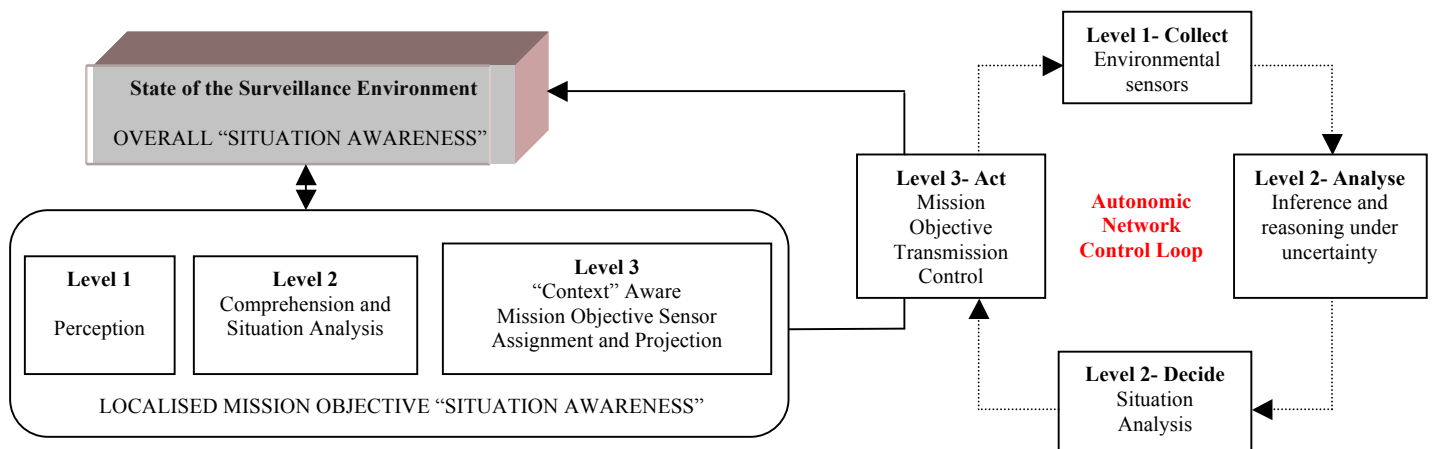


Figure 3. *VIGILANT⁺ approach to agile self-managed informed networking, to support the application interface layer, as shown in figure 2*

Level 1- Perception

False alarms have a distinct impact on level 1 perception performance, since it affects the ability for UGS nodes to detect and ascertain correctly whether a threat is present or not. A low false alarm rate, which is needed to avoid unnecessary responses (e.g. incorrect decision to invoke UGS group self-organisation), 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 towards capturing relevant information, while accommodating to the varying uncertainties present within the sensing environment, is therefore beneficial. Our evaluated situation assessment system, PORTENT [7], represents level 1 perception, accommodating the necessary sensitivity adjustment process needed to support requirement 2, detailed in table 1.

Level 2- Mission Objective Surveillance Comprehension and Analysis

Mission objective situations occurring in an uncertain environment also require a level of cognition to derive understanding (“*context*”) of those situations. Derived “*context*” is used to ascertain the level of confidence a UGS node might have towards a mission objective, in order to fulfil the required threat presence detection and geo-location capabilities. VIGILANT⁺, utilises an action orientated design approach, in the form of a Bayesian Belief Network (BBN) to support requirement 3, detailed in table 1. A BBN is a directed acyclic graph, using a collection of nodes denoting the random variables representing the mission objective surveillance domain (e.g. “Yes” threat present or “No” threat present). Random variables that are related to a specific mission objective

are linked together, in order to form an overall descriptive picture concerning the threat presence detection or geo-location operation. Corresponding links between nodes define the casual relationships between them, with conditional probability tables (CPTs) encoding the quantitative influence. Relevant probability derivations obtained from the designed BBN, can be appropriately applied for making agile “*context*” based decisions at local UGS level, concerning the current mission objective situation. Decisions based on “*context*” can assist UGS nodes to establish, which mission objective should be addressed at a particular point in time, so that correct and timely information concerning the threat (e.g. current location) can be provided for C2ISR tactical planning purposes.

Autonomic Self-Organisation

VIGILANT⁺ self-organisation is focused primarily on the combination of perception (level 1) and relevant derivation of “*context*” (level 2) about the current surveillance situation, in order to allow UGSs to autonomously decide whether to assign themselves to either threat presence, geo-location or a combination of both mission objectives. Self-assignment can be restricted to publish/subscribe querying about common certainty in mission objective “*context*”, supporting the need for a “*problem driven collection*” approach, as detailed in requirement 4, in table 1. Certainty concerning the “*context*” of a current mission objective can be established using reasoning methods such as the certainty-factor model [8].

Publish/subscribe querying on mission objective “*context*” enforces uncoupled coordination, where distributed UGS nodes are modelled as sets of components interacting with each other through analysing and reacting to their mission objective “*context*” independently. This supports flexibility through asynchronous communication, as well as scalability for UGS NCC surveillance missions. Publishing of queries to invoke UGS self-organisation can be managed according to the group initiator (GI), this being the UGS, which perceives the current threat presence to be highest within the neighbourhood, derived from level 2 BBN probabilistic evaluations.

Ad-hoc group self-organisation of UGS’s can therefore be enhanced by querying and assigning sensors that have common certainty in “*context*” to a specific mission objective. Communication efficiency is also improved by relying on mission objective “*context*” instead of traditional IP-style addressing, promoting in-network processing to provide further savings in bandwidth consumption.

Autonomic Network Control

Autonomic network control is orientated towards the management of network resources at infrastructure level, through monitoring temporal environmental dynamics, as shown in figure 2. Being efficient in terms of 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) [9]. Being in a particular state signifies an evaluation of the current shared mission objective “*context*”. An evaluation of shared “*context*” involves ascertaining the level of shared understanding that two UGS nodes may have towards a specific mission objective (e.g. current threat presence detection or geo-location) at that point in time. Through evaluating shared “*context*” the necessary feedback can then be applied within a temporal setting, for adaptive transmission control (selection, scheduling and prioritisation) decision making.

VIGILANT⁺ employs a priority-based transmission scheduling algorithm, which operates according to the current shared mission objective “*context*”. Scheduling according to shared mission objective “*context*”, with respect to a current GI, allows individual UGS nodes to access the channel at periods, which are unique to it rather than pre-defined, in order to facilitate the need for frequent or non-frequent UGS updating. Scheduling of channel access periods that are less frequent in nature, therefore implies a lower urgency in surveillance updating, since there is less uncertainty associated with the shared “*context*” regarding the presence or geo-location accuracy (in terms of geometric dilution of precision) concerning the common perceived threat, which further provides the necessary savings in communication energy and bandwidth consumption.

SWARM INTELLIGENT ODOUR BASED ROUTING

In this section we present our Swarm Intelligent Odour Based (SWOB) routing protocol [10], to solve requirement 5, detailed in table 1. SWOB is a geographic routing protocol, with added topology control capability, for supporting geographic directed information queries within the UGS network field, when location information of the deployed UGS nodes is available.

SWOB uses UGS network topology and geographic location information to effectively coordinate the routing tasks, for information requests and surveillance provisioning packets to traverse the network. Using geographic topology to support routing activities in an UGS surveillance scenario is efficient for several reasons. For one, UGS nodes need to know only the location of their direct neighbours and the final destination, in order to forward packets. Further geographic routing protocols conserve energy and bandwidth since discovery floods and the forwarding of routing state propagation tables are not required beyond a single hop. The main component of geographic routing is usually a *greedy* forwarding mechanism, whereby each UGS node forwards a packet to the neighbour closest to the destination.

Biological Inspiration

SWOB itself takes its inspiration from the basic principles and examples provided by social insects in odour localisation and tracking. A wide variety of insects use plumes of pheromone (odour) to locate prey, mates and other sources of particular interest. Insects themselves follow a route by means of *olfactory sensing* to regions of higher pheromone concentration, since this represents a higher order of relevance in finding the required designated odour source. Within an UGS surveillance scenario, illustrated in figure 4, odour sources are represented by an identified threat ROI's or gateway node location coordinates.

Virtual Odour Plume

In natural circumstances odour plumes are determined by the physics of atmospheric dispersion formed as the odour molecules are dispersed from their source. Naturally, the concentration of odour is highest at the odour source and diffuses further away from the source. The Gaussian model of diffusion is a widely used and accepted model to portray natural odour dispersion phenomena, since it describes neatly what is experienced in the real world, for a range of conditions [11]. For the purpose of this study, we assume a 2 dimensional Gaussian function to model odour concentration levels at any UGS node coordinate position (x,y) within the network region, given by $C(x, y)$, as shown in figure 4.

SWOB Forwarding Strategy

SWOB forwarding is based on a localised algorithm. Utilizing a localised process has the advantage of not relying on centralised control mechanisms. Therefore, the failure of UGS nodes and communication links does not result in catastrophic failure, but rather leads to graceful, scalable degradation. Each UGS node makes a decision as to which neighbour to forward information to, based only on the location of the destination (odour source) and its local virtual odour concentration level $C(x, y)$.

In this sense UGS nodes behave in *greedy mode*, where the node currently holding an information packet may “advance” it toward the destination. The “advance” in this sense, is defined according to the Gaussian odour plume function. In this case packets are forwarded in a unicast fashion to nodes that represent higher levels of odour concentration, $C(x, y)$, dictated by their geographic position in relation to the final destination (odour source) within a nodes neighbourhood, as shown in figure 4.

SWOB Topology Control

Topology control through a virtual odour plume, presents advantages in communication efficiency, since UGS nodes outside the virtual odour plume do not contribute to forwarding tasks. UGS nodes not contributing to forwarding tasks can conserve on energy consumption and as a result will not compete for bandwidth resource, as shown in figure 4. Plume shape characteristics (breadth of plume) governing UGS node forwarding tasks can

be matched to the characteristics of the deployed network, such as neighbourhood node density, as currently the case with SWOB [10]. This implies the breadth of a plume can be adapted, to ensure UGS nodes have at least k neighbours to communicate with, in order to avoid node isolation [10]. Further, research, however needs to be conducted in ensuring plume characteristics are also dynamic to the current communication conditions, which is unpredictable in nature, in order to ensure packets are forwarded reliably.

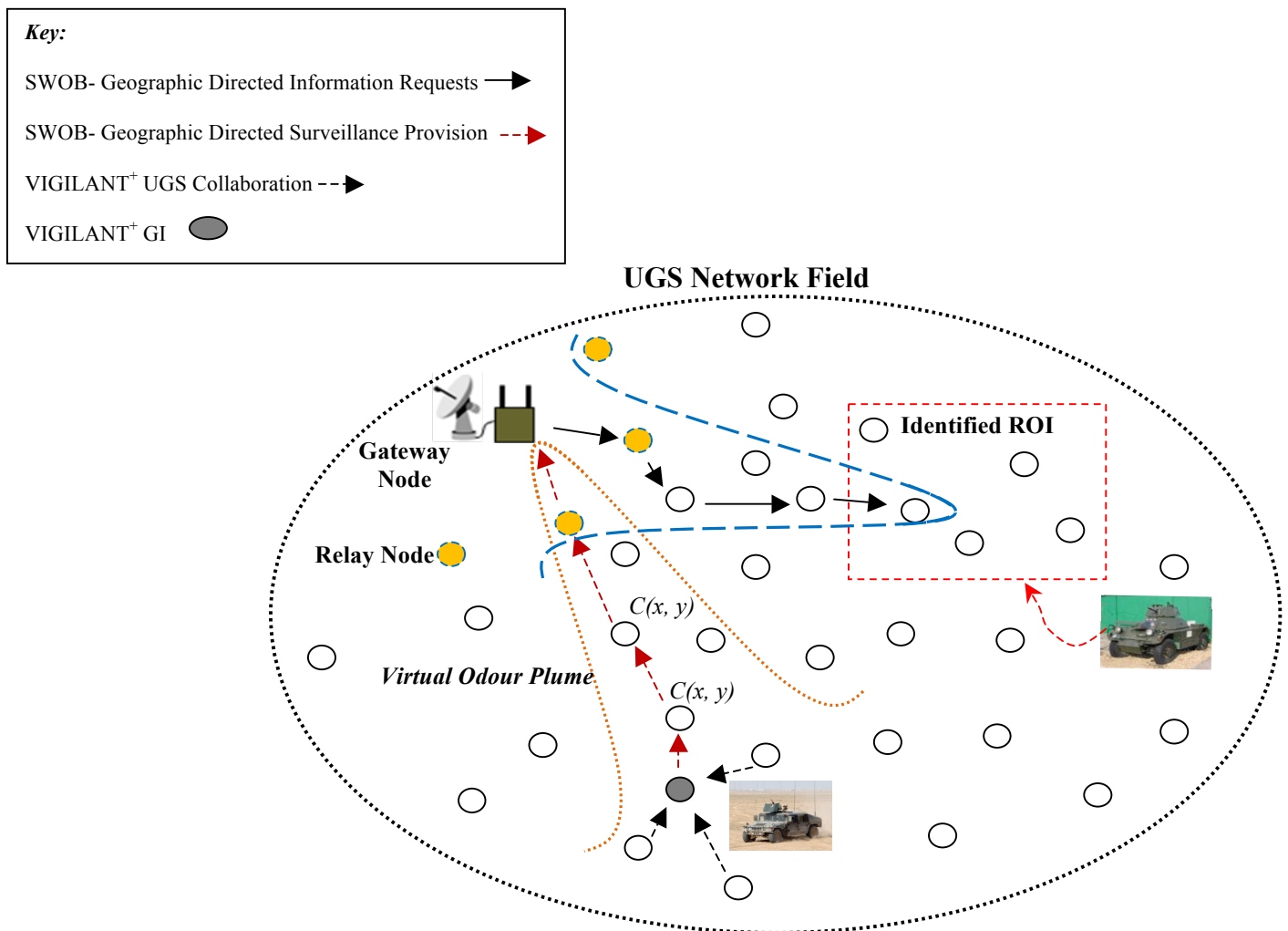


Figure 4. SWOB routing in support of distributed UGS geographic surveillance operation, to support requirement 5, table 1, as shown in figure 2

GENETIC ADAPTIVE FUZZY LOGIC NODE SELECTION

For UGS nodes operating in varying channel conditions, packet transmission reliability can be affected. Within a static UGS multi-hop network, varying channel conditions can make the existing point-to-point route to become invalid, before an alternative route can be chosen (*topology re-configurability*). The loss of nodes to link instability can therefore result in significant topological changes and reorganization of the network. Making

robust, adaptive and informed decisions on node selection for information forwarding as a result of link instability becomes an important issue.

In this section, we present our developed **Genetic Adaptive Fuzzy Logic (GAFO)** node selection scheme [12], as shown in figure 5, to support requirement 6, detailed in table 1. The main purpose of GAFO is to evaluate node-to-node link connectivity based on received link reliability measures (signal to noise ratio (SNR) and packet reception probability (PRP)) within the neighbourhood, so that reliable packet forwarding decisions (node selection) can be established.

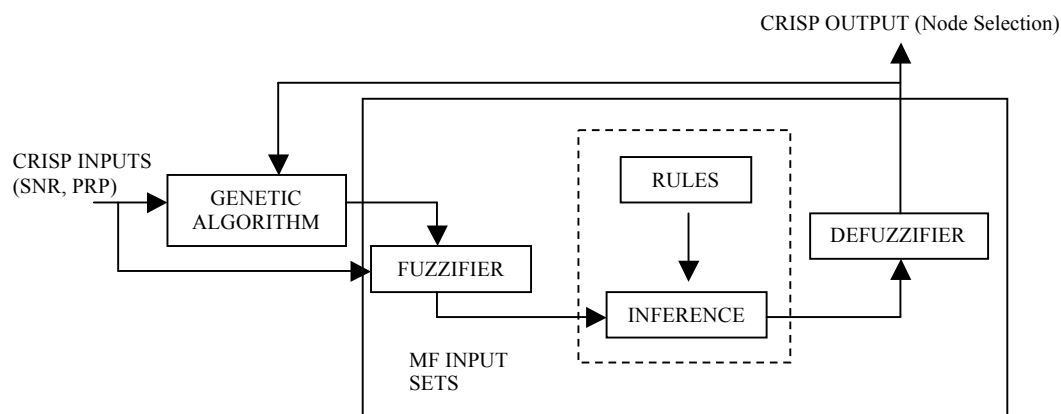


Figure 5. GAFO system structure for node selection to support requirement 6, table 1, as shown in figure 2

GAFO node selection exploits the inherent broadcast nature of wireless networks to decide on connectivity opportunities, to support dynamic information forwarding. Information packets en-route between sender and destination can therefore utilise UGS nodes *opportunistically* as the next hop, if it is likely to bring the packet closer to the final destination.

Forwarding information in this manner is based on UGS nodes storing (*cache*) information packets they have to forward until a UGS node deemed more suitable at a particular time, becomes available. Topology re-configurability therefore plays a crucial role, as it permits disconnected UGS nodes to forward information opportunistically, which ultimately enables end-to-end communications despite connectivity impairments.

Genetic Adaptability

Using both SNR and PRP as input parameters, provides suitability for dealing with unreliable communication environments, as well as for guiding the decision making process, as shown in figure 4.

Uncertainty of the channel environment is essentially characterized by the input *membership functions* (MFs) sets. Since MFs serve as a representation of the channel dynamics for the inference engine, GAFO utilises a

genetic algorithm to improve on hop selection performance, by tuning input MFs to match current received link conditions. GAFO focuses on tuning the parameters defining each MF, thus adapting their shape to reflect current received channel characteristics, influencing system performance in deciding on node selection, to facilitate reliable information packet delivery.

Using GAFO to support an information cache-forward approach offers advantages for surveillance missions, in disruptive environments since:

- Nodes are encouraged to behave opportunistically in discovering reliable connectivity, therefore increasing transmission packet success, which affects eventual surveillance provision utility.
- Only a select number of nodes with reliable channel link quality will be competing for available bandwidth.
- Nodes with unreliable link quality can cache more and not transmit immediately, improving on communication energy consumption.

CONCLUSION

Efficient UGS surveillance operations require systems that can self-manage mission objective priorities autonomically in a distributed manner, within both an uncertain situational and network resource constrained environment. A self-managed approach towards achieving efficiency in operations requires *agility* in UGS decision making ability, supporting the notion of a NCC environment. In this article we have presented our researched opinions and techniques, which provide the potential to facilitate NCC in an UGS mission orientated surveillance environment. Further experiments are to be conducted within a surveillance mission scenario, in order to fully test and verify the efficiency benefits proposed in our cross-layer approach.

ACKNOWLEDGMENT

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

REFERENCES

- [1] E.Onur et al., “Surveillance Wireless Sensor Networks: Deployment Quality Analysis”, *IEEE Network*, December 2007, vol.21, no.6, pp. 48 -53, December 2007.
- [2] Eiko Yoneki, “A Survey of Wireless Sensor Network Technologies: Research Trends and Middleware’s Role”, *Technical Report UCAM-CL-TR-646*, University of Cambridge Computer Laboratory, pp.1-46, September 2005.
- [3] S.Geyiks et al., “Dynamic Service Composition in Sensor Networks”, *7th IEEE International Conference on Services Computing (SCC 2010)*, Miami, USA, pp. 242-249, July 2010.

- [4] M.R Endsley, "Toward a Theory of Situation Awareness in Dynamic Systems", *Journal of Human Factors*, vol. 37, no.1, pp.32-64, 1995.
- [5] D.S Ghataoura, J.E Mitchell, G.E Matich, "VIGILANT⁺: Mission Objective Interest Groups for Wireless Sensor Network Surveillance Applications", *Submitted to the IET Wireless Sensor Systems Journal*, March 2011.
- [6] D.S Ghataoura, J.E Mitchell, G.E Matich, "VIGILANT: "Situation-Aware" Quality of Information Interest Groups for Wireless Sensor Network Surveillance Applications", *European SPIE Security and Defence, Unmanned/Unattended Sensors and Sensor Networks VII*, vol. 7833, September 2010.
- [7] D.S Ghataoura, J.E Mitchell, G.E Matich, "PORTENT: Predator Aware Situation Assessment for Wireless Sensor Network Surveillance Applications", *SPIE: Defence, Security and Sensing, Information systems and networks*, vol.7709, April 2010.
- [8] P Krause, "Representing Uncertain Knowledge", *Intellect Books*, 1st Edition, pp. 52-66, 1993.
- [9] O.H Lerma, "Adaptive Markov Control Processes", *Springer-Verlag*, New York, 2001.
- [10] D.S Ghataoura, Y.Yang, G.E Matich, "Swarm Intelligent Odour Based Routing for Geographic Wireless Sensor Network Applications", *Proc. of IEEE MILCOM '09*, Boston, USA, October 2009.
- [11] B.Turner, "Workbook of Atmospheric Dispersion Estimates: An Introduction to Dispersion Modelling", *Lewis Publication*, 2nd Edition, CRC Press, 1994.
- [12] D.S.Ghataoura, Y.Yang, G.E Matich, GAFO: Genetic Adaptive Fuzzy Hop Selection Scheme for Wireless Sensor Networks, *IWCMC 2009 Wireless Sensor Networks Symposium*, Leipzig , Germany, 21st -24th June 2009.

BIOGRAPHIES

DARMINDER SINGH GHATAOURA (dghataou@ee.ucl.ac.uk) is currently in the final year of his EngD at University College London, U.K. He received his MEng with honours in electrical and electronic engineering from the University of Nottingham, U.K, in 2005. Prior to beginning his EngD he spent two years at QinetiQ plc (Malvern and Farnborough), U.K, as a communications network engineer with responsibilities on aspects of system design, build and test for various military airborne platforms. His current research interests include sensor networking, network management, development of protocols for distributed systems and agility support for dynamic networking environments.

JOHN MITCHELL (jmitchel@ee.ucl.ac.uk) received the Ph.D. degree in Electronic Engineering from UCL (University College London), UK in 2000. In 1999 he became a Research Fellow in the Department of Electronic and Electrical Engineering at UCL (University College London), becoming a Lecturer and Senior Lecturer in 2000 and 2006 respectively. His research interests cover optical and wireless communications technologies with specific interest in wireless sensor network hardware, protocols and applications. He has been involved in developing systems for a variety of applications including Medical, Industrial and Defense working with a number of industry and academics partners. Dr. Mitchell is a Chartered Engineer and a Member of the Institute of Engineering and Technology (IET) and the IEEE Communications Society.

GEORGE MATICH (george.matich@selexgalileo.com) is the Chief Technologist (Communications and Network Systems) at SELEX Galileo Limited which is part of the Finmeccanica Company. In his current role he is responsible for the company's applied research activities in the network systems domain and manages its associate relationship with Academia and the Government research establishments. He has been in the defence electronics systems industry for some thirty years after starting his career with GEC Marconi. During his time he has held many senior engineering positions including that of chief engineer on the GTE AIRPHONE project. He has also worked with the UK-CAA/US-FAA in consultancy role during the development of the next generation digital radio communication system for ATC (VDL). George is named as the inventor on 4 patents and has held his current position in the applied research team within SELEX Galileo for the past 10 years, during which time he has published and presented papers to IET, ICAO and various industry symposia. In his current role he also has liaison responsibilities with the European Commission ICT team in the area of cooperating objects.