Intelligent Route Surveillance

Robin Schoemaker*, Rody Sandbrink, Graeme van Voorthuijsen
TNO Defence, Security and Safety, P.O. Box 96864, 2509 JG, The Hague, The Netherlands

ABSTRACT

Intelligence on abnormal and suspicious behaviour along roads in operational domains is extremely valuable for countering the IED (Improvised Explosive Device) threat. Local sensor networks at strategic spots can gather data for continuous monitoring of daily vehicle activity. Unattended intelligent ground sensor networks use simple sensing nodes, e.g. seismic, magnetic, radar, or acoustic, or combinations of these in one housing. The nodes deliver rudimentary data at any time to be processed with software that filters out the required information. At TNO (Netherlands Organisation for Applied Scientific Research) research has started on how to equip a sensor network with data analysis software to determine whether behaviour is suspicious or not. Furthermore, the nodes should be expendable, if necessary, and be small in size such that they are hard to detect by adversaries. The network should be self-configuring and self-sustaining and should be reliable, efficient, and effective during operational tasks – especially route surveillance – as well as robust in time and space. If data from these networks are combined with data from other remote sensing devices (e.g. UAVs (Unmanned Aerial Vehicles)/aerostats), an even more accurate assessment of the tactical situation is possible. This paper shall focus on the concepts of operation towards a working intelligent route surveillance (IRS) research demonstrator network for monitoring suspicious behaviour in IED sensitive domains.

Keywords: Intelligent sensor networks, unattended ground sensor networks, abnormal and suspicious behaviour, Counter-IED, intelligence gathering, situation awareness, route surveillance.

1. INTRODUCTION

The need for technological solutions that tackle the IED problem in operational domains has resulted in a vast array of different technologies ranging from radar, infrared, and visual remote sensing devices, to sniffer dogs, robust vehicles, metal detectors, and jamming devices. A novel force protection technology is an unattended ground sensor network that monitors activity at strategic spots along routes; it gathers and processes data in real time or stores the data *in situ* for subsequent analysis. Information on abnormal or suspicious activities over a required span of time can be stored for further analyses and intelligence gathering or can trigger an alarm in tactical situations.

Abnormal behaviour follows from measured anomalies in a regular or normal perception of events. It can lead to suspicious behaviour and even to hostile intent, although the latter is hard if not impossible to quantify. Moreover, abnormal behaviour can trigger false alarms for suspicious behaviour and/or hostile intent. On the other hand, hostile intent, non-observable in nature, can be genuinely disguised in the background of regular events, and do its job efficiently. Countering these actions depends on the situation, scenario and time frame at hand and the interpretation of the information and data. By analysing and interpreting retrieved data from a dedicated sensor network along roads combined with data from a regular event database with advanced software algorithms, it is possible to retrieve information on abnormal behaviour. By reducing the false alarm rate through more intelligent software solutions, our aim is to separate abnormal events from suspicious events for route surveillance applications along roads and at crossings.

This paper shall focus on the concepts of operation towards a working IRS demonstrator network at technology readiness level 6 (TRL6). Working demonstrations and results shall be presented in a follow-up paper. What follows is a short introduction to UGS (Unattended Ground Sensors) technology in the next section. Section 3 discusses the operational domain and appropriate network levels for which a future demonstrator will be tested. Section 4 highlights behavioural issues. Then in section 5 the concept of the IRS demonstrator set-up is presented. A final word is given in section 6.

* E-mail: robin.schoemaker@tno.nl. Tel: +31 70 374 0571. Fax: +31 70 374 0654

Unattended Ground, Sea, and Air Sensor Technologies and Applications XI, edited by Edward M. Carapezza,
Proc. of SPIE Vol. 7333, 73330H · © 2009 SPIE · CCC code: 0277-786X/09/$18 · doi: 10.1117/12.818447

2. UGS NETWORKS

Unattended ground sensor networks are passive sensor networks for applications in remote areas, ranging from local borders to foreign battlefields, where they work independently. UGS are developed for remote detection, localisation, identification and classification of targets mainly for force protection purposes (situation awareness, perimeter defence, border patrol, surveillance, target acquisition). The sensor nodes are low-cost, robust and small and should operate for extended periods of time within operational time frames. The networks are assemblies of hidden nodes that sense their surroundings and communicate information to each other and/or to a user. The type of sensors can be magnetic, acoustic, seismic, passive infrared (PIR), radar, or capacitive. The range of most ground sensors is limited due to weather conditions, diurnal changes, background noise, and battery power. Therefore the sensors should be robust and close enough to each other to cover the area of interest under all weather conditions. Smart power management helps by monitoring the environment only during short periods until detection takes place and the system commences the full power operation mode.

In most unattended sensor networks the topology is such that each node communicates its alarm to one central gateway node for long distance transmission. In self-organising smart sensor networks, though, the nodes communicate with each other and process the data inside the network. The real time data on detection, classification, tracking, etc., can be stored locally in one of the nodes for communication at short distance by a surveillance unit, or can be stored in a special gateway node for communication to a remote user in a base at larger distance.

UGS networks can be composed of complete operational COTS (Commercial-off-the-Shelf) systems for which software is required to specify and deploy the sensors in a desired operational setting. The software is often included with the system, but dedicated software applications are sometimes needed for further research in CD&E (Concept, Development & Experimentation) environments. Especially low TRL UGS research networks require dedicated software applications for processing, communication, and analyses. A nice example of such an application is TNO's TActical Sensor network TEstbed (TASTE) that works with different sensor types that can be deployed virtually and for which their individual and combined performances can be analysed (see [1]).

3. OPERATIONAL DOMAIN & NETWORK SCALES

The IRS demonstrator will consist of two UGS networks and a software application that runs on a laptop and/or PDA. This will be discussed in Section 6. The feasibility to be demonstrated with the IRS network demonstrator in a realistic operational setting requires prior knowledge of the terrain. The setting for IRS is considered in a hot, desert-like, mountainous land for which five typical domains have been identified, in order of operational priority:

1. The *Road* domain is characterised by roads outside the *Urban* domain (see 4) that run through the *Green* (see 3) or through the *Desert* (see 2) connecting communities and villages. The roads are of bad quality, have no lights and are unpaved most of the time. Paved roads also lack any lighting and lines. Bridges are part of *Road*. Transport vehicles from locals can consist of mules, horses, handcarts, bicycles, motor cycles, cars, small vans, pick-up trucks, and trucks. It can be busy during festivals and holidays and at specific moments of the day. Locals as well as foreign troops make frequent use of roads.
2. The *Desert* domain is characterised by a hot, inhospitable, non-cultivated, desolate and rocky terrain with high hills and small unpaved roads of bad quality (see 1), criss-crossing the land through valleys and open areas. Small rocky paths inaccessible for motorised transport are part of this domain type and not the *Road* domain type.
3. The *Green* domain is found along rivers, is semi-cultivated (agriculture) and close to communities. Next to the green are isolated small farms from the people who own the parcels of farm land. The rivers in this operational setting have very few bridges and can also be crossed when shallow enough. Important route for surveillance is along the river through the shallow riverbed. Local activity in the *Green* is limited to agricultural activities.
4. The *Urban* domain describes an operational setting for communal areas or small villages in which people interact, live together, and trade. Typical for an *Urban* domain are one or few main roads with several side-roads. Along the main road there are small houses, little shops and markets. *Urban* is characterised by a busy and chaotic atmosphere where people and live stock share little space.

5. The *Mountain* domain is not considered within the context of this research. Mountains in the current operational setting are high and difficult to patrol.

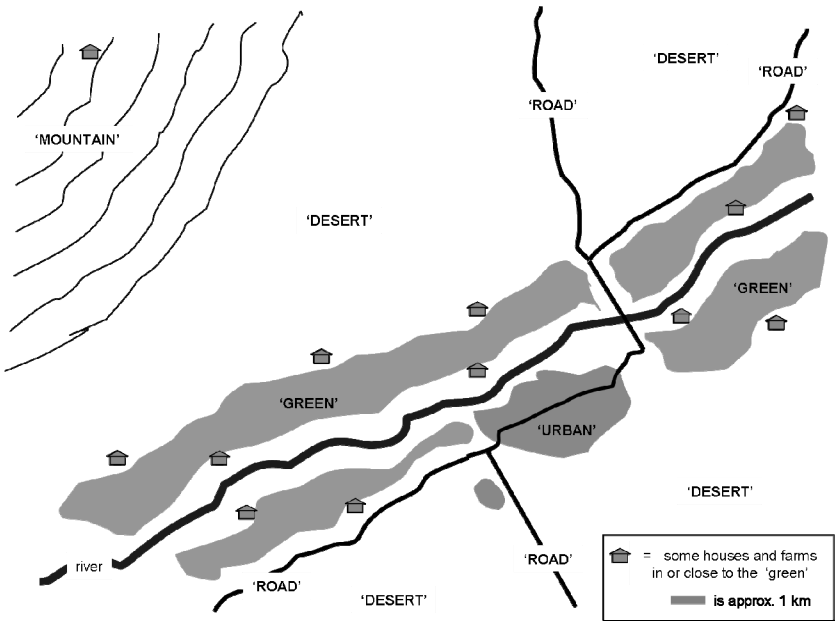

Figure 1. The five typical domains schematised.

The frequency of IED attacks is highest at so-called hot spots along roads and at crossings. This is supported in the next section, where behavioural patterns are discussed. The research of the IRS demonstrator therefore focuses on roads and crossings in the *Road* domain.

Two spatial levels – a micro and a macro level – for the *Road* domain are identified for the networks to operate in. The macro level consists of two or more micro level networks separated by several km, within range of their gateways. In Figure 2 a macro level with two micro levels is shown.

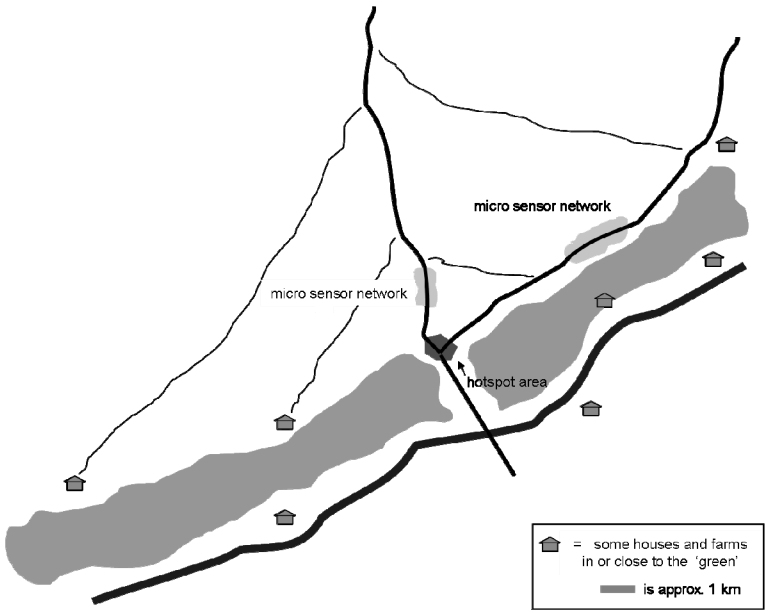

Figure 2. Macro level with two micro networks in an area with roads, smaller cut-off paths, semi-cultivated land and houses. Hot spots are locations that are known as old or potential IED spots. These spots are to be found along routes where surveillance troops have strategic interests. Hot spots can be re-used.

The macro level network, if strategically placed, should be able to monitor intensity of traffic along roads of interest on a larger scale. More micro networks are required if the road network is more complex. Any road traffic inside the cell can be monitored (motorised and non-motorised). The network is placed along a piece of the road (both sides) of 100 – 150 m in length and 10 – 20 m in width. A micro network, see Figure 3, consists of 10 to 20 sensors. The operational scope of IRS requires only two micro networks for only two or three main roads (see Figure 2). This, and the composition and topology of the network, is discussed in Section 6 where the IRS demonstrator set-up is presented.

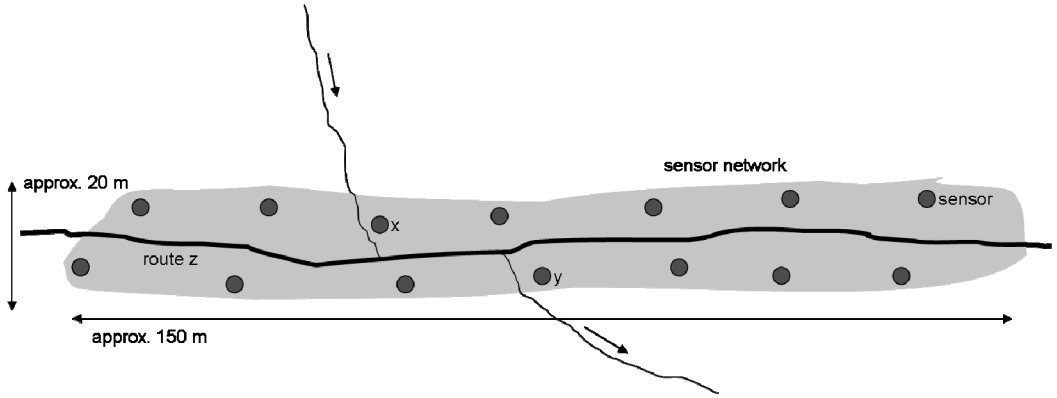

Figure 3. Micro level network surrounding a piece of road. Smaller track crosses the road and the micro network. Sensor x and y track an object that has not taken route z.

4. ROAD DOMAIN BEHAVIOUR

An elemental function of a micro network in the IRS context is the measurement of 'traffic in – traffic out' fluxes. Fine tuning on classification and identification requires more sophisticated algorithms, even more so for the analysis of complicated and abnormal behaviour. Behavioural issues and what to measure and analyse in a network and/or combinations of networks, is discussed in this subsection.

The temporal behaviour of suspects inside UGS networks is of great importance for this research. Patterns in time render a regular or normal perception of events, while deviations of these perceptions are indicative for suspicious behaviour. The normal perception patterns are to be constructed by means of data mining through the network or via *a priori* intelligence data. Daily fluctuations, weakly fluctuations, monthly fluctuations, and the local calendar for festivities and special days during the year, are patterns of local people that are indispensable. Behaviour of allied forces is to be incorporated as well. Experience dictates that most IED deployments happen during the night and that the digging of a hole and the placing of an improvised explosive in that same hole are not necessarily simultaneous acts and not necessarily by the same person. Moreover, adversaries use environmental markers for timing of the device, while IEDs can be buried for months either, leaving only the connection of a battery or cell phone. IED deployments are tactical as well as a strategic in character.

The event database mentioned in the introduction is a representation of regular activities along the route under surveillance and is being fed with detection data from the network(s) and if possible other intelligence data. More accurate data is retrieved when fresh and useful data is fed into this database for the area and time frame of interest. New deviations that seem suspicious at first become regular events after being identified as special or returning days for some communal festivity or religious event. The few quite roads in the operational setting are outside the *Urban* domain where traffic rules are absent. Close to communities the time dependent traffic is busier and more diverse and also more chaotic. There is an obvious diurnal rhythm with exceptions on holidays and festivities. The roads are in bad condition, marked by pits, rocks, and wreckage, which can generate choke points during busy times of the day, creating dangerous situations that demands an extra sharp-eyed attitude.

For the micro level network set-up, suspicious or abnormal behaviour of local people – especially women and children – is characterised by the avoidance of certain (parts of) roads, especially near known (older) hot spots. Nocturnal activity of one or two persons is considered to be suspicious to first degree. Even more when a network data pattern shows a moving object along an isolated road that stops at a location where moments later seismic patterns reveal the digging of a hole. The same applies for a spot along a road that is encountered sideways by foot. This is more difficult to monitor or

sense, yet, if the object (a walking person) enters a micro level network, he will be detected. Many examples can be given.

Macro level measurements, on the other hand, are used for large scale traffic flows along roads and at crossings. Travel time and intensity are two required parameters for the detection of abnormal behaviour of vehicles. Using micro networks with many nodes (Figure 3) one can measure the inflow and outflow of vehicles, but also activity *inside* a network. A micro network is too small to cover the entire suspect road; moreover, if it has been positioned at a random location along the road, there is little chance that suspicious acts happen inside the network. One can propose to use fewer nodes in a simpler network configuration for macroscopic traffic flow analysis. Positioning a micro network with many nodes at strategic locations (hot spots) on the other hand, the chance that an event occurs inside the micro network is more realistic. In that case the micro data is stored and analysed, and a more accurate assessment of the situation can be given in this case. Still, measurements inside any micro level site are expected to be rare, therefore large scale suspicious traffic flow analysis has priority in the IRS research.

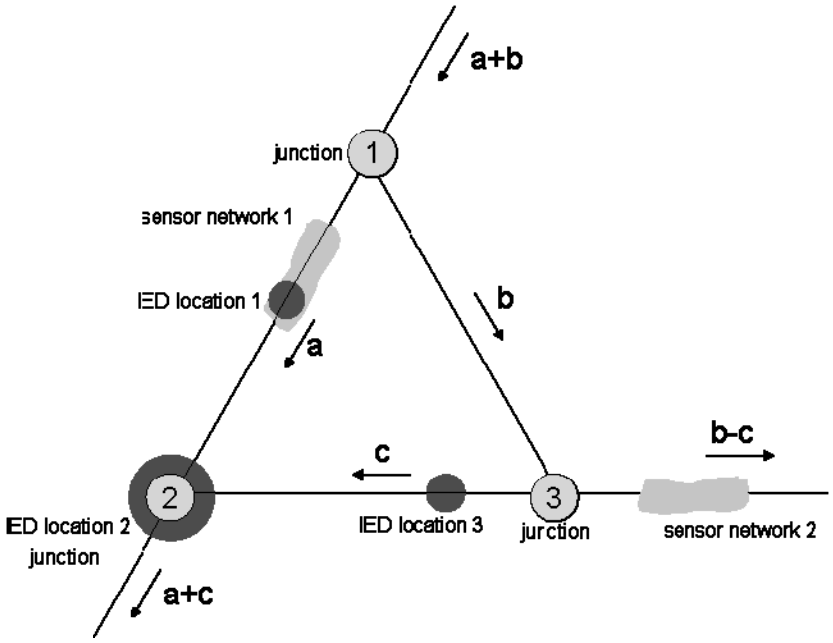

Figure 4. Possible macro level scenario for monitoring IED activities. If traffic flow **a** decreases (from 1 to 2) and flows **b** and **c** increase (from 3 to 2) and **b-c** stays equal, abnormal behaviour between 1 and 2 is detected. In that case the road between 1 and 2 should be searched for a potential IED threat. But if **b-c** decreases on the other hand, and **a** also decreases, then the locations 1, 2, and 3, are potential hot spots. Two micro networks is a minimum, more than two is even better.

5. THE IRS DEMONSTRATOR

The purpose of the IRS project is to demonstrate the detection of abnormal route behaviour – and ultimately suspicious behaviour – by analysing data from two UGS networks. The IRS demonstrator will work on the macro level as described above. Two micro networks of 10 - 15 COTS sensors each will monitor the flows of traffic for an appropriate road set-up.

The heart of the IRS demonstrator is a software application that operates on data from two sensor networks. Each sensor is equipped with a magnetic, seismic or acoustic unit. Some sensors may have a passive infrared unit (PIR) included. The 10 - 15 sensors communicate with their respective gateway node for communication with the user in the field during real time surveillance missions, with a base at larger distances, or with the other network.

5.1 Parameters for route surveillance

Important parameters for an Intelligent Route Surveillance system are *classification*, *location*, *intensity*, *route*, and *speed*. Classification within IRS is threefold and aims for a distinction between non-motorised traffic (people and stock), small

motorised traffic (motor cycles and cars/vans), and large motorised traffic (trucks and armoured (caterpillar-tracked) vehicles.) The types of sensors suitable for these parameters are magnetic, seismic and acoustic (and if appropriate PIR). Synergy is established by combining different sensors in the right network topology. Intensity of traffic flows is measured by counting objects in the networks. If traffic intensity is low the micro network should be able to estimate the parameters locally within certain accuracy, while the macro setting monitors the flows through the micro networks. If, for example, in a micro network an object is identified as a car with a certain speed driving towards a second micro network several kilometres onwards, it is expected that this car enters this second network with a similar speed at a plausible extrapolated time. If an object suddenly stops, its location is only detected in the vicinity of a magnetic type sensor (or PIR). Acoustic sensors and seismic sensors, that are close by, detect whether people step out, walk around, and change a tire or dig a hole. As indicated in Section 5, abnormal or suspicious behaviour detected in a micro network highly depends on its strategic position.

The speed and route of an object is determined by the detected locations of the vehicle synchronised in time. Object tracking is very dependent on traffic intensity and is less reliable if traffic intensity is high. The workable setting of IRS anticipates on relatively quite traffic, implying that inside a micro network in a *Road* domain (outside the *Urban* domain) traffic is limited to one or two objects at a time.

5.2 COTS ground sensors

The sensors to be used in the IRS demonstrator are very dependent on the above mentioned parameters. Sensor candidates are magnetic, acoustic, seismic, and passive infrared (PIR). GPS (Global Positioning System) must be included with each sensor for efficient localisation and object tracking. Without a GPS the software become more complex.

Table 1. Breakdown of sensors with capabilities required for IRS.

Sensor	Non-motorised	Small motorised	Large motorised
Geophone	detection	detection	detection
Microphone	detection	detection	detection
Magnetometer	N/A	detection + direction	detection + direction
PIR	detection + direction	detection + direction	detection + direction

A network consists of nodes that each contains a sensor and a transceiver. The performance of above sensors depends on certain default specifications and sensitivities, but also on external factors, mostly due to weather effects.

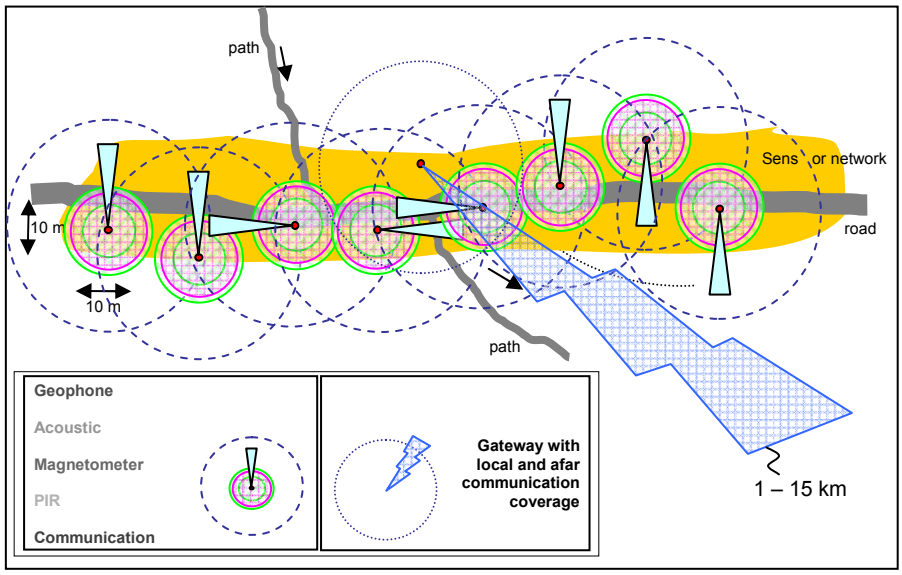

Figure 6. Example of a micro level network coverage of the IRS demonstrator with eight sensors and their respective coverage. Each node is equipped with four sensing technologies and one communication technology. Weak point in this set-up is when one node drops out and communication to the gateway is lost. (for color image, please see electronic version)

A geophone measures seismic activity which is subject to the weight of the object and the type of soil (soft or rocky, dry or wet). A microphone strongly depends on the direction of the wind and ambient noise (other vehicles or rain). A magnetometer only works for metallic objects and the passive infrared detector measures in a small sector only and is strongly dependent on visibility. Communication range is also very important. An IRS micro network consists of 10 to 15 sensors and is distributed over an area 100 – 150 m in length and 10 - 20 m in width. That implies a communication range among each sensor of at least 10 m. A typical coverage of the micro network is given in Figure 6. Other IRS sensor suite features are coverage, robustness, size, camouflage ability, signal processing, energy consumption, commercial availability, price, interface and included software. For IRS it is very important to work with a COTS network with open source interfacing so that dedicated software can be written for data analysis.

5.3 Software considerations

The results from an UGS network include sensor ID, location of an object, the time of detection, and classification. Processing at the micro level is done by combining detection data and track retrieval of an object. A track is a collection of detections that belong to each other and that contains the route taken by the object. In addition to this, the speeds in the micro network are to be determined by the average speed of the route taken and its deviations along this route. Collecting the data for the regular scene is accomplished by storing the tracking data as an item. An item must contain information on the route that has been taken, the object class, the time stamps of the first (and the last) detection but also the day of the week and the month, and the speeds on a route. From the collected data, several regular patterns – for a certain area under surveillance – can be retrieved, such as:

1. The routes are taken by an object of a certain class in a specific time frame.
2. The normal speeds on each route for each moment of the day for a certain object class.
3. The normal number of transits for each day of the week.
4. The frequency of routes taken each day of the week.

Detection of deviations in the regular scene is accomplished by comparing the new track of an object with the regular scene database in the micro level network. Is a detection of an object at this time of day a normal event compared to regular pattern 1? For example, how many pedestrians normally walk around in the night at 04:00 A.M.? Is the speed of the object normal at this moment in time, compared to regular pattern 2? For example, is the speed at this moment for this object normal? By comparing tracks of several objects in a time frame with the regular perception, deviations can be found, like: Has traffic been normal this day, compared to regular pattern 3? Or is the area avoided because something is afoot? Has there been a change in the routes taken, compared to regular pattern 4? Or is a certain part of the road being avoided and is another route being taken because something is afoot?

Processing on a macro level is achieved by tracking an object on the macro level by combining several tracks at the micro level. This track holds the route taken by the object. In addition to this, the average speed between the micro level networks is to be determined and the deviations of this speed in the micro networks. Collecting the data for the regular scene is accomplished by storing the tracking data as an item that has the same qualities as in the micro level case above: The route that has been taken, the object class, the time stamps of the first (and the last) detection but also the day of the week and the month, and the speeds on a route. From the collected data, several regular patterns – for a certain area under surveillance – can be retrieved, as given above (number 1 to 4), including a fifth:

5. The deviations in speed between the micro level networks (on a macro level) compared to those inside the micro networks.

Retrieving the deviations from the regular scene is accomplished by comparing a track of the object on macro level with the regular scene, as was explained for the micro level case. Also, by comparing tracks of several objects in a time frame with the regular event database, a deviation can be found. In addition to this, deviations in speed within a macro track can be traced.

6. CONCLUDING REMARKS

The IRS research aims for the development of a software tool for operational networks to be tested with real sensors in a demonstrator set-up. This paper started with an introduction to UGS technology and an explanation of the operational domain and network scales in which the IRS demonstrator will be tested. Also highlights on behavioural issues were

discussed, as well as the concept of the IRS demonstrator set-up and the choice of sensor types. The research presented in this paper is currently underway and the IRS demonstrator is to be tested in 2009. What we have discussed so far is the operational scope in which the IRS network will be demonstrated and also what the network should consist of. Results will be presented in a future paper.

Although the heart of IRS is a software tool that detects suspicious behaviour out of regular behavioural patterns, a hardware network is realistic and should as such be tested, although one can conjecture to fully simulate the network too. However, the demonstration of the hardware sensor network can be tested in the field in a shorter period of time if the regular daily pattern of events is simulated and constructed a priori.

Along with working results of the IRS demonstrator in a future paper, the deployment of the sensor nodes is considered as well. Deployment in an operational domain, preferable done at night, requires a cautious, inconspicuous and discreet attitude, while the nodes should be robust, small and invisible (see Section 2). The same applies to node exposure, which is an unacceptable situation. If one or more nodes are found, material is supplied (electronics, casings, GPS, etc.) that can be used in yet new improvised devices. It is therefore highly desirable that sensor nodes are tampering proof/self destructible, and/or extremely simple in form and composition. There are exceptions to this. For example, for intelligence gathering fake bugged network sensor nodes are to be found on purpose by an adversary who then can be traced back to a potential location of interest.

ACKNOWLEDGEMENTS

We thank the Netherlands Ministry of Defence for supporting this work. We further thank Alle de Jong of the Netherlands Ministry of Defence and his team for the many fruitful discussions and feedback.

REFERENCES

[1] Van Dorp, Ph., H.H.P.Th. Bekman, R.D.J. Sandbrink, "TActical Sensor network TEstbed (TASTE)", in *Umanned/Unattended Sensors and Sensor Networks V*, edited by Edward M. Carrapezza, Proceedings of SPIE Vol. 7112 (2008).
[2] TNO Report "Verkenning toekomstige OGS", van Hoof, van Voorthuijsen, FEL02-A291, March 2003.
[3] TNO Report "Technologieverkenning Inlichtingen 2004", Martis, den Hollander, TNO-DV1 2005 A021.
[4] TNO Report "Eindrapportage Defensieprogramma Inlichtingen (v007)", Verhaar, den Hollander, TNO-DV1 2006 A052.
[5] TNO Report "Het SOWNet Experiment", Ruizenaar, Boekema, van Hoof, van Voorthuijsen, TNO-DV 2008 A342.