Detecting Terrorists:

Requirements and system specifications for a radar-based system

H. Borrion, N. Bouhana, H. Guo, K. Chetty, G. Smith, K. Woodbridge and C. J. Baker
University College London
UCL Centre for Security and Crime Science
Brook House, 2-16 Torrington Place
London - WC1E 7HN, United Kingdom

cscs@ucl.ac.uk

ABSTRACT

In this paper, the authors derive the specifications for a security system capable to detect so-called suspicious human activities using an affordable network of radar sensors. This work constitutes a first step towards the development of a robust day-and-night twenty-four hour surveillance system performing real-time automatic detection of terrorists in public places. Such device would complement the work of screening officers and assist decision-takers by providing information and time required to trigger preventive and protective actions. This paper is the result of a collaborative work undertaken by a team of academics with expertise in both the physical and social sciences at University College London.

1.0 INTRODUCTION

1.1 Defining the problem

Terrorism has remained hard to define, either on a phenomenological, legal or political level. In order to overcome this difficulty and set up frameworks for collaboration and prevention, international bodies such as the United Nations have adopted a pragmatic approach. Until the attacks of 2001, which altered the international political environment with the consequences that we know, legislation addressed such concrete events as hijacking or hostage taking, rather than nebulous 'terrorist acts'.

1.2 Levels of crime prevention

The prevention of criminal and violent behaviour, such as terrorism, can be effected on three levels. This nomenclature is borrowed from the medical field. Each level of intervention is situated at a distance (spatial and temporal) from the criminal event to be prevented. *Primary prevention* addresses general risk factors, which correlate with criminal involvement, such as poor parenting skills, sometimes before the potential offender is even born. Primary crime prevention can be built into larger social programs and implemented universally. Its aim is to prevent the onset of criminality in individuals. *Secondary prevention* targets individuals, which have already demonstrated a propensity for deviant behaviour, or which are considered at risk of doing so. Offender rehabilitation programs fall into that category. *Tertiary prevention* occurs in response to specific acts of crime. It encompasses investigative efforts after a crime has been committed, in order to prevent further crimes, as well as situational detection and prevention of criminal behaviour.

In theory, if primary prevention were successful, further levels would not be required. However, the current level of understanding of the causes of criminal and violent behaviour, as well as the best way to

intervene on these causes, is such that primary prevention is an insufficient means of crime prevention. Proponents of tertiary prevention argue against proponents of primary and secondary interventions that the distal causes of crime (poor parenting or social disorganisation) and individual criminal propensity once acquired are harder to alter than proximal (immediate) crime factors (such as, for example, the absence of an alarm system against intruders, or of security measures in an airport) (Newman, 1997).

1.3 Technology and crime prevention

Technology can contribute to all levels of crime and terrorism prevention, but so far has made the most contribution, unsurprisingly, at the tertiary level.

Within the framework of Crime Prevention Through Environmental Design (Jeffery, 1971), technology has informed or has been incorporated into the design of the human built environment, including objects of everyday life, to prevent crime by acting upon criminal decision making (for example, designing underground stations with no columns, so as to offer no hiding place to robbers) or suppressing opportunities for crime (for example, designing mobile phones impervious to cloning).

Indubitably, technology's most visible contribution has been to the field of crime and terrorism investigation, through advances in the forensic sciences. Notwithstanding technology's contribution to criminal and terrorist investigations, the goal remains to prevent violent and destructive events from occurring in the first place.

2.0 TERRORIST DETECTION

2.1 Behind the words

The term ‘terrorist detection’, despite having a direct relation to a key operational aim, has in fact a rather imprecise meaning. As mentioned above, there is no global agreement on what a terrorist is. Furthermore, detection is a rather ambiguous word which bears different meanings to different professional groups. As a result, this expression is of limited use to criminologists who seek to understand the causes and manifestations of terrorism, to engineers who seek to develop state-of-the-art security technologies and to practitioners who aim at preventing so-called terrorist attacks. Instead it is admittedly more useful to provide a more limited, yet more accurate, description of the role and properties that security technologies should have to protect our societies and its citizens.

2.2 Principle of detection

The following ought to contribute to building a foundation for a better understanding and future development of technology-based security devices, starting by recognizing that technologies have specific capabilities that can only be applied to certain systems and in certain environments.

First, it should be recognized that the term ‘terrorist’ has different meanings to different populations and that no single piece of technology can be usefully applied to a loosely defined system or problem. In the context of this paper, we are interested in a person or a group of people who actively seek to cause physical harm to other people (e.g. the public, employees, security or military patrol), illegally gain access to or inflict serious damages to infrastructures (e.g. building, airport, embassy…). This precision inherently limits the scope of this paper to the majority of terrorists who have to expose themselves physically in order to conduct an attack.

Recent publications show that information and communication networks are perceived to be increasingly at risk; it must be mentioned that the reasoning developed in this paper does not necessarily apply to potential cyber-terrorists who may chose to operate remotely. It should also be mentioned that although knowledge of motivational factors may contribute to enhancing the performance of some security technologies, this information is not widely exploited by existing systems and should certainly not be considered as a key requirement for any system.

Second, as far as technology is concerned, 'detection of terrorists' does not exist as such. It is important to understand that technology-based detection is an indirect process by which the presence of a terrorist or group of terrorists is inferred from the detection of associated features. In fact, it can be seen through the following examples that this particularity of detection is not restricted to the sole aim of detecting 'terrorists'.

- In forensic investigation, the past presence of a suspect at the crime scene is often detected through detection of its fingerprints on a surface (e.g. door, glass, etc). In this example, the detection of an individual's presence is achieved through detection of a certain feature, i.e. a spatial pattern of molecules, which is characteristic to this individual.
- One could also draw a parallel with the biochemical field where research works on jellyfish have enabled scientists to understand that the presence of calcium ions can be detected by introducing proteins of a certain type in a sample. Their simultaneous presence in the solution results in the binding of the ions with the proteins, which is a fluorescent reaction that can be observed by human eyes. In this example, the observation of the calcium ion's characteristic property requires scientists to employ a more intrusive process.

Despite obvious differences, both examples tend to confirm that the detection of 'terrorists' requires terrorist-specific features to be identified and searched for.

2.3 Feature selection

The selection of characteristic features that would allow terrorist detection to be carried out successfully is both a critical and difficult stage in the design of detection systems. It must also be understood that it has direct implications on the operational success of the technology and ultimately on its future adoption.

Consideration for feature selection should include the following criteria: the selected features should be both

- Uniquely associated with the subject of interest or shared with a limited number of others groups
- Detectable using technologies that can meet the requirements of a given operational environment.

Failure to select uniquely associated features would result in a large number of false positives, making the system non operable. Failure to select detectable features would result in large number of false negatives, making the system useless at best and counter-effective at worst.

Whilst it is still virtually impossible to create and implement a technology that can perform detection of unknown terrorist prior an attack, it is believed that such a technology would aim at detecting terrorist-specific features that would be associated with either terrorist's *identity, weapon* or *behaviour*.

2.4 Identification and recognition

Prior knowledge of terrorist identities could be used to detect their presence in a public space, providing it is possible to compare people's identity with (all) those of (all) terrorists. The latter information may be publicly available or obtained by using intelligence analysis techniques (e.g. social network analysis). In both case, detection systems rely on a combined use of watch-lists and real-time recognition systems.

Various detection systems have already been designed and tested in real conditions. The principles behind most of them fall in two categories: cooperative or non-cooperative detection.

For techniques of the first kind, individuals are requested to provide a 'proof of identity' such as an official document (e.g. driving licence, ID-cards, etc.) or a biometric-identifier (e.g. DNA, fingertip, iris, etc.). These are used for large public systems of identification. They are generally compulsory and visible to the public eyes, including to terrorists' ones.

For techniques of the second kind, individual identity may be obtained without cooperation from the subject. Systems that fall in this category are mainly non-intrusive and may thus be used for covert operations, depending on their performance. In this case, detection of terrorists can rely on the combined use of remote-sensing devices, biometric watch-lists and biometric-based recognition technologies. These may be a combination of networks of cameras, libraries of terrorists' portraits, and face-recognition algorithms. Such systems have already been implemented and tested in public spaces such as these that hosted the American Super Bowl sport event in 2001 (McCullagh, 2001 and Bowyer, 2004). This trial led to the arrest of wanted criminals; none of them were terrorists.

Identity-based techniques for terrorist detection require large infrastructure and a priori knowledge. Their capability is limited and their use is restricted to certain applications as it may not always be possible to meet these conditions. These techniques would be mostly ineffective against unknown terrorists and against terrorists that use multiple identities.

2.5 Detecting concealed weapons

It is generally the case that terrorists hide weapons or carry weapons with them before an attack. Weapons that are 'popular' amongst terrorists include improvised explosive devices, knives, guns, etc.

During the last thirty years, a number of security technologies have been developed to detect these weapons. These include metal detector, radar systems, terahertz imaging devices, x-ray scanners, etc. More information on the use of radar imaging to weapon detection can be found in a previous NATO article by Griffiths and Baker (2006).

Their effectiveness in real environment is difficult to measure and queues at international airports suggest that more research efforts need to be placed in these areas in order to create efficient and reliable security systems.

2.6 Detecting deception and suspicious behaviour

The Grail, so to speak, is the ability to detect deception and suspicious behaviour, even in the absence of direct contact with the suspect or suspects. So far the preference remains for human-based techniques of detection.

The assumption is, of course, that deception and malicious intent is detectable through observation of the individual's behaviour, alone and in relation to his or her environment (as opposed to detectable through measurement of internal physiological responses, such as using polygraphs to detect concealed information (e.g. Verschuere *et al*., 2006), or employing neuroimaging techniques to observe neural responses thought to be associated with telling lies (e.g. Abe et al., 2007).

It is also assumed that deception and malicious intent can be detected in response to specific external stimulus (for example, a tone of voice or a visual cue) applied to the individual.

Police interrogators rely on these assumptions when interrogating suspects. They employ a number of interview styles (e.g. accusatory, information-gathering, behaviour analysis) in order to elicit verbal and behavioural cues, which indicate deceit. This identification can be based on experience, specialised training, or both. Research on police interrogations suggests that eliciting cues and correctly interpreting them depends on the choice of interviewing style, the non-reliance on stereotypical cues (e.g. fidgeting, averting eyes) to determine truthfulness or deception, and experience in interviewing suspects (Mann et al., 2004). The development of technologies to assist the detection of deception through analysis of facial and bodily movements is still in its infancy, though the research field is active (e.g. Dente et al., 2006; Rothwell *et al*., 2006).

These assumptions are also the basis of behavioural screening techniques used by immigration and security personnel in airports. Anyone who has ever travelled through an Israeli airport will have noticed that the behaviour of immigration officers differs frankly from behaviour in other countries. In the United States, the Screening Passengers by Observation Techniques [SPOT] programme has been rolled out by the Transportation Security Administration in forty major airports. Teams of trained officers observed travellers while they stand in line in various locations throughout the airport, looking for obvious signs of suspicious activity (e.g. wearing a winter coat in summer) or more subtle clues (e.g. facial movements suggesting emotional concealment). Passengers are unwittingly scored on a list of thirty questionable behaviours. ("Which Travellers Have 'Hostile Intent'? Biometric Device May Have the Answer," *The Wall Street Journal*, 14 August 2006). The preference among security practitioners remains for human-based detection supported by technology, such as biometric identification. To date, SPOT has led to the arrests of wanted individuals, would-be kidnappers and illegal immigrants, but not yet of a terrorist suspect (Source: TSA Website).

2.7 The future of technology-based profiling systems

It seems now widely accepted that technology will play a key role in tomorrow's counter-terrorism strategy. However, it is not clear whether it will be sufficiently effective to detect the presence of unknown terrorists who intend to carry out an attack.

As pointed out, 'visual' detection of deception rests on the assumption that deception manifests itself in the behaviour of the individual. What behavioural aspects should be the focus of attention, and whether all individuals betray themselves similarly in all settings, remain open research questions.

Future research efforts should focus on the identification of features that are characteristic to terrorists. More work also needs to be done to understand the variation of the environment prior terrorist attacks. To overcome the problem of replicating real-life settings in laboratory, data should be collected from automatic experimental systems operating in real environment.

The following chapter presents the principle and specification for a radar system that could be used to measure and analyse human behaviours at individual or group level. The dataset would then be processed by machine-learning techniques to identify the presence of 'characteristic features' that could used to detect the presence of abnormal behaviours of the individual or an environment. . The radar should be seen as the first component of a more complex technology-based profiling system which may include a number of other sensors.

3.0 RADAR BASED SYSTEM FOR TERRORIST DETECTION

3.1 Introduction

A large number of wireless local area networks (WLAN) are being developed based on the IEEE 802.11

standards. The three most commonly being deployed are 802.11a, 802.11b and 802.11g. These protocols operate in either the 2.4 GHz or 5 GHz spectrum bands and have different modulations and coding schemes which change with data rate and user range. These transmissions are becoming widely available and are therefore a reliable and regular transmission of opportunity for wireless based passive radar. Such radars have the advantage of measuring range, range rate and are able to track movement. Development of a surveillance capability from such a ubiquitous and accessible source will have major implications for improving security in all types of buildings and in the identification and tracking of goods and people. This type of passive sensing could be used in public areas such as railway and airport terminal or private commercial premises such as office buildings or warehouses. Some preliminary waveform analysis and simple detection experiments have been reported in a previous paper (Guo et al, 2007). In this work we examine in more detail the radar detection properties of an 802.11b beacon signal.

The target detection experiment was set up in a low clutter outdoor environment (college sport field). The WiFi transmitter (DWL-2000AP+) was configured to transmit in channel 6 of the Industrial, Scientific and Medical (ISM) license free frequency band, with a centre frequency of 2.437 GHz. The system, consists of three nodes; the WiFi transmitter, the target echo receiver and a reference receiver to enable measurement of the direct signal. Theoretically, the maximum EIRP of the WiFi device is 100 mW (20 dBm) (Griffiths and Baker, 2005), so the maximum transmitter output is 15 dBm based on the transmitter antenna gain which is 5 dBi and assuming zero loss. The receiver antenna gain is 24dBi; therefore, the maximum detection range for a 1 m^2 RCS human sized target in the monostatic configuration is approximately 120 meters. In order to simulate the envisioned indoor application more closely, the maximum distance between the three nodes were set to 50m and is shown schematically in figure 1.

Two moving human targets were measured which moved towards the receiver at a speed of approximately 1 m/s and a spacing of 12 m or 35 m (Figure 1). This distance is much smaller (12 m) or larger (35 m) than the theoretical bistatic resolution value calculated above. This was designed to test the target resolution capabilities of the system. The targets at 12 m separation can therefore effectively be expected and considered as a single target.

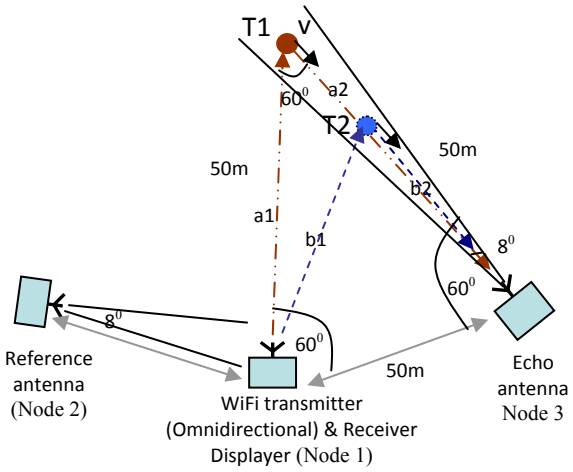

Figure 1 – Geometry configuration for WiFi based passive radar measurement. The filled and dotted circles represent the human targets moving towards the receiving antenna.

3.2 Doppler signal processing

To resolve the human target moving at a speed of 1m/s, an integration time of at least 62.5 ms is needed. This has been calculated from the bistatic Doppler equation (1). (Willis, 2005)

$$\Delta f = \frac{1}{T} < f_D = \frac{|v| \cdot \cos(\beta/2)\cos(\alpha)}{\lambda} \qquad (1)$$

where Δf is the Doppler resolution, T is the observation time. f_D is the Doppler shift, v is the target velocity. λ is the wavelength which is 0.125. α = the angle between the bistatic bisector and the direction of target motion

Following the record of the experimental data, the 100 ms and the 300 ms durations of captured signal were subsequently processed for the cross ambiguity function analysis using the reference and target echo signal. In Figure 2, the cross ambiguity diagram of 100 ms integration time is displayed. The presence of the target can be detected by an asymmetry in the Doppler sidelobes. Theoretically, the target appears at about (50 m, 12 Hz) (black dashed circle) in Figure 2. Thus the target in the predicted region has been detected but is being masked somewhat by the sidelobes caused by direct signal breakthrough from the transmitter. Although it appears to be easier to detect a long range target, for example around 300 m, this is probably not going to be generally of interest in indoor applications due to attenuation and transmitter range limitations.

To reduce the Doppler sidelobe effect, the integration time can be increased to a full 300 ms data whose analysis result is processed as in the Figure 3. Compared to the above figure, the Doppler sidelobe effect is being reduced. However, the target is still not very clearly detected due to the correlation from the reference and the interference signal in reflected signal.

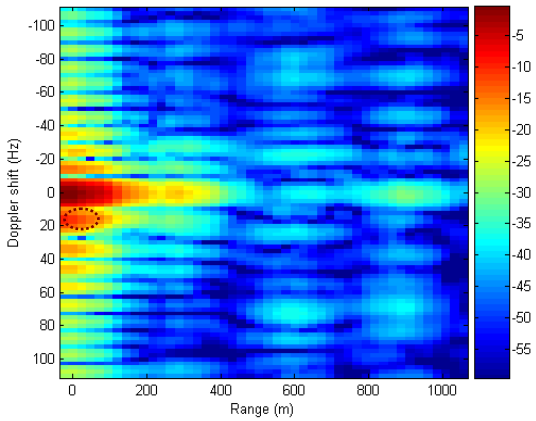

Figure 2 – Cross Ambiguity diagram for 100 ms integration time when the target is moving towards the receiver

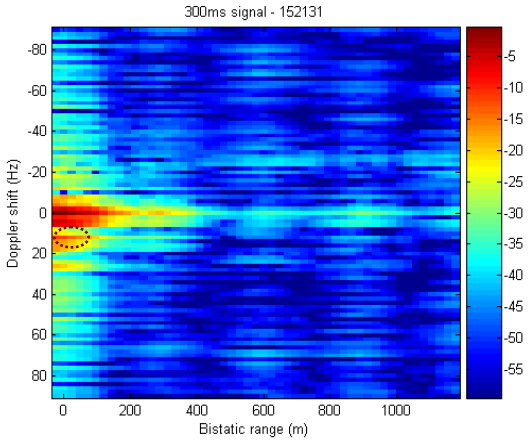

Figure 3 – Cross Ambiguity diagram for 300 ms integration time when two targets (12 m) are moving towards the receiver

As mentioned in previous text, the two targets were measured. However, because of the sidelobe effect, even the distance between two targets is long enough, it still impossible to separate the targets based on the resolution analysis (Figure 4), except for the stronger power which is due to one of the target which was moving closer to the receiver.

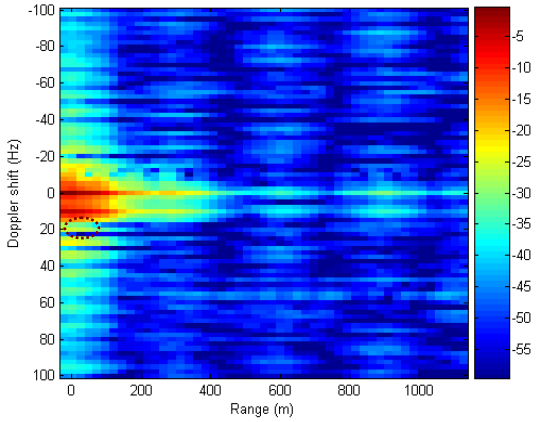

Figure 4 – Cross Ambiguity diagram for 300 ms integration time when two targets (35 m) are moving towards the receiver

3.4 Discussions

These preliminary results presented show that the 802.11 Beacon transmission can potentially be used as a transmitter of opportunity for a passive radar system. The Doppler resolution appears to be suitable for detection of moving human targets although interference from direct signal breakthrough is a potential problem as previously seen in other studies (Guo, 2007). This can be quantified for this experiment to give an idea of the suppression needed. In this case the ratio of the received power to the direct signal breakthrough power is as follows:

$$\frac{P_R}{P_D} = \frac{\sigma_B L^2}{4\pi (R_T R_R)^2} \cdot \frac{G_{Rmain}}{G_R} \qquad (3)$$

where PR and PD are the power of the reflected signal and the power of direct signal both received by echo antenna, L is the bistatic baseline. RT and RR are the distance between the transmitter and target, receiver and target, respectively. G_{Rmain} is the peak gain of the surveillance antenna, G_R is the antenna gain at 60^0 away from the peak which is -30 dB in our experiment. This seems to be promising for detection with the direct signal interference in the reflected signal. However, although the SIR ratio of the passive radar is acceptable, the target is still invisible because of the sidelobe from the Doppler-range figure above. Besides, in a typical indoor application it can be expected that multipath and clutter would be significant.

In a real situation echoes could be received from a number of transmitters. Wireless LAN protocols, such as the IEEE 802.11g standard, allow for several different RF channels to be used. Multiple wireless LANs may therefore exist in the same geographical area so long as they operate on different channels. If the passive radar system were able to receive on all channels of the protocol there may be an appreciable increase in the information available for a target. Such capability expansion will require further investigation. This study had only examined the situation of an idle network emitting the Beacon signal only. This would be the scenario in quiet areas and periods so has relevance to, for example, night security applications. However further work on typical user active environments is under way.

ACKNOWLEDGEMENTS

We thank the organisations, including the UK Ministry of Defence, the UK Engineering and Physical Sciences Research Council, who have supported the various pieces of work whose results are reported here.

REFERENCES

[1] Abe, N., Suzuki, M., Mori, E., Itoh, M. and Fugii, T. (2007). "Deceiving others: Distinct neural responses of the prefrontal cortex and amygdale in simple fabrication and deception with social interaction." *Journal of Cognitive Neuroscience*, 19(2): 287-295.

[2] Bowyer, K. W. (2004) “Face recognition technology: Security versus privacy” *IEEE Technology and Society Magazine*, 9-20.

[3] Dente, E., Bharath, A.A., Ng, J., Vrij, A., Mann, S., and Bull, A. (2006). "Tracking Hand and Finger Movement for Behaviour Analysis." *Pattern Recognition Letters*, 27(15): 1797-1808.

[4] Griffiths H. D. and Baker C. J. (2005), "Passive coherent location radar systems. Part 2: Waveform properties", *IEE Proc., Radar Sonar Navig*., 152.

[5] Griffiths H.D. and Baker C.J. (2006), “Radar Imaging for combating terrorism”, *NATO’s Advanced Study Institutes on Imaging for Detection and Identification.*

[6] Guo H. Coetzee S., Mason D., Woodbridge K. and Baker C. (2007), "Passive radar detection using wireless networks", *European Radar conference*, Edinburgh.

[7] Jeffery, C.R. (1971). *Crime Prevention Through Environmental Design*. Beverly Hills, CA: Sage.

[8] McCullagh D. (2001), “Call it Super Bowl Face Scan I”, *wired.com.* Feb. 2 2001

[9] Mann, S. And Vrij, A. (2006). "Police Officers' Judgements of Veracity, Tenseness, Cognitive Load and Attempted Behavioural Control in Real-Life Police Interviews." *Psychology, Crime and Law*, 12(3): 307-319.

[10] Mann, S., Vrij, A., Bull, R. (2004). "Detecting True Lies: Police Officers' Ability To Detect Suspects' Lies." *Journal of Applied Psychology*, 89(1): 137-149.

[11] Newman, G. (1997). "Introduction: Towards a Theory of Situational Crime Prevention." In G. Newman, R.V. Clarke and S.G. Shoham, *Rational Choice and Situational Crime Prevention*, pp. 1-24. Aldershot: Dartmouth Publishing.

[12] Rothwell, J., Bandar, Z., O'Shea, j., McLean, D. (2006). "Silent Talker: A New Computer-Based System for the Analysis of Facial Cues to Deception." *Applied Cognitive Psychology*, 20(6): 757-777.

[13] Verschuere, B., Crombez, G., Koster, E.H.W. and Uzieblo, K. (2006). "Psychopathy and physiological detection of concealed information: A review." *Psychologica Belgica*, 46(1-2): 99-116.

[14] Willis, N. J. (2005), Bistatic Radar, *SciTech Publishing*