Unattended Monitoring of Suspicious Behaviour for Route Surveillance

Robin Schoemaker, Rody Sandbrink, Graeme van Voorthuijsen
TNO Defence, Security and Safety, P.O. Box 96864, 2509 JG, The Hague, The Netherlands
Tel: +31 70 374 0571, Fax: +31 70 374 0654,
E-mail: robin.schoemaker@tno.nl

ABSTRACT

A priori information on suspicious behaviour is extremely valuable for countering threats involving improvised explosive devices (IEDs). Suspicious activities along routes during expeditionary operations can be monitored by unattended networks using simple sensing nodes that can gather data for continuous monitoring of daily vehicle activity. Dedicated software yields the necessary intelligence on these activities by filtering suspicious behaviour from anomalous behaviour (including false alarms). Research has started to equip a commercially available sensor network with data analysis software. It aims at demonstrating the detection of suspicious behaviour along roads, within a required time span. Three phases are distinguished. First phase is the analysis of traffic flux in a simple scenario with three networks lying at three junctions. The second phase investigates the ability to track and classify one object in this scenario, while the third phase aims to track and classify two or more objects. Findings are presented for phase one, flux measurements.

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

1. INTRODUCTION

Improvised explosive devices are a constant threat during operational tasks. The burying of an IED (or parts of it) is an act that takes place mostly in the dark and in secret. Some IED's can be buried for months and only need a battery installed when tactics demand a quick response. Many IED's have a self-detonation feature; some are detonated from a distance by a person. An exploding IED marks the end stage of a whole chain of activities. Prior to that event a buried and activated IED forms an instant threat for every person not in the know, both civilians and peacekeeping forces.

Unattended camouflaged ground sensor networks are ideally suited for long term monitoring of activity at strategic spots along routes in operational domains. They gather and process data in real time for immediate analysis or for back-up. Local people with some knowledge of what is going on, e.g. women and children, behave differently when rumour has it that a certain road or crossing is to be avoided. It is this behaviour that can be monitored with sensors for longer periods of time. 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. Unfortunately, hostile intent, non-observable in nature, is often genuinely disguised in the background of regular events.

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 for force protection. Countermeasure operations depend 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 an evolutionary event database with advanced software algorithms, it is possible to retrieve information on abnormal behaviour. A research project has started to do just this for route surveillance along roads and at crossings. By reducing the false alarm rate through more intelligent software solutions, the aim of this research is to detect genuine abnormal events in the regular setting and to recognise this abnormal behaviour as suspicious or as non-suspicious.

This paper shall focus on measurements done with a commercially available unattended ground sensor (UGS) network applied to large scale flux measurements data in a project called Intelligent Route Surveillance (IRS). What follows is a description of the relevant domain of operation in which an IRS like operational system should function. Section 3

Unattended Ground, Sea, and Air Sensor Technologies and Applications XII, edited by Edward M. Carapezza,
Proc. of SPIE Vol. 7693, 76930S · © 2010 SPIE · CCC code: 0277-786X/10/$18 · doi: 10.1117/12.850134

shortly discusses traffic behaviour along the roads of interest, followed by Section 4 on the UGS networks used. Section 5 discusses the flux measurements done and the accompanying results. A final word is given in section 6.

2. RELEVANT DOMAIN OF OPERATION

An IRS like operational network is considered for a hot, desert-like, rough 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.

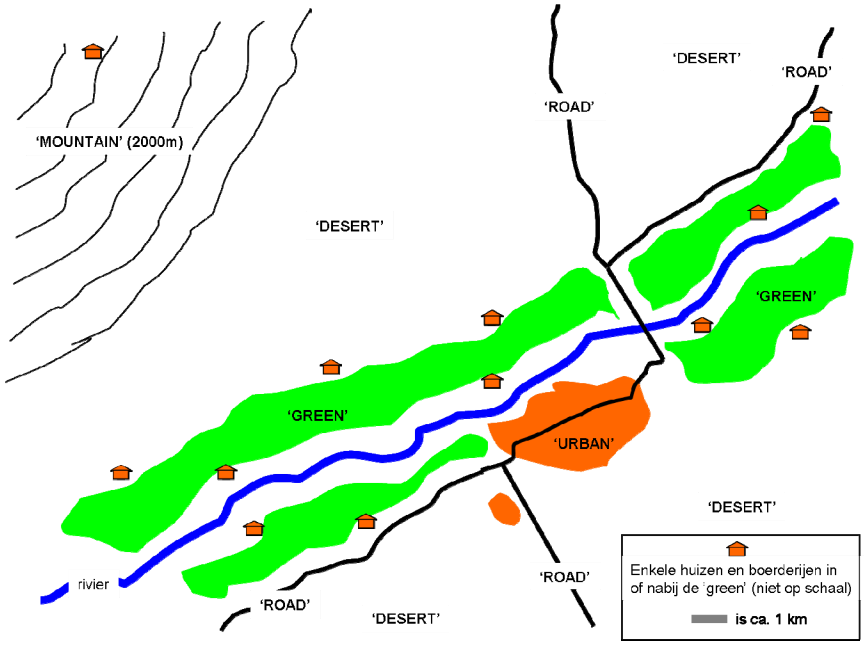

Figure 1. The five typical domains schematised. The orange coloured houses depict a sparse collection of houses and farms in or close to the 'green', not to scale. The gray bar in the legend box marks the domain scale of approx. 1 km.

2.1 Spatial levels

The frequency of IED attacks is highest at so-called hot spots along roads and at crossings. The IRS project therefore focuses on roads and crossings as given in the *Road* domain described in Section 3. In earlier studies of the IRS project, see [6], two spatial levels were identified for *Road* domain networks to operate in, a micro level and a macro level. The macro level consists of two or more micro level networks separated by several km, within range of their gateways, depicted in Figure 2 where a macro level with two micro levels is shown. The macro level, if strategically placed, should be able to monitor intensity of traffic along roads of interest on a larger scale. A micro network covers a small area 100 – 150 m wide and 10 - 20 m in width. Cluster is a more appropriate name for the micro network definition in the context of this research. We shall use cluster from now on.

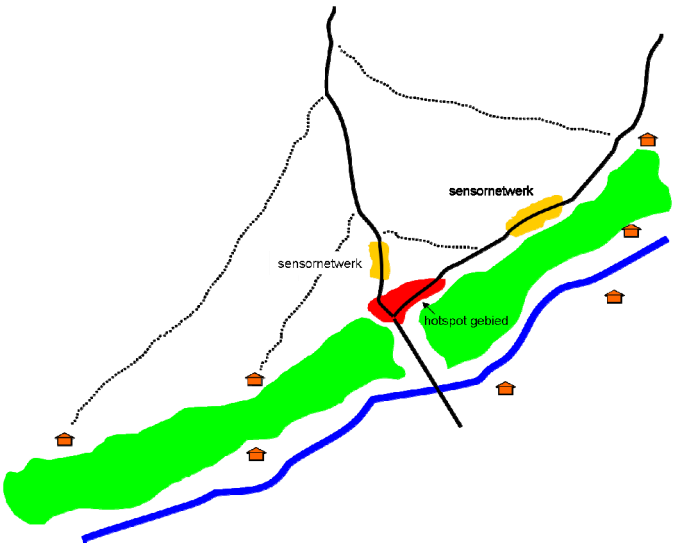

Figure 2. Macro level with two clusters in an area with roads, smaller cut-off paths, semi-cultivated land and houses. Hot spots are locations that are known as potential IED spots. These spots are to be found along routes where surveillance troops have strategic interests. Hot spots can be re-used.

3. ROAD DOMAIN BEHAVIOUR

3.1 Behaviour

Behavioural patterns in time render a regular or normal perception of events, while deviations of these perceptions are indicative for suspicious behaviour. The event database mentioned in Introduction is a representation of regular activities along the route under surveillance and is being fed with detection data from the network(s) and 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. Daily fluctuations, weakly fluctuations, monthly fluctuations, and the local calendar for festivities and special days during the year, are patterns of local behaviour that are indispensable. Behaviour of allied forces is to be incorporated as well.

The few quite roads in the operational setting are outside the more chaotic *Urban* domain. Close to communities the time dependent traffic is busier and more diverse. There is an obvious diurnal rhythm with exceptions on holidays and festivities. The roads are in bad condition, marked by pits, rocks, wreckage, that can cause choke points to develop during the busy times of the day, creating dangerous situations (digestion) that demands an extra sharp-eyed attitude.

Nocturnal activity of one or two persons is considered to be suspicious to first degree.

Macro level measurements 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, see also Section 3.2. For this traffic flux setup the aim is to identify suspicious or abnormal behaviour of local people – especially women and children – that is

characterised by the avoidance of certain (parts of) roads, especially near known (older) hot spots. Clusters with many nodes can measure the inflow and outflow of vehicles, but also activity *inside* a network. A cluster is too small to cover the entire road under suspicion, but if it was positioned at a random location along a road, there is little chance that suspicious acts happen inside the network. In that case one can use fewer nodes in a simpler network configuration for macroscopic traffic flow analysis. The chance that an event occurs inside the cluster is more realistic when a cluster is positioned with many nodes at strategic locations like hot spots and choke points. In that case the cluster data is stored and analysed, and a more accurate assessment of the situation can be given in this case.

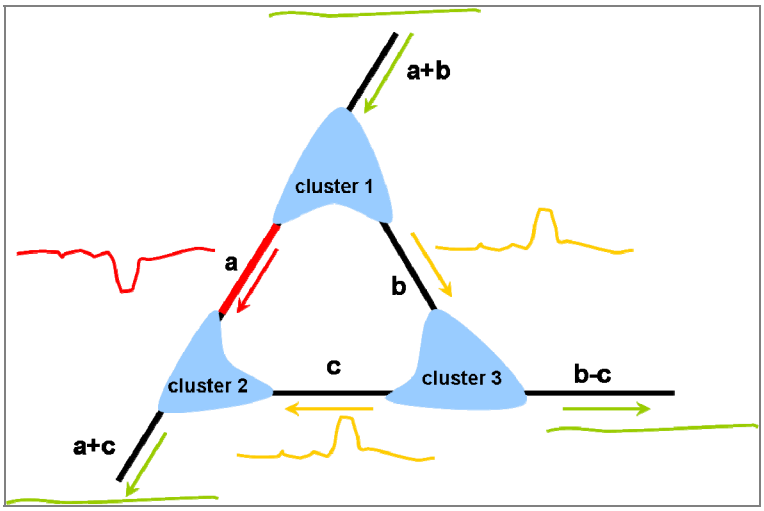

Figure 3. Possible macro level scenario for monitoring IED activities. If traffic flow **a** decreases and flows **b** and **c** increase and **b-c** stays equal, abnormal behaviour on road **a** is detected and a route clearance procedure can be initiated.

3.2 Analysis methodology

Required parameters for an Intelligent Route Surveillance system are *classification*, *location*, *intensity*, *route*, and *speed*. Location, route, and speed refer to the *tracking* of one or more objects. *Classification* 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). *Intensity* refers to macroscopic traffic flux. The types of sensors suitable for these parameters are: magnetic, seismic, and acoustic (and if appropriate passive infrared (PIR)). Synergy is established by combining different sensors in the right network topology. Intensity of traffic flows is done by counting objects in all the clusters. The speed and route of an object is determined by the detected locations of the vehicle synchronised in time.

Three basic methodologies or phases can now be identified for UGS data analysis if the five required parameters mentioned above are considered: Traffic flux measurements, one object tracking and classification, and the tracking and classification of multiple objects.

The IRS research aims for an investigation of each phase at a time. Figure 3 sketches the working setup for phase one, a traffic flux analysis. To test this with a commercial-off-the-shelf (COTS) UGS network, the IRS project used a system that should satisfy the objectives of at least this first phase. The next section deals with such a network.

4. UGS NETWORKS

Unattended ground sensor networks are passive sensor networks for applications in remote areas where they work independently. The remote areas range from local borders to foreign battlefields. Unattended ground sensors 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 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 on the other hand 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. UGS research networks with a low technology readiness level (TRL) require dedicated software applications for processing, communication, and analyses. A nice example of such an application is TNO's TActical Sensor network TEst bed (TASTE) that works with different sensor types that can be deployed virtually and for which their individual and combined performances can be analysed (see [2]). High TRL COTS networks on the other hand offer robust functionality for a specific application. Primary software is often included with the system, but for specific applications in CD&E (Concept, Development & Experimentation) projects more functionality requires additional software engineering on the data.

4.1 The IRS sensor test bed

The purpose of the IRS project is to demonstrate the detection of abnormal route behaviour – and ultimately, suspicious behaviour – by analysing data from UGS networks. The IRS demonstrator will work on the macro level as described above and the networks will be constructed with COTS sensors for *Road* domain scenarios. IRS is a software application that works with UGS network data. Its feasibility is to be demonstrated for the three methodologies mentioned in Section 3.2. For IRS's purpose affordable COTS sensor systems are not abundantly present in stores. A system has been purchased comprising 27 sensors and three gateways (repeater/bas stations). See specifications further on.

This COTS network works with an SQL database in which the data from every sensor is available. An XML file is the being pushed by other modules through TCP/IP. This XML file can be read with IRS software. See Figure 4.

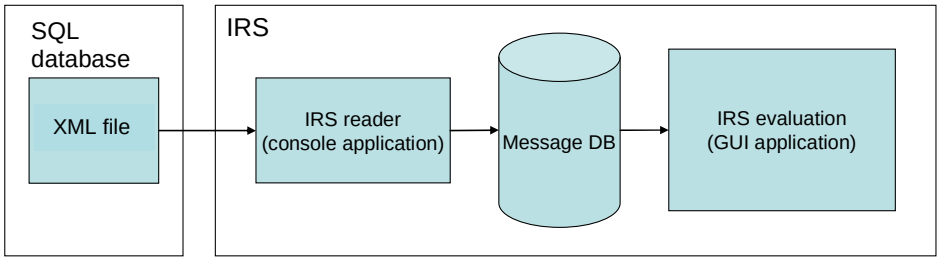

Figure 4. Context of the IRS software application.

For all the three IRS segments, IRS reader, Message DB, and IRS evaluation, prototype software applications have been written. These have been tested in a relevant domain.

Each sensor is equipped with a magnetic, seismic, acoustic, and passive infrared (PIR) unit. The 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(s). It is a communication and sensor network in one.

Table 1.Sensitivity specifications of the used sensor. The PIR is a passive infrared contrast sensor.

Sensor P	erson	Vehicle	Gun shots
geophone	20-30 m	50-150 m	×
magnetometer	×	3 m	×
PIR	20-30 m	30-50 m	×
microphone	×	×	20 m

The sensors to be used in the IRS demonstrator are very dependent on the above mentioned parameters. Each sensor houses, next to a magnetic, an acoustic, a seismic, and a PIR sensor, a GPS (Global Positioning System) chip for proper localisation and tracking. Without a GPS the software algorithms become exponentially complex an expensive. The sensors also have a temper alarm, 900 MHz spread spectrum communication, water-proof housing and are using two AA batteries. The energy consumption is however high when the seismic sensor is on, especially if activity is very high, the batteries last for two days in that case. If the seismic sensor is off, and only PIR is used, then the life time of the two AA batteries is 10 days. This has been tested, see Section 4.

When the buried geophone is used, the PIR and the microphone do not work. The four geophone classifications are: persons inside a building, persons outside a building, vehicles, persons and vehicles. Sensitivity can be adjusted to four levels.

The performance of the sensors depends on certain default specifications and sensitivities, but also on external factors, mostly due to weather. 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 is strongly dependent 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 field of view and is strongly dependent on contrast variability.

The communication aspects are important of course if such a system is to work autonomous for longer periods of time. The sensor set at hand has gateways for communication transfer over longer distances, while the sensors require at least one gateway inside the network. This network gateway, also called repeater/base station, depending on its function, needs to be within a range of 300 – 500 meter for buried sensors, 500 – 1000 meters for sensors between 0 and 1 meter above the flat ground, and more than 1000 meter for sensors that are at least 1 meter above the flat ground. The repeater/base stations carry other energy sources and can reach 6 – 8 km. In Figure 5 a future IRS system is schematised.

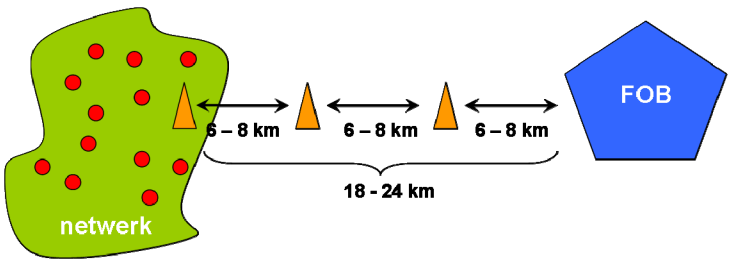

Figure 5. Outline for an IRS like operational system for military applications. FOB = Forward Operating Base. One network gateway resides in the network and communicated all the data to the operator.

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 could be applied for data analysis.

5. FLUX MEASUREMENTS

A first test has been performed in a relevant domain to get acquainted with the sensors and the IRS prototype software. As mentioned earlier, an elemental function of the network is the measurement of 'traffic in – traffic out' fluxes. This is part of phase one of the software development process (Section 3.2). Fine-tuning on classification and tracking requires more sophisticated algorithms and is not considered in this first phase.

5.1 The test

The unpacked network was put in place very quickly in order to test its robustness in combination with the first IRS software applications. Twenty four sensors where densely placed in an area around a building with a capacity of a few hundred working people. A parking lot is included, so motorised activity as well as walking and biking activity have been monitored. Not all corridors and entrances where covered though. At first three sensors per sensornode where switched on: seismic, magnetic, and PIR sensors. The enormous amount of activity resulted in an unworkable situation concerning the energy consumption and battery replacements, mostly due to the very sensitive geophone. It was decided

to use only the PIR sensor for each sensornode for the remainder of the test. Figure 6 nicely shows a two-week measurement for one of the 24 sensors. Still, two days pop-up where battery life problems occurred, even with only the PIR sensor. The green spiky patterns are characteristic for the daily activity around this building. Clearly a morning peak is visible when all people arrive and also a peak in the late afternoon when people depart and go home. Sometimes, probably during a sunny day, the lunch reveals a tiny peak where a moderate number of people go out for a walk.

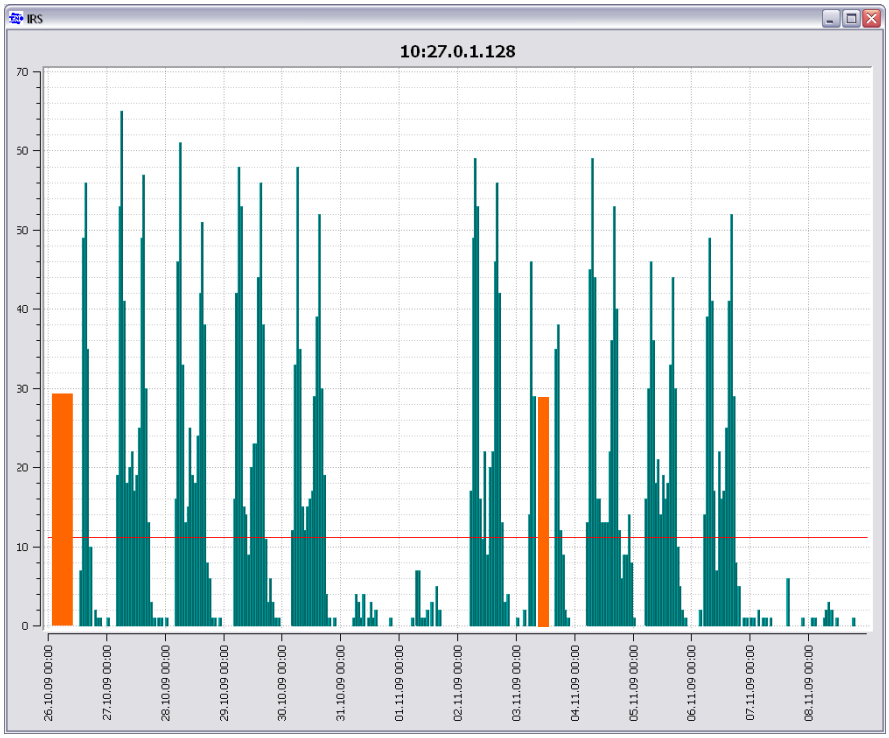

Figure 6. Sequence of weeks of measurements for one sensor. Green spiky typical patterns represent the working days. Two weekends are clearly visible in the middle and at the end with a very low number of detections. The orange bars are missing dat for this sensor due to empty batteries.

Figures 6 and 7 show typical patterns and typical numbers of detection. The typical patterns are indicative for the regular scheme of events. Anomalous deviations from this pattern can trigger alarms. This is a qualitative and tactical aspect of the use of these kinds of networks. By quantifying these measurements in more detail, more in-depth analyses can result in better intelligence gathering during longer periods of time. However, both aspects can of course be used in real time.

In Figure 7 a single-sensor graph is shown with comparisons for one day during three consecutive weeks. It shows a typical working day at the facility. Although the facility houses 380 parking lots, not all lots are filled; between 280 – 380 is a good daily estimate to work with. Due to its strategic location, this particular sensor delivered all detections regarding cars, motor bikes, and bicycles. A three day average gives approx. 230 detections per day for all incoming vehicles if the hourly data is added up between 6 and 11 in the morning. The same applies to the summation of data for the afternoon. Not all entrances of the facility where covered and people who use public transport for example are missing from the measurements. However, the average figure of 230 is still way too small, compared to the 375 – 475 people that are on average inside.

The cause is inherent to sensor systems. It's called 'dead time' and this is discussed in Section 5.2.

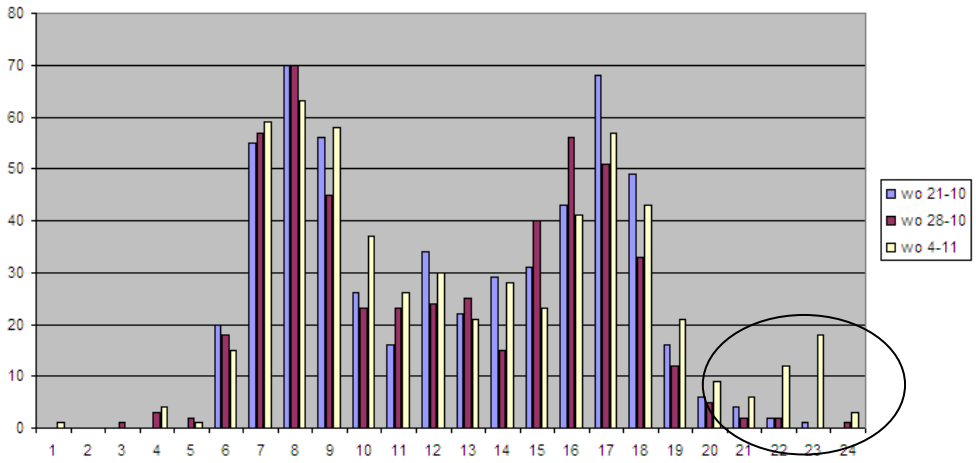

Figure 7. Normal activity on Wednesday 21 October and Wednesday 28 October. One week later, the 4th of November, anomalous events, late at night, where detected by the network. Horizontal axis: Time of day. Vertical axis: number of detections. See text for further details.

Apart from these quantitative measurements and its obvious accompanying errors, a qualitative measurement is required by the IRS software. By detecting anomalies in the regular day detections, i.e. as a relative measure to the regular scheme of events, an alarm can be given of. The number of detections is not relevant. And as shown in Figure 7, this was the case on 4 November. It seemed that extra vehicles have entered the perimeter due to a symposium that was being held that evening. Figure 8 shows the prototype alarm screen with the anomaly detected on 4 November.

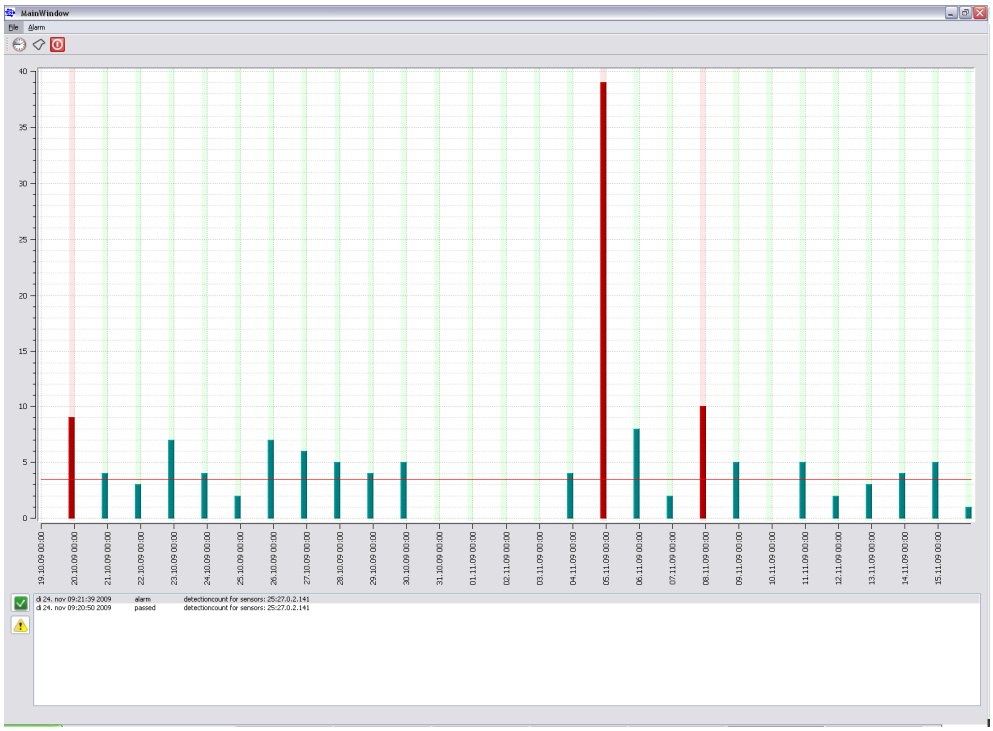

Figure 8. Prototype alarm screen. The software has retrieved three anomalous instances (red bars). Only one is significant enough to be stored as a true anomalous event with a deviation of 40 detections from the regular scheme. The other two short red bars are false alarms. The genuine alarm is the 4 November symposium.

5.2 Dead time restriction

When a sensor is triggered by a target, a short period of time is required for the sensor to get triggered again by a new target. Time is needed for the first target to leave the detection zone. This so-called 'dead time' is a general and known feature of sensor systems. It is mostly hard-coded in the sensor. Two aspects arise. A sensor is called 'parallelisable' if the dead time starts each time a new target is detected within the previous dead time. Thus only one detection is stored, the first one, if all detections (high target density) happen within the dead time. This severely limits the number of detections and does not represent reality much, if reality consists of detection zones with large numbers of targets. A second aspect is a ' non-parallelisable' sensor. Here the new target does not trigger the previous dead time; the first dead time must go by first before any new detection takes place. This also limits the number of detections, yet is still better than the 'parallelisable' sensor. See Figure 9.

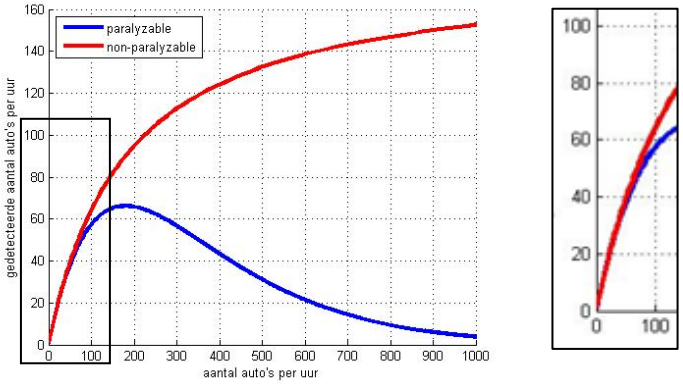

Figure 9. On the y-axis the detected cars per hour. On the x-axis the real number of passed cars per hour. The dead time in this example with the sensor used is 20 seconds. Panel on the right is interesting for correction factor computations.

If traffic density, i.e. detection frequency, is low and every now and then a vehicle or person traverses a cluster of sensors, the dead time does not cause any inconsistencies as long as each detection happens after the dead time interval. This applies, for example, perfectly for border control applications in desolate country sides and other sparse-activity regions.

As mentioned above, for a high throughput network the dead time limitation is clearly a limiting factor for processing every target. From Figure 9 a casual relationship can be used to correct the measurements to certain degree. This is however not trivial, because not all detections are dead time detections. The targets don't follow a homogeneous distribution. If on the other hand a qualitative alarm generator is required, the precise number of detections is not important as long as the regular course of events (or daily scheme) is known and recorded, as was demonstrated in Figure 8. The regular scheme is used as a reference for anomaly detection.

5.3 Corrections

A quantitative analysis requires some form of correction with the help of the relationships given in Figure 9. This correction will result in an even more accurate assessment of the situation if *a priori* information on the maximum number of detections in the detection zone is at hand.

For the test described in Section 5.1 the *a priori* average number of cars per hour is 55 – 75. If we take 65 cars per hour, the number of detected vehicles is approx. 45, see Figure 9, right panel. The correction factor becomes approx. 1.44 and the number of detected incoming vehicles in the morning, 230, now can be computed to a more realistic value of 325. This number does not represent all people inside, as was mentioned above, but is the greater part of 375 – 475, while the remaining people travel by public transport or by other means.

6. SUMMARY AND CONCLUSIVE REMARKS

In this paper first findings are presented on the use of unattended ground sensors for route surveillance. This first test was set up in a brute force manner to see what results could be generated if a robust COTS sensor network was ordered, delivered, unpacked, and quickly installed and placed in position in a relevant environment using IRS software in combination with sensor software. While 24 sensors have been set up in the first place, many sensors showed similar activity detections, others showed hardly any activity. The findings presented are for one representative sensor,

The hardware and the software, i.e. sensor software and IRS prototype software, performed according to the expectations when the qualitative aspect of the IRS research is considered, i.e. giving off an alarm in case a deviation is observed in the regular scheme of events. While this first test concerned relatively simple measurements, some practical problems surfaced regarding specifications and environmental issues. The quantitative analysis, on the other hand, thus required some corrections regarding the dead time interval, which was not known *a priori*. *A posteriori* corrections, made through the known relationships for dead time processes, resulted in good estimations for the measurements performed in the test.

At this moment a good understanding has been acquired of the used COTS network in combination with the prototype IRS software as used in this first test. In the near future the IRS project will look into developments regarding enhancements of the flux measurements and the classification and tracking of one object (phase two). These developments are to be combined with field tests.

ACKNOWLEDGEMENTS

We thank Alle de Jong of the Ministry of Defence for supporting this work. We further thank him and his colleagues 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 *Unmanned/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.

[6] Schoemaker, R., Sandbrink, R., van Voorthuijsen, G., " Intelligent route surveillance" in Unattended Ground, Sea, and Air Sensor Technologies and Applications XI, edited by Edward M. Carapezza, Proceedings of SPIE Vol. 7333 (SPIE, Bellingham, WA 2009) 73330H