Defence Research and Development Canada
Recherche et développement pour la défense Canada

DEFENCE R&D DÉFENSE

Considerations for Wireless Network Situational Awareness

James E. Gort

The scientific or technical validity of this Contract Report is entirely the responsibility of the contractor and the contents do not necessarily have the approval or endorsement of Defence R&D Canada.

Defence R&D Canada – Ottawa
CONTRACT REPORT
DRDC Ottawa CR 2006-238
November 2006

Considerations for Wireless Network Situational Awareness

James E. Gort
TRM Technologies Inc.

Prepared by:

TRM Technologies Inc.
151 Slater Street Suite 100
Ottawa, Ontario K1P 5H3

Contract number: W7714-6-3307
Contract Scientific Authority: Lynne Genik, DRDC Ottawa, 3701 Carling Ave, K1A 0Z4

The scientific or technical validity of this contract is entirely the responsibility of the contractor and the contents do not necessarily have the approval or endorsement of Defence R&D Canada.

Defence R&D Canada – Ottawa

Contractor Report
DRDC Ottawa CR 2006-238
November 2006

Abstract

Within the realm of information operations, computer network defence (CND) focuses on managing the vulnerabilities and risk inherent in all computer networks. While much of the current research in the field of CND situational awareness (SA) is focusing on a bottom-up approach of how to define meaning out of the abundance of sensor information, DRDC has done work in defining the information requirements for CND SA from a top-down approach. The Joint Network Defence and Management System (JNDMS) is a Technical Demonstrator Project (TDP) implementation of a service that will provide this situational awareness; however, the focus is on wired networks. The question which this report addresses is: What is important for situational awareness in a wireless network and how does it differ from that of a wired network?

Résumé

Dans un monde axé sur les opérations d'information, la défense des réseaux informatiques (CND) s'attache surtout à gérer les vulnérabilités et les risques inhérents à tous les réseaux informatiques. Alors que la majorité des recherches dans le domaine de la connaissance de la situation (SA) en CND gravite autour d'une approche ascendante pour soutirer de l'information parmi le fort volume de données captées, le RDDC a entrepris des travaux sur la définition de la connaissance de la situation en CND en recourant à une approche descendante. Le système JNDMS (système de gestion et de défense conjoints de réseau) est une réalisation de démonstration technique (TDP) d'un service qui fournit cette connaissance de la situation. Cependant, il concerne les réseaux câblés. La question abordée par ce rapport est : qu'est-ce qui est important pour la connaissance de la situation dans un réseau sans-fil et comment cet aspect est-il différent de ce qui prévaut dans un réseau câblé ?

This page intentionally left blank.

Executive summary

Within the realm of information operations, computer network defence (CND) focuses on managing the vulnerabilities and risk inherent in all computer networks. While much of the current research in the field of CND situational awareness (SA) is focusing on a bottom-up approach of how to define meaning out of the abundance of sensor information, DRDC has done work in defining the information requirements for CND SA from a top-down approach. The Joint Network Defence and Management System (JNDMS) is a Technical Demonstrator Project (TDP) implementation of a service that will provide this situational awareness; however, the focus is on wired networks. The question which this report addresses is: What is important for situational awareness in a wireless network and how does it differ from that of a wired network?

This report identified three major areas where the inclusion of wireless networks into the SA model could impact the model:

- vulnerabilities unique to wireless networks
- safeguards unique to wireless networks
- situational awareness data unique to wireless networks

The report went on to describe 15 specific wireless network vulnerabilities, 18 wireless network safeguards, and 8 areas where additional wireless network information can be captured and sent on to JNDMS for analysis.

Not all of the above are mutually exclusive; the type of routing protocol chosen influences all three area. The type of wireless network architecture (e.g., MANET, fixed star, full mesh, etc.) also influences most of the areas.

Many types of wireless networks were addressed, and there are consequently many variables (e.g., system type, topology, security policies, routing protocol, etc.) affecting SA. The report provides the background necessary to identify specific SA impacts once any particular system is chosen and the variables selected.

From a global perspective, wireless networks require considerably more “SA data” than their wired counterparts. Their nodal mobility and rapidly changing link characteristics are two of the most important factors. In wired networks, topology messages certainly need not be sent every few seconds as is required in MANETs, for instance.

The frequency of information and bandwidth required to send timely SA data were estimated, and found (in most cases) to be a small impact on link capacity.

There was found to be no need to change DRDC’s existing SA model’s terminology or overall approach to provide meaningful situational awareness for wireless networks

Gort, J. 2006. Considerations for Wireless Network Situational Awareness. DRDC Ottawa CR 2006-238, Defence R&D Canada - Ottawa.

Sommaire

Dans un monde axé sur les opérations d’information, la défense des réseaux informatiques (CND) s’attache surtout à gérer les vulnérabilités et les risques inhérents à tous les réseaux informatiques. Alors que la majorité des recherches dans le domaine de la connaissance de la situation (SA) en CND gravite autour d’une approche ascendante pour soutirer de l’information parmi le fort volume de données captées, le RDDC a entrepris des travaux sur la définition de la connaissance de la situation en CND en recourant à une approche descendante. Le système JNDMS (système de gestion et de défense conjoints de réseau) est une réalisation de démonstration technique (TDP) d’un service qui fournit cette connaissance de la situation. Cependant, il concerne les réseaux câblés. La question abordée par ce rapport est : qu’est-ce qui est important pour la connaissance de la situation dans un réseau sans-fil et comment cet aspect est-il différent de ce qui prévaut dans un réseau câblé ?

Ce rapport dégage trois zones importantes où l’inclusion de réseaux sans-fil dans le modèle SA pourrait le perturber :

- vulnérabilités exclusives à des réseaux sans-fil;
- protections exclusives à des réseaux sans-fil;
- données sur la connaissance de la situation uniques aux réseaux sans-fil.

Ce rapport réussit à décrire 15 vulnérabilités propres aux réseaux sans-fil, 18 protections exclusives aux réseaux sans-fil et 8 secteurs où il est possible de capturer de l’information d’un réseau sans-fil et la transmettre au JNDMS pour analyse.

Les risques précédents ne sont pas tous mutuellement exclusifs; le type de protocole de routage choisi a une incidence sur trois secteurs. Le type d’architecture de réseau sans-fil (p. ex. MANET, étoile fixe, maillés) a également une incidence sur la plupart des secteurs.

Plusieurs types de réseaux sans-fil sont étudiés, et de ce fait il y a de nombreuses variables qui affectent la connaissance de la situation (p. ex. type de système, topologie, stratégies de sécurité, protocole de routage).

D’un point de vue général, les réseaux sans-fil exigent beaucoup plus de « données SA » que leurs pendants câblés. Les caractéristiques de la mobilité de leurs noeuds et celles des liaisons évoluant rapidement sont les deux facteurs majeurs. Dans les réseaux câblés, on doit cependant envoyer des messages de topologie à quelques secondes d’intervalle, comme dans MANET.

On a estimé la fréquence et la largeur de bande requises pour communiquer rapidement les données SA et on a pu conclure que dans la plupart des cas l’impact était négligeable sur la capacité de la liaison.

On a trouvé qu'il n'était pas nécessaire de changer la terminologie ou l'approche globale du modèle SA existant à la RDDC pour obtenir une bonne connaissance de la situation dans les réseaux sans-fil.

Gort, J. 2006. Considerations for Wireless Network Situational Awareness. DRDC Ottawa CR 2006-238 R & D pour la défense Canada - Ottawa.

This page intentionally left blank.

Table of contents

List of figures

List of tables

This page intentionally left blank.

1. Introduction

Within the realm of information operations, computer network defence (CND) focuses on managing the vulnerabilities and risk inherent in all computer networks. While much of the current research in the field of CND situational awareness (SA) is focusing on a bottom-up approach of how to define meaning out of the abundance of sensor information, Defence Research and Development Canada (DRDC) has done work in defining the information requirements for CND SA from a top-down approach. The Joint Network Defence and Management System (JNDMS) is a Technical Demonstrator Project (TDP) implementation of a service that will provide this situational awareness; however, the focus is on wired networks. The question which this report attempts to address is: What is important for situational awareness in a wireless network and how does it differ from that of a wired network?

To ensure that most types of wireless technologies which are or could potentially be used in a military environment were included in the analysis, 18 separate wireless systems were studied, including military and civilian, terrestrial and satellite.

The CND SA model [1] was examined to determine the unique wireless characteristics which could impact SA. It was determined that those characteristics could best be grouped using the terminology of the SA model:

- vulnerabilities unique to wireless networks
- safeguards unique to wireless networks
- situational awareness data unique to wireless networks

The characteristics related to wireless networks in each of the above broad categories were numerous; the ones judged to have the greatest influence on SA were highlighted and briefly described. The caveat is that only three wireless network routing protocols were included due to the study terms of reference and limitations. Including such routing protocols as dynamic source routing (DSR) [2] would have been desirable, although probably not significantly affecting the major findings.

To provide timely wireless network situational awareness information to JNDMS, the frequency of information updates and bandwidth required was estimated.

The major features impacting the SA model were highlighted, and changes to the SA model to include wireless networks were recommended. Future work in this area was identified.

Following the introduction, a literature review on top-down wireless network situational awareness is presented in section 2. Section 3 attempts to place the wireless network information in the context of CND SA requirements. Section 4 is a more detailed look at the wireless network SA issues, including wireless network safeguards, vulnerabilities, and SA data available from various sources. The results are applied to the SA model in section 5. References are given in section 6.

2. Literature Review

2.1 Purpose

This literature review examines professional, academic, and unclassified military literature on top-down wireless network situational awareness.

2.2 Summary of Results

There is much literature on bottom-up wireless network situational awareness. That literature generally focuses on the abundant wireless sensor information, routing information available at the protocol level, mobile agent technology, and wireless network characteristics which could be used to extract information which can answer commander-level questions, that is, provide at least components of situational awareness. Some of the more relevant literature is in section 7.

This section focuses on a relatively small subset of literature available on top-down wireless network situational awareness.

Recent work at Defence Research and Development Canada (DRDC) [1] defines information requirements needed to achieve CND SA. A common operating picture (COP) is one of possibly several tools that can be used to achieve SA. Lefebvre et al [1] model CND SA as a parallel domain of military operations to battlefield SA, with each supporting an Observe-Orient-Decide-Act (OODA) cycle. This paper also. defines a set of abstracted services as the means to define a military commander's objectives from a computer network. These abstracted services would be defined in terms of quality of protection (QoP) along the lines of confidentiality, integrity and availability. These services then become the semantics for describing CND SA through indications where services have been, or are potentially capable of being, impacted. Although this paper does not explicitly mention the unique questions a commander may ask relevant to wireless SA, the abstracted services are, in general, common to all computer networks and may be used to form a baseline of information requirements wireless CND SA.

Froh [3] defines the need for Coalition Information Assurance (CIA) COP for both strategic and tactical computer networks. Again, wireless networks are not explicitly mentioned, but the CIA COP architecture can readily be adapted to tactical wireless networks in particular and to wireless SA in general.

Breton and Rousseau [4] provide a review of research into SA, and summarizes the principal SA functions as:

- Perception - What are the current facts?
- Comprehension - What is actually going on?
- Projection - What is most likely to happen?
- Resolution - What exactly shall I do?

These are not particular to wireless network SA, but are common to all environments. They therefore can be used to determine the relevant functions which must be provided to achieve wireless network SA.

Salerno et al [5] define a conceptual information flow model for fusing information into SA. They also define measures of performance (MOP's) and measures of effectiveness (MOE's) to determine how well the fused information satisfies SA requirements. But considering SA from a perspective of fusing information to meet the requirements is a bottom-up approach to the problem. Although its principles can be used in wireless network SA, the model does little to shed additional light on problems unique to wireless network SA.

Cumiford [6] postulates that to achieve cyber situational awareness for defensive capabilities in the face of hostile attacks, it is critical to understand the complexity of such a domain. He describes the domain as characterized by sets of complex, interacting issues that are ill-defined, ambiguous, and evolving in time. Although the paper describes what he considers essential characteristics for the achievement of cyber SA capability, as well as characteristics for approaching higher level SA behaviour, it is only indirectly applicable to wireless network SA.

More directly applicable to wireless network SA is the paper by Migas et al [7]. They propose a mixture of static and mobile agents to gather information relevant to ad hoc networks, which can then be used for routing purposes or discovering the time-dependent network topology. Such a technique is very useful to provide wireless network SA, but is again a bottom-up approach to the problem.

Another paper dealing directly with the wireless SA problem is Bordetsky et al [8]. They propose a means of providing feedback (which they term 'Network Awareness', also interpreted as 'situational awareness') to users for wireless peer-to-peer collaborative environments. As part of this work, they investigated the Complex Humanitarian Emergency (CHE) Situational Awareness Tool (SAT), which include software agents which provide a number of SA functions. They also included Defence Advanced Research Projects Agency's (DARPA's) techniques to control, coordinate, and manage large systems of autonomous software agents (employing the Control-of Agent-Based Systems – CoABS) grid. Their experiments and results provide good insight into the types of feedback which could support wireless SA, at least from a bottom-up approach.

Similarly, papers by Li and Lamont [9] and Chandra et al [10] describe topology and service discovery mechanisms using certain capabilities of the wireless protocols. Although useful in providing SA information, it does so as a bottom-up approach.

Although a few references provide generic SA information requirements which could be adapted to a wireless network environment, and a few references deal with delivering bottom-up wireless SA functions, no references have been found which specifically address a top-down wireless network SA approach.

There are various global initiatives underway which are dealing directly or indirectly with wireless SA, some of which are briefly outlined below:

Defence R&D Canada [1] is researching CND SA from a top down approach. Some of the strategic objectives of DRDC research include knowledge modelling, discovery and creation for improved situational awareness. The Joint Network Defence and Management System (JNDMS) Technical Demonstration Project (TDP), an initiative of the Network Information Operations (NIO) Section at DRDC, is a current area of R&D, whose goals are to:.

- Provide commanders, network controllers and security analysts with an integrated computer network defence SA picture of the computer networks being used for military operations
- Support operation-centric computer network defence and network management
- Support sharing of network information among CF and international coalition partners to enhance the CF ability to identify network threats and support network defence within coalition operations

The U.S. Department of Defence Research Projects Agency has initiated a Knowledge Based Networking project, which is examining wireless network SA from the standpoint on mobile ad hoc networks (MANETS) and software defined radio technology.

The U.S. National Science Foundation has several wireless network research programs. In particular, the Information and Intelligent Systems (IIS) Division has a program on “Data, Inference, and Understanding”, which includes components of wireless network SA.

The Swedish Defence Research Agency is researching problems, including SA, of secure MANETS in tactical military use. They also developed a Modelling and Simulation (M&S) Testbed Framework to facilitate research activities in wireless sensor technology, fusion and decision support. The framework facilitates research activities through the creation and sharing of common resources like scenario generators, simulation engines, sensor/target models and visualisation tools.

The National Institute of Standards (NIST) Computer Security Resource Centre has a number of mobile agent projects, the results of which could contribute to wireless SA. They also have a project on MANET intrusion detection systems which could have application to wireless network SA.

The U.S. National Telecommunications and Information Administration Institute for Telecommunications Sciences has developed wireless network discovery tools which can collect link and node information to determine wireless network behaviour and network topology.

The University of California has a project on Intrusion Detection for tactical Mobile Ad Hoc Networks, considering information provided by AODV, OLSR, and other protocols.

Iowa State University also has a project on Intrusion Detection for tactical MANETS, using mobile agents to provide SA.

The U.S. Army has a set of network operations (NETOPS) tools, applicable to a wireless environment, comprising the following functional areas:

- Systems and network management (S&NM). This consists of classic FCAPS—fault, configuration, accounting, performance and security—management. The focus is on assured system and network availability, as well as information protection. There are four major sub-functions under S&NM: systems management, network management, satellite communications management and electronic spectrum management.

- Information assurance (IA) and computer network defence (CND). This functional area focuses on protection, monitoring, detection, analysis and response capabilities necessary to ensure end-to-end availability of friendly information systems while denying adversaries access to the same information systems.

- There are three major sub-functions in IA/CND: protection, detection and response. Protection covers prior actions taken to counter vulnerabilities, such as firewall systems, cryptography and communications security. Detection includes the monitoring of information systems to sense abnormalities such as damage, attack, unauthorized modification or performance degradation. This is where intrusion detection systems and similar anomaly monitoring apparatuses are used. Response includes the actions taken to mitigate the operational impact of an attack, damage, performance weakness, intrusion or similar event. It also involves restoration of essential systems to full capability.

- Information dissemination management (IDM). This focuses on providing the right information to the right person in the right format, at the right time and place to meet commanders' policies. It involves compiling, cataloguing, caching, distributing, retrieving and displaying data for purposes of situational awareness, information access, delivery management and dissemination support.

NETOPS is an integrated approach to S&NM, IA/CND and IDM. It is the enabling operational and technical capability for net-centric warfare, given that it is about getting "the right information to the right place at the right time", which is certainly a goal of situational awareness.

Stanford Research Institute and Virginia Polytechnic Institute have programs to study policy-defined cognitive radios, each node of which is a "cognitive radio agent" which can supply information required for wireless SA.

The 2006 Software Defined Radio Technical Conference and Product Exposition, which has potential impact on wireless SA capabilities, will take place November 13-17, 2006 in Orlando, Florida.

3. CND SA Information Requirements

3.1 Top Down Requirements

In a top down approach to SA, the operational capability requirements of a mission drive the need for, and capability of, the computer network (CN). This paper does not independently develop the top-down requirements for computer networks in general and for wireless networks in particular. Rather, it adopts the approach for determining top-down requirements developed in [1]. The infrastructure has no (or very little) bearing on the types of broad questions a Commander may ask concerning the CN mission, resources, normal state, and failure states. More specific questions may deal with the specific resources (such as link availability over time) and specific failure states (such as the status of an ongoing denial of service attack); these questions certainly require some knowledge of the infrastructure and depend significantly on whether a wired or wireless network forms part of the CN.

In order for those SA questions to be answered, regardless of whether they are broad or specific questions, requires a detailed assessment of the type of infrastructure (i.e., whether wired or wireless) and a detailed look at its nodes, links, service applications, traffic, management structure, perimeter defences, etc. This paper examines some of the bottom-up factors which influence the top-down questions and which differentiate the wired and wireless network worlds.

3.2 CND SA Model

This paper follows the approach, terminology and some of the information processing flows required to orient the Commander in the Observe-Orient-Decide-Act (OODA) cycle [1]. It examines the SA model and decomposes wireless networks based on the terminology of the SA model:

- IT infrastructure (ITI) , including the nodal and link characteristics and the network logical and physical topology,

- Vulnerabilities, or the negative CND characteristics, which threat agents can exploit and use to compromise assets,

- Safeguards, or the positive CND characteristics, which reduce the severity of a vulnerability (or vulnerabilities) and therefore reduce the likelihood of the vulnerability (ies) being successfully exploited, and

- Exploits, which are described in terms of vulnerabilities which may permit certain types of exploits, and in terms of monitoring and intrusion detection safeguards, which help to determine when an exploit is taking place and the specific attack vector used.

The paper concentrates on the “observe” and “orient” parts of the OODA cycle. Sensor observation of the network is critical to provide information to be analyzed and used in the orientation phase. It therefore examines sensor data (termed “SA data” in this paper), including its potential sources and potential applications in providing situational awareness.

3.3 Application to Wired Networks

There are certain CN characteristics of wired networks which are understood, but not usually explicitly stately. They nevertheless profoundly influence the types of sensor data and analysis which ultimately can be used to provide SA. Among these characteristics are:

- Topology is relatively fixed in time, although the physical and logical location of threat agents within the network may change with time.

- Links and link characteristics are relatively static in time, although link occupancy changes.

- Routers (nodes) have relatively static routing tables, with little processing required (since fixed topologies and links comprise the network).

3.4 Extension to Wireless Networks

Wireless networks similarly have understood CN characteristics, but which vary significantly from those of wired networks. This difference impacts the types of sensor data available (and required) and the type of analysis which can be used to provide SA. The main differences (a priori, without looking more extensively at wireless network characteristics as examined in section 4 of this report) are:

- Dynamically changing topology, with nodes entering and leaving the network, and threat agents having ready access to the “open” air interface.

- Links (to nodes which change) and link characteristics (caused by nodal movement and environmental factors) can rapidly change.

- Routers must keep track of the changing topology and adapt routing tables according. The adaptation must include mechanisms for routing around compromised nodes.

All of the above factors present challenges for collecting and analyzing sensor data to help achieve SA. Nevertheless, they are challenges which are being addressed in standards bodies’ working groups and in university, industrial, and military laboratories. This report attempts to describe the current state of that research and the overall implications of wireless technology in providing SA.

4. Types of Wireless Networks Considered

Parts of the electromagnetic spectrum has been allocated for communications by world standardization bodies (e.g., the International Telecommunication Union or ITU) and by national authorities (e.g., Industry Canada).

Within those allocations, numerous public and private, military and civilian communications systems were developed. Some have undergone approval at standards bodies, such as the IEEE 802.11 series, while others are commercial, industrial, or military systems which may have proprietary or open interfaces.

Among the many systems currently in use within North America, 18 have been selected for this study. They represent both RF and infrared portions of the spectrum, and include both terrestrial and satellite systems. Table 1 lists the systems considered in this report, along with some important characteristics, such as frequency, range, modulation, and security. Some of the systems were described more fully in [11]

As wireless network issues which relate to situational awareness are described in sections 5, 6, and 7 of this report, the issues (or characteristics) and mapped back to the technologies found in Table 1.

Table 1 Wireless Technologies and Selected Characteristics

Standard, System, or Technology	Frequency Spectrum	Max. Rate and Range	Modulation / Signal Spreading	Medium Access	Security	Principal Use	Network Topologies
IEEE 802.11	2.4 GHz	2 Mb/s Range not specified.	FSK/FHSS or QPSK/DSSS	CSMA/CA	Open system / Shared key authentication, WEP, WPA, WPA2	Any	Ad Hoc, Star, Ring, Mesh[1]
Notes	This specification has been extended into 802.11b. WPA2, the security specification for wireless LANs, is standardized in IEEE 802.11i.						
IEEE 802.11a (Wi-Fi)	5 GHz	54Mb/s 30 m range	BPSK, 4QAM, 16QAM, 64QAM/OFDM	CSMA/CA	Open system / Shared key authentication, WEP, WPA, WPA2	Any	Ad Hoc, Star, Ring, Mesh
Notes	Products that adhere to this standard are considered "Wi-Fi Certified." Eight available channels. Less potential for RF interference than 802.11b and 802.11g. Better than 802.11b at supporting multimedia voice, video and large-image applications in densely populated user environments. Relatively shorter range than 802.11b. Not interoperable with 802.11b.						

[1] In this context, mesh refers to a fixed topology wireless mesh networks. Ad hoc networks are also mesh networks, but the topology is constantly changing.

Table 1 Wireless Technologies and Selected Characteristics (2)

Standard, System, or Technology	**Frequency Spectrum**	**Max. Rate and Range**	**Modulation / Signal Spreading**	**Medium Access**	**Security**	**Principal Use**	**Network Topologies**
IEEE 802.11b (Wi-Fi)	2.4GHz	11Mb/s 100 m range	DQPSK/DSSS with CCK	CSMA/CA	Open system / Shared key authentication, WEP, WPA, WPA2	Any	Ad Hoc, Star, Ring, Mesh
Notes	Products that adhere to this standard are considered "Wi-Fi Certified." Not interoperable with 802.11a. Requires fewer access points than 802.11a for coverage of large areas. Offers high-speed access to data at up to 100 metres from base station. 14 channels available in the 2.4GHz band with only three non-overlapping channels. With high-gain external antennas, the protocol can also be used in fixed point-to-point arrangements, typically at ranges up to 8 kilometres although some report success at ranges up to 80–120 km.						
IEEE 802.11g (Wi-Fi)	2.4GHz	54Mb/s 100 m range	64QAM/OFDM above 20Mb/s, DQPSK/DSSS with CCK below 20Mb/s	CSMA/CA	Open system / Shared key authentication, WEP, WPA, WPA2	Any	Ad Hoc, Star, Ring, Mesh
Notes	Products that adhere to this standard are considered "Wi-Fi Certified." May replace 802.11b. Improved security enhancements over 802.11. Compatible with 802.11b. 14 channels available in the 2.4GHz band with only three non-overlapping channels.						

Table 1 Wireless Technologies and Selected Characteristics (3)

Standard, System, or Technology	Frequency Spectrum	Max. Rate and Range	Modulation / Signal Spreading	Medium Access	Security	Principal Use	Network Topologies
IEEE 802.16-2004, 802.16a (WiMAX)	2 to 66 GHz	134 Mb/s in each 20 MHz channel bandwidth Typically 40 Mb/s. (3 to 10 km cell – Maximum 50 km)	16QAM or 64QAM/OFDM with 256 subcarriers, 128QAM/single carrier	TDM – downlink, TDMA - uplink	DES3 and AES	Commercial	Ad Hoc, Star (cellular), Ring, Mesh
Notes	Formerly 802.16 and 802.16a. Commonly referred to as WiMAX or less commonly as Wireless MAN, IEEE 802.16 is a specification for fixed broadband wireless metropolitan access networks (MANs). Initial equipment in the 3.3 to 3.8 GHz and 5.7 to 5.8 GHz bands. These profiles cover both TDD and FDD systems. The WiMAX Forum has developed system profiles addressing the 5.8 GHz license-exempt band, and the 2.5 and 3.5 GHz licensed bands.						
IEEE 802.16e-2005 (Mobile WiMAX)	2 to 6 GHz	15 Mb/s in 5 MHz channel bandwidth (2 to 5 km cell)	16QAM or 64QAM/OFDM with subcarriers variable with bandwidth	TDM – downlink, TDMA – uplink	DES3 and AES	Commercial	Ad Hoc, Star (cellular), Ring, Mesh
Notes	Formerly 802.16e. Added mobility. Uses multi-input multi-output (MIMO) multi-antenna system to improve link robustness. Software defined radio flexible air interface.						

Table 1 Wireless Technologies and Selected Characteristics (4)

Standard, System, or Technology	Frequency Spectrum	Max. Rate and Range	Modulation / Signal Spreading	Medium Access	Security	Principal Use	Network Topologies
IMT-2000 IMT Multi-carrier (MC) (CDMA2000) .	400 MHz, 800 MHz, 900 MHz, 1.7 GHz, 1.8 GHz, 1.9 GHz, 2.1 GHz	3.1 Mb/s (1xEV-DO Rev A) 4.9 Mb/s (1xEV-DO Rev B) The radio frequency and power of the handset determine the cell size.	Adaptive modulation Multilevel modulation	CDMA	SHA – 1, 128 bit AES	Commercial	Star (cellular)
Notes	International Mobile Telecommunications (IMT) 2000 (ITU-R M.1457) is the global standard for third generation (3G) wireless communications. Five radio interface standards have been approved. Common interface used in North America is CDMA2000, the successor to 2G CDMA (IS-95) . CDMA2000 1x Evolution – Data Optimized (EV-DO) is a further refinement of the air interface, and has been implemented within North America.						
Broadband Fixed Wireless – Local Multipoint Communications System (LMCS)	2.4 GHz 2.5-2.7 GHz 24 GHz 28 GHz 38 GHz	10 Mb/s (<2.7 GHz) 1.5 Gb/s downlink, 200 Mb/s uplink (>24 GHz) 100 km (<2.7 GHz) 10 km (>24 GHz)	4QAM, 16QAM, 64QAM	TDMA, FDMA	DES3	Commercial, Industrial	Star, Point-to-point, Point-to-multipoint, Ring
Notes	Line of Sight. Generally uses IEEE 802.16.3 air interface. Above 24 GHz being replaced by WiMAX.						

Table 1 Wireless Technologies and Selected Characteristics (5)

Standard, System, or Technology	Frequency Spectrum	Max. Rate and Range	Modulation / Signal Spreading	Medium Access	Security	Principal Use	Network Topologies
Industrial, Scientific, Medical (ISM)	900 MHz 1.8 GHz 2.4 GHz 5.8 GHz	Range depends on power and antenna. Typically, max is: 32 km (900 MHz) 16 km (2.4 GHz)	FHSS, DSSS		None	Any	Ad Hoc, Star, Ring, Mesh
Notes	Power < 100 mw. Packet radio (2.4 GHz band) can support 56 kb/s using PSK or ASK modulation.						
Blackberry	850 MHz 900 MHz 1.8 GHz 1.9 GHz	576 kb/s Cell size 500m (cities) to 30 km (flat terrain)			3DES, S/MIME module, SSL/TLS, BES Security policies	Commercial	Star (cellular)
Notes							

Table 1 Wireless Technologies and Selected Characteristics (6)

Standard, System, or Technology	Frequency Spectrum	Max. Rate and Range	Modulation / Signal Spreading	Medium Access	Security	Principal Use	Network Topologies
Global System for Mobile Communications (GSM)	850 MHz 1.9 GHz	9.6 kb/s Cell radius depends on antenna height, antenna gain and propagation conditions. Varies from 300 m to 35 km.	Gaussian minimum shift keying (GMSK)	TDMA	SIM card, shared secret authentication, A5/1, A5/2 crypto	Commercial	Star (cellular)
Notes	2G interface. Circuit switched. EDGE increases bit rate to 384 kb/s.						
General Packet Radio Service (GPRS)	1.9 GHz	114 kb/s (56 kb/s is practical)	Gaussian minimum shift keying (GMSK)	TDMA	SIM card, shared secret authentication, seven GPRS encryption algorithms	Commercial	Star (cellular)
Notes	2.5G interface. Packet-switched extension to GSM.						

Table 1 Wireless Technologies and Selected Characteristics (7)

Standard, System, or Technology	Frequency Spectrum	Max. Rate and Range	Modulation / Signal Spreading	Medium Access	Security	Principal Use	Network Topologies
Laser / IR	700 – 1600 nm	In 802.11 standard, IR physical layer allows a 1 – 2 Mb/s 10 Mb/s, 100 Mb/s, T1 (1.5 Mb/s), T3 (45 Mb/s), OC3 (155 Mb/s) Range depends on frequency, power, detector technology. Currently, from 150 m to 6 km.				Industrial	Point-to-point
Notes	Line of sight. Affected by path intrusions (e.g., birds), sun transits, rain/fog.						

Table 1 Wireless Technologies and Selected Characteristics (8)

Standard, System, or Technology	Frequency Spectrum	Max. Rate and Range	Modulation / Signal Spreading	Medium Access	Security	Principal Use	Network Topologies
Satellite	UHF - .2 - .4 GHz	56 kb/s		DAMA	ANDVT, KG-40, KG-84, KW-46, KY-58 STU-III[2], KG-84	Military	Point-to-point, point-to-multipoint
	L – 1.5-1.7 GHz	64 kb/s		SCPC		Commercial	Pt-to-multipt
	C – 6/4 GHz Ku – 14/12 GHz Ka – 30/20 GHz	64 kb/s to 1.5 Mb/s		DAMA, SCPC	STU-III[2], KG-84C, KG-194A, KG-175 (Taclane)	Comm / Mil	Point-to-point, point-to-multipoint
	X – 8/7 GHz	256 kb/s		SCPC	KG-84C, KG-194A	Military	Point-to-point, point-to-multipoint
Notes							
Link 11	2-30 MHz 224-400 MHz	1.4 kb/s 2.3 kb/s 500 km (HF) 30 km (UHF)	DQPSK	TDMA	KG-40	Military	Star (polled) Broadcast
Notes	Range can increase to 200 km (UHF) ground to air. UHF is line of sight.						

[2] STU-III will be removed from service in Canada as of September, 2007 [12]

Table 1 Wireless Technologies and Selected Characteristics (9)

Standard, System, or Technology	Frequency Spectrum	Max. Rate and Range	Modulation / Signal Spreading	Medium Access	Security	Principal Use	Network Topologies
Link 16	1-1.2 GHz	115.2 kb/s 500 km range	FHSS	TDMA	KGV-8B	Military	Star
Notes							
Link 22	2-30 MHz 224-400 MHz	4 kb/s (2 kb/s FHSS) 12 kb/s 500 km (HF) 30 km (UHF)	FHSS	TDMA	KIV-21	Military	Star
Notes	Improvement over Link 11, in speed and robustness. Range can increase to 200 km (UHF) ground to air. UHF is line of sight.						
TCCCS/Iris	1.6-150 MHz (30-88 MHz using AN/PRC-521 radio)	16 kb/s Range depends on antenna – 500m to 3 km	FSK/FHSS		Iris key management system, Cryptographic material management system, KYK-13	Military	Ad hoc, Star
Notes	Iris resources are used to distribute, store, and display situational awareness data. Uses GPS and SA software.						

5. Vulnerabilities Unique to Wireless Networks

5.1 The Role of Vulnerabilities in SA

According to [1], vulnerabilities describe the negative computer network defence (CND) characteristics of an IT infrastructure. They are critical components of threat vectors, since threat agents can attack an asset only through exploiting vulnerabilities. Threat vectors, in turn, play a key role in understanding defensive posture, or the protection against the set of threat vectors capable of exploiting vulnerabilities in IT resources supporting mission critical services. For such an exploit to occur, there must be insufficient safeguards protecting the asset or service (see section 6).

A knowledge of defensive posture, then, is required to understand both "risk" and the nature of real security incidents affecting IT services. An understanding of the IT infrastructure and the nature of security incidents are necessary to "Observe" the CN mission, in terms defined in the SA model described in [1]. An understanding of the risk of impacting IT services is necessary to "Orient" oneself to the current mission situation.

Awareness of vulnerabilities is therefore necessary, in the SA model, to provide information required to Observe and Orient, as part of the Observe-Orient-Decide-Act Situational Awareness cycle.

5.2 Description of Vulnerabilities

Wireless networks are subject to a wide variety of vulnerabilities unique to the fact that at least part of the end-to-end connection is carried over an "air interface". Of course, any wired links forming the end-end-connection would be subject to their own unique vulnerabilities, beyond the scope of this paper.

In the analysis below, some of the vulnerabilities are termed "impairments". Impairments refer to those vulnerabilities only affecting integrity and/or availability of assets, while the more general term "vulnerability" refers to any security weakness which could affect the confidentiality, integrity, and/or availability (C, I, A) of assets.

5.2.1 Routing protocol vulnerabilities

Routing protocols, in the context of this paper, carry information to identify the network paths (internodal links) between a source node and destination node. This broad definition holds for any circuit or packet-switched network, whether wired or wireless.

This paper concentrates on several routing protocols used in wireless ad hoc networks, namely Open Shortest Path First (OSPF), Ad Hoc On Demand Distance Vector (AODV), and Optimized Link State Routing (OLSR).

OSPF

In an ad hoc wireless network of a potentially large number of nodes, routing can be quite complex. Within a wireless subnet, an interior gateway protocol (IGP) is used for routing.

One type of IGP is the distance vector routing protocol, such as the Routing Information Protocol (RIP). In this routing technique, each wireless router does not possess complete network topology information. Rather, it transmits its distance from other neighbours, and receives similar information from other routers. As the cycle of information progresses, a more detailed network picture emerges and each router updates its routing tables, which slowly converge to stable values.

OSPF [13] is a more complex example of an IGP link state protocol, in which each node possesses a complete network topological picture. Each node independently calculates the best (shortest) next hop to every network destination based on such parameters as route cost, load balancing, number of hops, transmission speed, and route diversity. Its internodal management communication is very limited, consisting of "Hello" messages to determine whether nodes are alive and reachable.

OSPF has many inherent vulnerabilities [14], perhaps the most obvious being that routing data is carried in the clear, resulting in a risk to routing data confidentiality. Messages can also be modified, inserted, or deleted, although this vulnerability can be largely mitigated through the use of cryptographic authentication. It is also susceptible to man-in-the-middle and denial of service attacks.

From a wireless perspective, OSPF assumes a static full mesh connectivity between all routers on the subnet, but in mobile wireless networks, connectivity may be partial and constantly changing. An Internet-Draft [15] recently was submitted to the Internet Engineering Task Force (IETF) to address this problem, based on the concept of using multipoint relays (MPRs) in the wireless network. An MPR is a node which is selected by its one-hop neighbour to retransmit all messages it receives from that node. The OSPF MPR Extension for Ad Hoc Networks [15] modifies OSPF as follows :

A router with a wireless interface sends and receives Wireless Hello packets to detect neighbours. A Wireless Hello packet is similar in format to a normal Hello packet, the difference being that it lists the sender's MPR selection, it distinguishes between 1-way and 2-way neighbours, and it does not include fields for designated router or backup designated router. The router dynamically detects its neighbouring routers by sending its Wireless Hello packets to the multicast address AllSPFRouters.

OSPF adjacent neighbours are not formed on wireless networks. Instead, nodes keep a table of neighbours who have selected them as an MPR (MPR selectors). The distribution of topology information is performed by MPRs flooding link state information periodically on all wireless interfaces.

The OSPF management traffic for wireless network routing is obviously much greater than for wired fixed networks, resulting in more opportunity for threat agents to compromise the C, I, and A of routing information. It also impacts the wireless channel utilization, potentially impacting the channel allotment available for information transfer. Finally, the vulnerabilities of OSPF as described in [14] still exist with the implementation of wireless extensions.

AODV

The ad hoc on demand distance vector (AODV) protocol [16] is primarily used for routing unicast or multicast data across wireless networks. It is reactive in the sense that it establishes a destination route only when required (on demand). OSPF, in contrast, calculates the best next hop to each destination, whether or not that route is ever used.

A node needing a connection broadcasts such a request. Each node receiving the request forwards the message to neighbours and records the node from which the request was heard (this may or may not be the node originally requesting the connection). When a node receiving the request already has a route to the originally requesting node, that node notifies the requesting node. The requesting node usually accumulates several possible routes, and begins using the route with the least number of hops.

If a link fails, a routing error is sent to the transmitting node along a different route, and the process repeats.

The AODV algorithm attempts to minimize the amount of management traffic along wireless links. The protocol includes several features to ensure superfluous traffic is kept off the wireless bandwidth. For example, every route request has a sequence number, and nodes keep track of those so they don't repeat requests which have already been passed along. Each route request also has a finite lifetime, limiting the number of times requests can be retransmitted. And if a route request fails, there's also a limit on when a new request can be sent.

The advantage of AODV is that it doesn't require much management bandwidth (when no route is needed), memory, or processing power. However, the request can be slow to propagate over a complex network. And management traffic goes up dramatically when a route request is made.

Vulnerabilities exist in the assumed trust relationship between nodes. There is no agreed method by which to authenticate reliable nodes, or conversely, to identify rogue nodes. In a mobile ad hoc network, the changing topology (neighbouring nodes are constantly changing, and some may not be friendly), lack of a standard security infrastructure, and open wireless media make AODV (and other ad hoc routing protocols) vulnerable to compromise by a threat agent. The problem is the identification of a spoofed node within the wireless subnet, which makes the network subject to a variety of attacks, including rushing attacks[3] [17].

There is also a vulnerability affecting the availability of AODV-routed connections. Due to the protocol's safeguards to save bandwidth if a route request fails, each rebroadcast of the route request must wait twice as long as the previous request's timeout. In an wireless ad hoc network where transmission impairments can negatively impact node responses received, the delay in setting up a route can be appreciable and the associated management traffic can affect available bandwidth for data.

OLSR

OLSR [18] is a link state protocol (as in OSPF), but is "optimized" through the use of the multipoint relay (MPR) concept as in the OSPF wireless extensions. A node needing a connection sends Hello messages to locate its one and two-hop neighbours. The sending node then selects its MPR based on the one-hop node which offers the best routes to all two-hop nodes. In this way, the sending node develops a localized optimal routing table for every destination node.

Using MPRs reduces the possibility of flooding the network with control messages, since only MPRs forward the messages.

Although connections can be made quickly with this protocol, in an ad hoc network, the changing topology requires continuous neighbour discovery messages (the default is every two seconds) to determine MPRs for each destination node. For complex networks, this requires considerable processing power and bandwidth utilization. Because of this, some computers could become overloaded and cause delays and availability problems. And the additional management bandwidth required could negatively impact data channel allocations. The advantage is that no delays are incurred when a new route is required (as would be incurred using AODV, for instance).

Each MPR in the network shares topological information with other nodes through topology control (TC) messages (the default is every five seconds).

[3] In a rushing attack, an attacker that can forward 'route requests' to a neighbour of the target node more quickly than legitimate nodes can do so, and can therefore increase the probability that routes that include the attacker will be discovered rather than other valid routes. This is similar to the 'wormhole attack' described in section 5.2.2.

This information enables each node to compute the shortest route to all known destinations using Dijkstra's shortest path algorithm. A new routing table is computed when there is a change in topology.

The protocol suffers from other vulnerabilities, besides processing power and bandwidth. OLSR (and other ad hoc routing protocols) assume that the network is homogeneous; that is, that nodes are not differentiated by processing power or link interface characteristics. Links may have different data rates, channel capacities, range, etc. It does not choose routes based on any other considerations than the number of hops at a particular point in time. Therefore, less than optimal routes, in terms of quality of service or link availability, may be chosen. This may also cause scalability problems, since the protocol can't differentiate between nodal capacities. As the traffic increases or the number of nodes increase, network performance may degrade, since nodes at or near their capacity may be chosen along the route.

OLSR, OSPF and other link state protocols are considered stable, since routes are generally available when needed. However, if a node is moving quickly, or if wireless propagation is fading in and out due to mountainous terrain or other considerations, the links with its neighbours are only valid for a short period of time. If packets are sent on an invalid link, one not yet detected as broken, they are lost. Broken links between nodes whose state is changing must be detected quickly to minimize packet loss.

5.2.2 Wormhole Attack Vulnerabilities

Wireless ad hoc networks are susceptible to wormhole attacks, no matter which routing protocol is used. In a typical wormhole attack (see [19] and [20]), a threat agent receives packets over a wireless link and forwards (or "tunnels") the packets to a cooperating node, and replays them (or alters them) into the network from that point. The threat agent may use a high gain antenna to forward the packets to a distant cooperating node, such that those packets arrive before packets received via the "normal" multi-hop route. To minimize delays and to ensure the rogue connection is set up first, the threat agent could even forward each bit as it arrives, without waiting for the entire packet.

Once the threat agent "controls" the connection by being the first distant node to receive a connection request, the connection can be exploited even if data is protected cryptographically. In AODV, for instance, the threat agent may require all packets to be routed through the rogue node (since other routes will be discarded). In this instance, the threat agent could discard packets rather than forwarding them, creating a denial of service attack.

In OLSR and OSPF, the threat agent's node could respond to Hello packets with other Hello packets, setting up a neighbour relationship as part of the routing table. If the threat agent's node then ceases to be a cooperating neighbour, the routing table is no longer valid.

5.2.3 Geospatial link impairments

Wireless networks are subject to a variety of geospatial link impairments which affect the range of transmissions and the quality (bit error ratios and retransmissions) of the connections. Some of the impairments are predictable; the free space loss L of a radio signal, for instance, is given by :

$$L = \left(\frac{4\pi d}{\lambda} \right)^2 = \left(\frac{4\pi df}{c} \right)^2$$

where d is the distance between transmitter and receiver, λ is the RF wavelength, f is the radio frequency, and c is the speed of light. The formula is valid for d >> λ , and does not take into account antenna gains or obstructing elements causing additional loss.

The principal contributors to geospatial link impairments, which could affect availability and integrity of connections are as follows. There are numerous models which predict losses under the following conditions, and these models could be used as inputs to the SA CND model to help determine risks to availability and integrity. Of course, link sensors which determine real time performance, including error ratios, should provide the additional information required by commanders to determine wireless network situational awareness.

- shadowing – This is the attenuation of a wireless signal caused by large objects (e.g., buildings or walls) blocking the line of sight between transmitter and receiver. The size of the obstruction is generally greater than several wavelengths of the electromagnetic wave. This may be modelled as a lognormal term with spatial correlation.

- multipath fading – This is the attenuation of a wireless signal caused by the constructive/destructive superposition of radio waves reflecting from objects. These could be relatively small objects, on the order of a wavelength in size, and may be modelled using random distributions such as Rayleigh channels. In an ideal static environment (no moving objects or nodes), the fading should be time invariant.

- Doppler effects – This refers to the frequency change caused by nodal movement along a component parallel to the transmission path, which could affect the received power within a narrow bandwidth of a selective receiver. It also can affect timing and synchronization relationships between nodes.

- terrain effects – These include a combination of shadowing and multipath fading caused by transmitter and/or receiver locations within a spatially complex terrain. This is particularly applicable to military environments, but is more difficult to model theoretically. Numerous models have, nevertheless, been developed, such as the irregular terrain model (ITM) by the Institute for Telecommunications Sciences [21].

- rain/fog fade – Certain parts of the spectrum used in wireless networks are particularly susceptible to absorption by some air molecules, particularly water vapour, and to scattering by dust particles (Mie and Rayleigh scattering).

- sun transits – When the line or sight between transmitter and receiver nears the line of sight to the sun, the signal to noise ratio generally goes down, resulting in increased bit error ratios and even temporary loss of connection. This vulnerability particular applies to satellite wireless networks.

- sunlight terminator effects – The proximity of the transmitter and/or the receiver to the sunlight terminator affects the propagation characteristics of certain RF wavelengths.

- seasonal effects – Seasonal conditions (temperature, humidity levels, length of day) result in propagation and link attenuation affects.

- solar cycle / flares – The sun exhibits a 11-year cycle between sunspot maxima, resulting in a periodic change in the state of the ionosphere (caused by particle and x-ray emission). Since the ionosphere reflects certain high frequency radio waves, long range propagation can be affected. In addition, very large sunspots and solar flares can eject high energy changed particles (mainly electrons and alpha particles) which can disrupt local radio communication on earth.

- link anisotropies – Real wireless transmissions are not isotropic. Anisotropies[4] can result from many of the effects listed above, and the effect of directional antenna gains with pronounced lobes.

5.2.4 Temporal link impairments

Many of the geospatial link impairments listed above have a time-variable component, some of which are predictable and some appear more random. In addition, mobile nodes moving relative to each other and to the environment

[4] The property of being directionally dependent. Typically, RF links are anisotropic, having different characteristics in different directions, caused by antenna gain beamwidth patterns or other effects.

place a temporal component in link attenuation characteristics, which may require real-time GPS coordinates to help model.

5.2.5 Link asymmetries

In general, most of the link attenuation affects such as the inverse square path loss due to range, shadowing, and multipath fading are symmetric effects. Nevertheless, link asymmetries are common with wireless networks. The most common cause, which could translate to one-way availability problems, is a difference in the hardware calibrations.

5.2.6 Multihop routing impairments

In each hop of an end-to-end connection, not all packets normally get through due to various impairments. If the probability of a packet getting through is P, then the probability of a packet getting through an end-to-end connection of N hops is P raised to the N power. The throughput can therefore go down dramatically on multihop connections (or, conversely, the number of retransmissions can go up). This can affect overall delay and availability.

5.2.7 Jamming / interference

A threat agent's transmitter, tuned to the same frequency as a target receiving equipment and generally with the same type of modulation scheme, can override RF signals associated with a legitimate wireless connection at the receiver. Most receivers are vulnerable to this attack, although some techniques, such as frequency hopping, make the receiver more immune. The most common types of this form of signal jamming are random noise, random pulse, stepped tones, warbler, random keyed modulated continuous wave, tone, rotary, pulse, spark, various sounds, and frequency sweep-through. Unfortunately, the 802.11 medium access control (MAC) layer[5] avoids transmitting when it senses other RF activity, including RF jamming signals, so even if the signal had a chance of being received through the noise, it would never be transmitted. This gives the threat agent enough control to keep users from accessing network services, creating a denial of service attack. From an SA model perspective, this vulnerability can affect asset availability.

5.2.8 Denial of Service attacks

Wireless networks are particularly vulnerable to denial of service attacks. This may be due to a threat agent's control of a node through a wormhole

[5] Actually, this is the result of the distributed coordination function, or DCF protocol. The point coordination function (PCF) protocol avoids this problem, but it is not widely implemented.

attack (see section 5.2.2), for instance, or through interference of the RF link itself (see section 5.2.7).

5.2.9 Rogue access points

Rogue access points can be installed on a wireless LAN network, and the installation can have minimal or no security features enabled. Communications to the access point may be unencrypted, passwords may be observed, and the access point may be positioned in a non-secure area such that unauthorized people may have wireless access to it. Once a non-authorized wireless access point is installed with unknown security policies, the wireless network (and interfacing wired network) is subject to a variety of attacks against assets' confidentiality, integrity, and/or availability. For instance, a rogue access point can spoof its MAC address to the identity of an authorized access point. Users can unknowingly associate to the rogue access point, creating attack vectors such as man-in-the-middle or denial of service.

5.2.10 Access point reassociation vulnerabilities

A threat agent could send an 802.11 deauthenticate frame to a client using the basic service set identifier (BSSID) of the client's access point. The result is another denial of service attack.

A legitimate user could inadvertently reassociate to a rogue access point, potentially placing assets at a risk of C, I, and/or A compromise.

5.2.11 Subnet roaming vulnerabilities

Similar to reassociation vulnerabilities, a roaming wireless user could roam to a hostile subnet if authentication credentials were spoofed.

5.2.12 User authentication vulnerabilities

Wireless handheld devices are mobile by their nature and can be lost or stolen, falling into the hands of a threat agent. Therefore, the user of an authenticated device may not be an authorized user of the wireless network. A wide variety of C, I, and A attacks may be launched by a legitimate device operated by a threat agent.

5.2.13 Device authentication vulnerabilities

The device Media Access Control (MAC) address (used in most wireless devices) and service set identifiers (SSIDs, used in 802.11 devices) can easily be determined and spoofed.

Node authentication is especially relevant in mobile ad hoc networks (MANETs), where nodes may constantly enter or leave a network. It can be difficult to quickly identify the presence of a rogue node before damage is done to assets. Various schemes have been proposed to deal with MANET authentication, some of which are described in section 6.2.1, 6.2.2, 6.2.3, and 6.2.15.

A user's privacy also could be comprised by a threat agent identifying a transmitting node through the measurement and analysis of a wireless network interface card's distinctive electromagnetic signature [22].

Device authentication using RADIUS Response Authenticator and Message-Authenticator attributes are vulnerable to a dictionary attack[6]

5.2.14 Channel resource allocation vulnerabilities

Wireless channel bandwidth is normally at a premium. If channels are allocated incorrectly, wireless resources may be wasted. Queued transmissions may need to wait for an available channel, resulting in connection availability problems.

5.2.15 Physical handheld access vulnerabilities

Wireless handheld units are vulnerable to access by threat agents due to their portability. This could result in a threat agent obtaining access to a protected wireless network (see section 5.2.12) or access to sensitive resources stored on media resident on the handheld device itself.

[6] The RADIUS Extensions Working Group of the IETF focuses on extensions to the RADIUS protocol required to enable its use in wireless network authentication, authorization and accounting.

5.3 Mapping of Vulnerabilities to Wireless Technologies

Table 2 maps the above potential vulnerabilities to the wireless technologies listed in Table 1.

Table 2 Wireless Vulnerabilities Mapped to Technologies

Potential Vulnerability	Applicable Wireless Technology
Routing protocol vulnerabilities	All routed ad hoc wireless topologies
Wormhole vulnerabilities	All routed ad hoc wireless topologies
Geospatial link impairments	All (severity depends on RF frequency, power, antenna)
Temporal link impairments	All
Link asymmetries	All
Multihop routing impairments	All routed technologies
Jamming / interference	All (CDMA more robust)
Denial of Service attacks	All
Rogue access points	802.11 (WiFi)
Access point reassociation vulnerabilities	802.11 (WiFi)
Subnet roaming vulnerabilities	802.11, cellular
User authentication vulnerabilities	All
Device authentication vulnerabilities	All
Channel resource allocation vulnerabilities	All
Physical handheld access vulnerabilities	All

6. Safeguards Unique to Wireless Networks

6.1 The Role of Safeguards in SA

Again referring to [1], safeguards describe the positive CND characteristics of the IT infrastructure. They are the explicit security measures included in the CN. Each safeguard protects against the potential exploit of one or more vulnerabilities. They therefore influence both the system description (a knowledge of which is required to establish situational awareness) and potential threat vectors. With regard to the latter, threat vectors attempt to exploit assets either by altering the vector to “work around” safeguards or by compromising vulnerabilities in spite of existing safeguards (if the safeguards were not sufficient to prevent an exploit). Either way, the establishment of safeguards impact the SA model’s risk assessment, which ultimately influences the determination of defensive posture, a key component of SA.

6.2 Description of Safeguards

Safeguards for wireless networks are directly related to the wireless networks’ vulnerabilities. They reduce the severity of vulnerabilities, making exploit by threat agents more difficult (in general, less probable). Without vulnerabilities, there would be no need for safeguards.

Each of the safeguards described below is therefore related to one or more vulnerabilities described in section 5.

6.2.1 Routing Protocol – OSPF

As described in section 5.2.1, OSPF has many inherent vulnerabilities [14], most of which have not been addressed by effective safeguards. However, the protocol has an option for 64-bit cryptographic authentication, and data payload can be protected with a message authentication code.

The OSPF extensions for wireless ad hoc networks [15] are relatively new, and may be considered as the set of safeguards required to implement OSPF effectively on a wireless network. No additional safeguards for wireless OSPF have been proposed, although generic safeguards applicable to all ad hoc routing protocols (see section 6.2.4, for instance) are certainly applicable to OSPF.

6.2.2 Routing Protocol – AODV

Several safeguards have been proposed to address AODV vulnerabilities. In particular, [17] proposes an instantly verifiable broadcast authentication protocol using digital signatures. They also propose overlaying AODV with a secure neighbour detection protocol.

Patwardhan et al [23] proposed a "secure AODV, or simply SecAODV" which includes mechanisms for non-repudiation and authentication using statistically unique and cryptographically verifiable (SUCV) identifiers, without resorting to a certificate authority or key distribution centre. The SUCVs associate a host's IP address with its RSA public key (generated by the nodes) to provide verifiable proof of ownership of that IP address to other nodes.

Security can, of course, be also improved by implementing one or more of the following safeguards :

- prior trust relationship between pairs of nodes, and might be brokered by a trusted third party or through a distributed trust establishment,
- time synchronization between pairs of nodes, or
- prior shared keys or other form of secure association.

6.2.3 Routing Protocol – OLSR

Fast OLSR has been proposed [24] as an extension to the OLSR protocol to more rapidly respond to fast-moving nodes, to eliminate broken links (and lost messages) prior to their being discovered by the sending node. They envisage a fast moving node being able to quickly discover a small number of neighbours, so that neighbourhood changes can be rapidly detected and responded to. Among the discovered neighbours, a number of slower-moving MPRs are selected to maintain connectivity to the network. The fast moving node maintains communications with the selected MPRs through Fast Hellos, or Hello messages refreshed at a much higher frequency than traditional Hello messages. This, of course, adds to the management bandwidth (locally), but is weighed against the additional bandwidth and delay penalties realized with broken links.

Hierarchical OLSR (HOLSR) has been proposed [25] to reduce routing control message overhead and improve performance in large ad hoc networks. HOLSR dynamically organizes nodes into cluster levels, and the clusters are organized into a hierarchical architecture, taking into account the different node capacities and capabilities. Within a cluster, moving nodes need exchange fewer topological control messages. Communications between clusters take better advantage of high capacity nodes. These improvements make HOLSR a much more scalable protocol than OLSR, and simulations indicate that it dramatically reduces packet overhead. It also achieves shorter end to end delays and reduced packet loss (a safeguard against link non-availability).

Node authentication is a major issue for most ad hoc routing protocols. A fully distributed certificate authority for an OLSR ad hoc wireless network has been proposed [26] using the existing control packets to exchange security information to minimize overhead.

Finally, the IETF has recently (October, 2006) [27] published an Internet-Draft on quality of service for ad hoc routing protocols. In particular, a QOLSR protocol is proposed as an extension to OLSR, with additional fields about QoS conditions added to both the Hello and topology control messages. Such an extension should help OLSR provide integrity and availability safeguards by influencing MPR and link selection based on time-varying QoS conditions.

6.2.4 Wormhole Safeguards

There are safeguards proposed which prevents a threat agent from exploiting the wireless network wormhole vulnerability. There also have been several means proposed to quickly detect a wormhole attack in progress, which then can permit the astute network manager to implement additional safeguards to contain the attack. Understanding a wormhole attack in progress (part of wireless intrusion detection) is therefore very much a component of situational awareness.

Hu et al [19] proposed a concept called packet leashes, which restricts each packet's maximum allowed transmission distance. The restriction can be either geographical or time-based. They also propose a protocol for implementing these leashes, the temporal ones based on precise timestamps and accurate time synchronization using either GPS or LORAN-C signals. The geographic leashes require broadcast authentication.

Gorlatova et al [20] proposed a means of detecting wormhole attacks in networks with proactive protocols such as OLSR and OSPF by analyzing behavioural anomalies in protocol packets. They also propose signal processing techniques applied to the periodic neighbour discovery (Hello) and topology control messages. Simulations indicate that this technique can detect a pending wormhole attack, even with an intelligent attacker choosing which packets to drop, before significant damages can result.

6.2.5 WEP / WPA2

WEP

Wired equivalent privacy (WEP) was introduced as a safeguard to provide confidentiality of 802.11 wireless communications "equivalent to that achieved in a wired network". Due to its many vulnerabilities, it was abandoned as an effective safeguard, and is included in this analysis for completeness, and to help the reader understand the additional safeguards afforded by WPA2.

The WEP protocol provides a means of encrypting the wireless transmissions. However, even with WEP enabled, there exists ways of breaking the encryption using a combination of intelligent sniffing and brute force. This vulnerability exists due to the weakness of the WEP protocol and due to the static nature of the WEP keys.

WEP uses shared keys (40-bit) and a pseudo random number as a 24-bit initial vector (IV) to encrypt the data portion of network packets. This is based on the use of secret keys with symmetric encryption algorithms. The 802.11 wireless LAN network headers (including the IV portion and key number) themselves are not encrypted. The static WEP encryption key can then be determined by capturing a substantial amount of wireless traffic. Numerous publicly available software packages can help a user crack WEP encryption.

The cyclic redundancy check (CRC) to ensure payload integrity is also insecure; it is possible to alter the payload and change the CRC without even knowing the WEP key.

Finally, WEP does not address other areas such as user authorization and non-repudiation.

WPA2 (802.11i)

WiFi Protected Access (WPA) was developed as an improved safeguard for 802.11 wireless networks. It has undergone a few variations, and the latest (WPA2) was approved as the 802.11i standard.

Briefly, 802.11i lengthens both the shared keys (128-bits long) and the IV (48 bits long). A major enhancement is the ability to change keys during a connection using the temporal key integrity protocol (TKIP). If there is an attempt to break TKIP, communication with the attacker is halted. These safeguards make key recovery attacks much more difficult.

802.11i also replaced the WEP CRC with a message integrity code (MIC), which includes a frame counter to thwart replay attacks.

802.11i also adds the advanced encryption standard (AES) algorithm, which is a preferred algorithm by the Communications Security Establishment [28] for symmetric key cryptography.

Although the standard recommends authentication and key distribution by an 802.1X authentication server, it is possible to use the much less secure pre-shared key, in which all users are given a common passphrase. Stronger authentication is also provided by the Extensible Authentication Protocol

(EAP) dialog. Authentication, of course, is still a problem in all mobile ad hoc networks, and some ad hoc routing protocols have added a distributed certificate authority to address this problem (see section 6.2.3 as an example).

As of March 13, 2006, 802.11i certification is required for all new devices wishing to be Wi-Fi certified.

6.2.6 Blackberry-specific safeguards

The vulnerabilities of Blackberry systems were not listed separately in section 5, since there are no vulnerabilities unique to the Blackberry system; all vulnerabilities are common to many wireless handheld devices. Like all cellular systems, they are vulnerable to propagation and range limitations (affecting link availability). And like many wireless systems, they are vulnerable to link confidentiality compromises, device authentication attacks, and denial of service attacks. However, Research in Motion (RIM) has introduced a wide range of safeguards to protect Blackberry email[7], which, if invoked by users, are sufficient to warrant the approval by CSE for the transfer of Protected B information [29] [30].

The safeguard options offered by RIM are too numerous to list in the body of this report; rather, refer to Annexes A [31] and B [32]. Some of the principal safeguards offered are end-to-end (handheld to computer or LAN) triple DES or AES encryption. They also offer an S/MIME encryption option (required by CSE for protected B data) and IT security policy settings (see Annex A).

6.2.7 Military authentication/encryption

Various types of communications security (COMSEC) modules are used for military wireless networks and satellite communications, as indicated in Table 1. The units are designed to interface to certain types of wireless links (e.g., IP, ATM, satellite, etc.) and provide such services as link encryption, key management, and mechanisms to recovery from compromise. They provide confidentiality and integrity safeguards for both classified and unclassified (but protected) data, usually depending on the key chosen.

6.2.8 Commercial link encryption

Commercial link encryption is not unique to wireless networks, but is a more important confidentiality safeguard for wireless networks to implement, since the air waves are more open to intruders than are wired networks (which can be physically secured).

Triple DES and AES are the strongest encryption protocols generally used on commercial wireless networks. Of these, AES has been recommended by

[7] Except short message service, where messages are scrambled but not encrypted.

CSE [28] for the transmission of sensitive data, up to Protected B. The modes of AES operation are specified in NIST Special Publication 800-38A [33]. According to CSE [28], the crypto period of any one key shall not exceed seven days.

6.2.9 Adaptive modulation

Adaptive modulation and coding systems, such as implemented in the CDMA2000 cellular network and some satellite systems, alter the transmission characteristics (i.e., transmitter power, bit rate, etc.) depending on conditions of the link. This improves the throughput and/or bit error ratios by exploiting the channel information that is present at the transmitter. The technique is especially effective over fading channels suffering certain propagation impairments. In that scenario, adaptive modulation exhibits considerable performance enhancements compared to systems that do not exploit knowledge of the channel at the transmitter.

6.2.10 Multiuser diversity

A major feature of mobile wireless networks is the random fading of the communication link channel strengths. In a large system with users fading independently, there is likely to be a user with a very good channel at any particular time. Multiuser diversity exploits this concept by scheduling transmissions so that users transmit when their channel conditions are most favourable. This safeguard, implemented in some CDMA2000 networks, can be used to greatly increase the throughput of mobile ad-hoc networks with delay tolerant applications. It therefore can improve link availability and/or integrity.

6.2.11 Frequency hopping

Frequency hopping, or frequency hopping spread spectrum (FHSS) is a method of transmitting radio signals by switching a carrier among many frequency channels, using a sequence known only to the transmitter and receiver.

This technique offers certain advantages over a fixed-frequency transmission:

- Spread spectrum signals are more resistant to noise and interference. The process of assembling a spread signal spreads out noise and interference, increasing the signal to noise ratio.

- Spread spectrum signals are more difficult to monitor by a threat agent. An FHSS signal sounds like a momentary noise burst or simply an increase in the background noise for short frequency hop codes on any narrowband receiver except an FHSS receiver using the exact same channel sequence as was used by the transmitter. This safeguard is not as effective with the 802.11 standard, however, since that standard describes the spreading codes publicly so that third parties can design interoperable 802.11 components. As a result, a threat agent needs only an 802.11-compliant interface card as the basis for connectivity, which negates some of the security benefits of spread spectrum.

- Spread spectrum transmissions can share a frequency band with many types of conventional transmissions with less interference. The spread spectrum signals add little noise to the narrow frequency communications, and vice versa. As a result, bandwidth can be utilized more efficiently.

In a multipoint radio systems, space allows multiple transmissions on the same frequency to be possible using multiple radios in the same geographic area. This creates the possibility of data rates that are higher than the Shannon limit for a single channel. This property is also seen in MIMO systems (see section 6.2.13). Beam steering and directional antennas also facilitate increased performance by providing isolation between remote radios.

6.2.12 High gain antennas

A high gain antenna significantly increases wireless signal strength on a link. High-gain antennas may be necessary to increase the range of wireless networks or to reduce the effect of geospatial or temporal link impairments. They therefore can be used as safeguards to increase availability and/or integrity.

Note that high gain antennas can also be used by threat agents to launch wormhole attacks (see sections 5.2.2 and 6.2.4).

6.2.13 Multiple input – multiple output (MIMO) systems

MIMO is a multi-antenna communication system which leverages multipath propagation to increase data throughput and range and/or reduce bit error ratios, rather than attempting to eliminate undesirable effects of multipath propagation (see section 5.2.3). MIMO is now part of the IEEE 802.16 standard and will also be part of the IEEE 802.11n high throughput standard, which is expected to be finalized in mid 2007. Standardization of MIMO is expected in 3G standards such as CDMA2000.

MIMO achieves higher spectral efficiency in wireless systems, especially with a large number of antennas, OFDM and higher order modulation such as 64-QAM. However, the computational complexity is exponential in the number of bits transmitted simultaneously in each symbol interval [34]. In addition, channel estimation schemes must be used to estimate (and compensate for) channel conditions.

MIMO shows great promise for providing an additional wireless safeguard against wireless network integrity and availability.

6.2.14 Wireless network discovery mechanisms

Network discovery mechanisms are not true safeguards, but they assist in providing knowledge of the network required in order to apply effective safeguards. Network discovery may locate a rogue node, for instance, but safeguards should be in place (or be put in place) to isolate the node and prevent damage. Nevertheless, merely knowledge of the rogue node is important SA data.

Network discovery involves each node obtaining information about its neighbours through some sort of protocol. Three such routing protocols were described in sections 6.2.1, 6.2.2, and 6.2.3. There was recently a new IETF Internet-Draft [35] submitted (June, 2006) which describes a MANET neighbourhood discovery protocol which can efficiently discover neighbours and may be incorporated into any of the above routing protocols.

There have been other efficient and lightweight network and service discovery mechanisms developed for mobile wireless networks, some of which are described in [9], [10], and [36]. All provide topology information such as provided in proactive routing protocols (e.g., OLSR and OSPF), but claim greater efficiencies, adaptabilities, and/or scalabilities.

6.2.15 Wireless network intrusion detection tools

Intrusion detection tools are not safeguards in the strictest sense, since they do not reduce the effects of a vulnerability. Rather, they detect attempts at compromise or actual compromise of a vulnerability. They are therefore useful tools to facilitate the application of additional safeguards to contain the attack and/or to prevent future compromises.

Wireless networks in general, and MANETs in particular, present a number of unique problems for intrusion detection systems (IDS). A principal function of an IDS is to differentiate between malicious network activity and spurious, but typical, network behaviour. In an ad hoc wireless network, malicious nodes may enter and leave the transmission range at random intervals, or may collude with other nodes to disrupt the network and avoid detection. Malicious nodes may behave maliciously only occasionally, further complicating their detection. A node that sends out false (or incorrect) routing information could be one that has been compromised or one that has an outdated routing table due to volatile network conditions.

Dynamically changing topologies in a MANET make it more difficult to obtain a global view of the network, and any view becomes quickly outdated.

Intrusion monitoring in a wired network is usually performed at switches, routers, gateways, or sensors on fixed links, but a MANET does not have these elements where an IDS can collect information relevant to the entire subnet. MANET sensors on nodes or links can only monitor and report traffic and anomalies within the observable radio transmission range.

A number of neighbour-monitoring, trust-building, and cluster-based voting schemes have been proposed (see [37], [38], [39], [40], [41], and [42]) to monitor, detect, report, and diagnose malicious activity in MANETs. A comparative study of various routing protocols and their application in signature-based IDS in given in [43]. This is the subject of considerable current research.

6.2.16 MANET Key Management Protocols

Several protocol-specific key management schemes have been proposed (see sections 6.2.2 or 6.2.3, for instance), but there have also been generic "efficient and robust" key management schemes developed for large MANETs [44]. That scheme provides various parts of the MANET the flexibility to select appropriate security configurations according to risks faced, the adaptability to cope with rapidly changing environments, the ability to issue certificates with different levels of assurance, and the tested ability to function well even in hostile wireless environments.

6.2.17 Power Control

Adaptive power control attempts to mitigate the effects of fading on the transmission link and maintain the highest possible data throughput. Some techniques employed, especially on satellite systems, include uplink power control (ULPC), end-to-end power control (EEPC), downlink power control (DLPC) and on-board beam shaping (OBBS).

6.2.18 Software Defined Cognitive Radios

Software defined radios can adapt to link conditions and improve throughput by negotiations between the transmitter and receiver. By querying such quantities as delays, errors, buffer state, channel occupancy, etc., the link can adapt to new policies, change modulation (e.g. QAM-16 or 64), increase power, or change other characteristics. Cognitive radios can learn the effects of the changes to optimize negotiated changes to maximize throughput or to achieve other goals. These safeguards make the link more robust against a wide variety of impairments and therefore improve availability.

6.3 Mapping of Safeguards to Wireless Technologies

Table 3 maps the above possible safeguards to the wireless technologies listed in Table 1.

Table 3 Wireless Safeguards Mapped to Technologies

Possible Safeguards	**Applicable Wireless Technology**
Routing Protocol - OLSR	All routed ad hoc wireless topologies
Routing Protocol – OSPF	All routed ad hoc wireless topologies
Routing Protocol - AODV	All routed ad hoc wireless topologies
Wormhole safeguards	All routed ad hoc wireless topologies
WEP / WPA2	802.11 (WiFi)
Blackberry-specific safeguards	Blackberry
Military authentication/encryption	Military wireless networks
Commercial link encryption	CDMA2000, LMCS, Blackberry, GSM, GPRS
Adaptive modulation	CDMA2000
Multiuser diversity	CDMA2000
Frequency hopping	FHSS, CDMA
High gain antennas	All
Multiple input – multiple output (MIMO) systems	All
Wireless network discovery mechanisms	All
Wireless network intrusion detection tools	All
MANET key management protocols	All ad hoc wireless topologies
Power control	CDMA2000, Satellite systems, Link 11, Link 16, Link 22
Software defined cognitive radios	All

7. Situational Awareness Data Unique to Wireless Networks

7.1 Description of SA Data

In a top down approach, it is necessary to examine the SA model [1] and determine the information required to satisfy the SA needs of the commander. From that model, it is clear that SA requires knowledge of defensive posture, the risk of security incidents (potential), and security incidents (actual) which have taken place or are taking place.

Both defensive posture and risk requires a knowledge of the state of the system, including the system's instantaneous topology, rate of change of the topology, connectivity, link and node occupancy, and the quality of service of links and end-to-end connections.

Actual or attempted incidents require real time monitoring of intrusions, which includes knowledge of anomalous state changes in the wireless network.

The following lists the potential sources of this data, along with an estimate of the frequency of data updates required to maintain a good situational awareness and the bandwidth which may be required to transfer this data.

7.2 Potential Sources of SA Data

7.2.1 Routing protocol – OSPF

In the wireless extensions to OSPF, nodes keep a table of neighbours who have selected them as an MPR. Topology information (shortest hop MPRs to each destination node) is available for SA data. This gives a complete topological picture of the network, periodically updated, which JNDMS can use.

7.2.2 Routing protocol – AODV

Each node keeps tracks of route requests, request sequence numbers, completed connections, and retransmitted requests. JNDMS can therefore collect the end-to-end connection data and information on the time-varying condition of the links (or nodal movement), based on retransmitted requests.

7.2.3 Routing protocol – OLSR

Each node computes and stores the shortest route to all known destinations using Dijkstra's shortest path algorithm, updated periodically (the default is every five seconds). As in OSPF, this gives a complete topological picture of the network (time varying) which JNDMS can use in its determination of SA.

7.2.4 Mobile agents

There is much current research on the roles and capabilities of mobile agents, especially in the real-time reconfiguration of MANET topology to improve performance and in wireless intrusion detection. See, for instance, [7], [45], [46], [47], [48], and [49]. This section only briefly describes the potential roles of mobile agents providing SA data. A brief review of agent technologies is provided in Annex C.

A mobile agent is a self-contained program that can traverse a network to provide capabilities to nodes that change with changing network conditions. It can work autonomously toward a goal, and can interact with other agents and its environment. For example, in a MANET, a mobile agent can cause any host in the network to act as a router for any other host in the network, dynamically changing the network topology. Mobile agents can also discover preferred routes in wireless networks and help to determine to the level of trust associated with neighbouring nodes.

The Mobile Agent Routing protocol [60] uses agents to propagate routing information through MANETs, by allowing each agent to record nodes it has visited. In this technique, a global registry of mobile agents is used; however, it is not always possible to apply a global data structure in an ad-hoc network. Rather, an improved agent-based ad-hoc routing protocol [61] was proposed to remove the global registry and use only local information of nodes to build the routing table.

There are many benefits of mobile agents [47], among them are reduced latency (since they can operate at remote nodes), reduced network load (since information does not need to be sent to remote nodes where an agent is operating), they can sense the environment and react to change, and there distributed nature makes them robust to a partial network failure.

Of particular relevance to SA, agents can relocate when sensing danger (and send to danger signs to JNDMS), clone for redundancy, collaborate and share knowledge, and dynamically reconfigure to compensate for failures or attacks. In a complex attack vector, agents can readily correlate network anomalies and more easily determine origins of the threat and/or the network vulnerability (ies) permitting the initial compromise. This is also vital SA data which could be sent to JNDMS.

Once an attack is detected, mobile agents can more easily respond to the attack, since they may be resident in the affected nodes and can isolate the attacker and minimize further damage.

Finally, mobile agents resident at nodes which are part of the attack vector can reconstruct the attack and gather post-mortem evidence to prevent future attacks (possibly, dynamically reconfiguring to make the network more resilient). Again, this evidence is important SA data.

7.2.5 Management protocols

There are a wide variety of management protocols capable of providing SA data. Among the main classes are:

- simple network management protocol (SNMP) – can provide link and end-to-end connectivity, performance, and fault management data
- location/mobility management protocol (including GPS) – can provide node location information
- power management protocol – can provide power and link characteristic information
- key management protocol – can provide access control information
- connection management protocol – can provide link occupancy and nodal connection information

7.2.6 Wireless IDS sensors

Various MANET sensors and tools are under research and development which will be able to monitor, detect, report, and diagnose malicious activity in MANETs, as described in section 6.2.15. The outputs of these tools can provide important information on pending incidents and the dynamic state of the network to JNDMS.

With 802.11 networks, there are numerous wireless sniffing tools (e.g., AirMagnet or NetStumber) that capture information regarding access points that are within range. These can identify the presence of rogue access points.

Other selected 802.11 IDS tools include:

AirDefense Guard: AirDefense Guard is an 802.11a/b/g wireless LAN intrusion detection and security solution that identifies security risks and attacks, provides real-time network audits and monitors the health of the wireless LAN. It detects rogue nodes and performs real-time network audits to inventory all hardware. It tracks wireless LAN activity and enforces security policies. It also monitors the health of the network to identify and respond to hardware failures, network interference, and performance degradation.

Snort-Wireless: Snort-Wireless is an attempt to make a scalable (and free) 802.11 intrusion detection system that is easily integratable into an IDS infrastructure. It is backwards compatible with Snort 2.0.x and adds several additional features. Currently it allows for 802.11 specific detection rules through the new "wifi" rule protocol, as well as rogue access point, ad hoc network, and Netstumbler detection.

WIDZ: WIDZ (Wireless Intrusion Detection System) is an IDS for 802.11. It monitors access points and the local RF neighbourhood for potentially malevolent activity. It can detect scans, association floods, and rogue access points, and it can be integrated with SNORT or Realsecure.

Neutrino: The Neutrino Wireless Sensor is equipped with its own intelligent surveillance agent, built specifically for 802.11. It looks at packets, devices, and clients to automatically detect a number of conditions that can impact wireless network security and performance. The Neutrino sensors are small hardware appliances and include two network adaptors, one wireless and one Ethernet.

7.2.7 QoS monitors

Important wireless network data includes fault management information, performance measurements, usage data records (UDRs), and IP service monitor (ISM) data; these may be available from standard management tools. Quality of service indicators available from wireless network monitors include latency, throughput, bit error ratio, and transmitted/received RF power.

MANET QoS is the subject of much current research in the IETF MANET working group, and MANET QoS monitors are generally in the research stage.

7.2.8 Software Defined Radios

Software defined radios store a considerable amount of information about real-time link conditions, which form part of the system description specified in the SA model [1]. Changes in the link conditions or quality of service can indicate a change in the risk of asset compromise or they can indicate a security incident, both of which are important components of SA data.

7.3 Message Frequency and Bandwidth

The timeframe for any of the above SA data to be sent to JNDMS is on the same order as topology control (TC) messages sent using the OLSR protocol (the default is every five seconds). However, in a fast changing topology, where nodes are moving quickly, fast OLSR requires a much greater TC message frequency. If we assume fast TC messages must be sent every second, and SNMP packets are usually between 64 and 1500 bytes long, then the management messages require a bandwidth between 500 bits/s and 12 kbits/s[8]. If, however, a five second message interval is acceptable, the required maximum bandwidth is less than 2 kbits/s.

7.4 Mapping of SA Data to Wireless Technologies

Table 4 maps the above potential sources of SA data to the wireless technologies listed in Table 1.

Table 4 Sources of SA Data Mapped to Technologies

Sources of SA Data	Type of SA Data	Applicable Wireless Technology
Routing protocol – OLSR	Connectivity, nearest neighbours	Ad hoc wireless topologies
Routing protocol – OSPF	Connectivity, nearest neighbours	Ad hoc wireless topologies
Routing protocol - AODV	Connectivity, nearest neighbours	Ad hoc wireless topologies
Mobile agents	Connectivity, network health, intrusion vector information	All
Management protocols	Traffic patterns, traffic prioritization, channel resource allocation, channel occupancy, hardware status	All
Wireless IDS sensors	Security incidents, network anomalies, rogue access points, rogue nodes	All
QoS monitors	SNR, link budget, path loss, errors	All
Software defined radios	Link characteristics, QoS	All

[8] 64 bytes x 8 bits/byte / 1 sec = 512 bits/s

8. Application to CND SA Model

8.1 Summary of Wireless Network Features Impacting SA

This report identified three major areas where the inclusion of wireless networks into the SA model could impact the model:

- vulnerabilities unique to wireless networks
- safeguards unique to wireless networks
- situational awareness data unique to wireless networks

The report went on to describe 15 specific wireless network vulnerabilities, 18 wireless network safeguards, and 8 areas where additional wireless network information can be captured and sent on to JNDMS for analysis.

Not all of the above are mutually exclusive; the type of routing protocol chosen influences all three area. The type of wireless network architecture (e.g., MANET, fixed star, full mesh, etc.) also influences most of the areas.

Many types of wireless networks were addressed, and there are consequently many variables (e.g., system type, topology, security policies, routing protocol, etc.) affecting SA. Hopefully, the report provides the background necessary to identify specific SA impacts once any particular system is chosen and the variables selected.

From a global perspective, wireless networks require considerably more “SA data” than their wired counterparts. Their nodal mobility and rapidly changing link characteristics are two of the most important factors. In wired networks, topology messages certainly need not be sent every few seconds as is required in MANETs, for instance.

The frequency of information and bandwidth required to send timely SA data were estimated, and found (in most cases) to be a small impact on link capacity. SA information could even be “piggy-backed” onto existing topology control messages, but this would need to be studied and modelled..

8.2 Recommended SA Model Enhancements

The SA model [1] is very generic. It is not tailored for any particular type of network or technology. For that reason, this report used the language of the model and looked at unique wireless network “vulnerabilities” and “safeguards” (sections 5 and 6). The SA data mentioned in this report (section 7) refers to the model’s “system description” and “alarms/events”. There is therefore no need to change the model’s terminology or overall approach to provide a meaningful situational awareness for wireless networks.

From an implementation perspective, of course, there are considerable differences in providing SA for wireless networks (as opposed to wired networks). There are very different vulnerabilities and safeguards to consider, and different types and frequency of data to report on the state of the network.

Of particular importance, SA data might be arriving at a central point (e.g., JNDMS) at a rate of one message every one to five seconds per node (or MPR) for a highly mobile wireless network This data must be processed so that an officer or network manager can make sense of the state of the network. The onus is therefore on JNDMS to process rapidly time-variable data into a much slower time-variable component of trends or real-time events, at a rate which can make sense to a human operator. This is a major difference in how JNDMS will process data for wired networks.

8.3 Future Work

This report was only a first step in understanding the SA implications of wireless networks and the interfaces which may be required between wireless nodes and JNDMS to assemble and analyze SA data.

Wireless network technology is quickly evolving. Two areas which will certainly have an impact on JNDMS in the near future are the inclusion of high-mobility nodes (4G high rate mobility cellular or high rate – high mobilty (HRHM) is the commercial application) and self-configuring secure MANETS using cognitive radio technology. Both will impact the type and quantity of management data required for effective wireless network situational awareness, and new coding techniques may be required to minimize the effects on bandwidth.

9. References

1. Julie Lefebvre, Marc Gregoire, Luc Beaudoin, and Michael Froh, “Computer Network Defence Situational Awareness: Information Requirements”, DRDC Ottawa TM 2005-254. Defence R&D Canada – Ottawa. 2005.

2. “The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks (DSR)”, IETF Internet-Draft, June 19, 2004, draft-ietf-manet-dsr-10.txt

3. Michael Froh, “Coalition Information Assurance (CIA) Common Operating Picture (COP) Requirements”, DRDC Ottawa CR 2006-125. Defence R&D Canada – Ottawa. 2006.

4. Richard Breton and Robert Rousseau, “Situation Awareness: A Review of the Concept and its Measurement”, DRDC Valcartier TR 2001-220, Defence R&D Canada – Valcartier. 2003.

5. Dr. John Salerno, Mr. Mike Hinman, Mr. Doug Boulware, Mr. Paul Bello, “Information Fusion for Situational Awareness”, AFRL/IFEA, Air Force Research Laboratory, Rome Research Site, Rome, NY, 2003

6. Leslie D. Cumiford, “Situation Awareness for Cyber Defense”, Sandia National Laboratories, Alberquerque, NM, 2006

7. Nikos Migas, William J. Buchanan, and Kevin A. McArtney, “Mobile Agents for Routing, Topology Discovery, and Automatic Network Reconfiguration in Ad-Hoc Networks”, 10th IEEE International Conference and Workshop on the Engineering of Computer-Based Systems (ECBS'03), 200-206, 2003

8. Alex Bordetsky, Susan G. Hutchins, William G. Kemple, Eugene Bourakov, “Network Awareness for Wireless Peer-to-Peer Collaborative Environments”, Proceedings of the 37th Hawaii International Conference on System Sciences, 2004

9. L. Li and L. Lamont, "A Lightweight Service Discovery Mechanism for Mobile Ad hoc Pervasive Environment using Cross-Layer Design", Proceedings of the 2nd Mobile Peer-to-Peer Computing Workshop (MP2P), in conjunction with the 3rd IEEE International Conference on Pervasive Computing and Communications (PerCom'05), Kauai Island, Hawaii, USA, March 2005.

10. R.Chandra, C. Fetzer, K. Hogstedt, “Adaptive Topology Discovery in Hybrid Wireless Networks”, Informatics '02, 2002

11. Lynne Genik, “A Survey of Canadian Forces Wireless Systems and their Security”, DRDC Ottawa TM 2004-005. Defence R&D Canada – Ottawa. 2004.

12. “STU III Replacement Reminder”, IT Security Bulletin ITSB-24, Communications Security Establishment, July 6, 2005

13. Internet Engineering Task Force (IETF) Request for Comment (RFC) 2740, OSPF for IP v6, called OSPF version 3

14. “OSPF Security Vulnerabilities Analysis”, IETF Internet-Draft, June 16, 2006, draft-ietf-rpsec-ospf-vuln-02.txt

15. “OSPF MPR Extensions for Ad Hoc Networks”, IETF Internet-Draft, March 6, 2006, draft-baccelli-ospf-mpr-ext-01

16. IETF RFC 3561, “Ad Hoc On-Demand Distance Vector Routing”

17. Hu, Yih-Chun, Perrig, Adrian, and Johnson, David, “Rushing Attacks and Defense in Wireless Ad Hoc Network Routing Protocols”, WiSe 2003, San Diego, September 19, 2003

18. IETF RFC 3626, “Optimized Link State Routing Protocol”

19. Yih-Chun Hu, Adrian Perrig, and David Johnson, “Packet Leashes: A Defense Against Wormhole Attacks in Wireless Ad Hoc Networks”, Technical report, Department of Computer Science, Rice University, September, 2002

20. Maria Gorlatova et al, “Detecting Wormhole Attacks in Ad Hoc Networks through Protocol Breaking and Packet Timing Analysis”, DRDC Ottawa, unpublished, 2006

21. “Propagation Model Development and Comparisons”, Institute for Telecommunications Sciences, 2005 Progress Report, U.S. Department of Commerce, January, 2006

22. K.A. Remley, C.A. Grosvenor, R.T. Johnk, D.R. Novotny, P.D. Hale, M.D. McKinley, A. Karygiannis, E. Antonakakis, "Electromagnetic Signatures of WLAN Cards and Network Security," The 5th IEEE International Symposium on Signal Processing and Information Technology (IEEE ISSPIT 2005) Athens, Greece, December 18-21, 2005

23. A. Patwardhan, J. Parker, A. Joshi, A. Karygiannis and M. Iorga, “Secure Routing and Intrusion Detection in Ad Hoc Networks”, Third IEEE International Conference on Pervasive Computing and Communications, Kauaii Island, Hawaii, March 8-12, 2005

24. Mounir Benzaid, Pascale Minet, and Khaldoun Al Agha, “Integrating Fast Mobility in the OLSR Routing Protocol”, Fourth IEEE Conference in Mobile and Wireless Communications Networks, Stockholm, Sweden, September 2002

25. Luis Villasenor-Gonzalez, Ying Ge, Louise Lamont, "HOLSR: A Hierarchical Proactive Routing Mechanism for Mobile Ad Hoc Networks", IEEE Communications Magazine, Vol 43, No. 7, July, 2005

26. D. Dhillon, T. Randhawa, M. Wang, L. Lamont, "Implementing a Fully Distributed Certificate Authority in an OLSR MANET", WCNC 2004 IEEE Wireless Communication and Networking Conference, Atlanta, Georgia, USA, March 21-25, 2004

27. “CEQMM: A Complete and Efficient Quality of Service Model for MANETs”, IETF Internet-Draft, October 6, 2006, draft-badis-manet-ceqmm-01.txt

28. CSE Approved Cryptographic Algorithms for the Protection of Protected Information and for Electronic Authentication and Authorization applications within the Government of Canada, CSE, ITSA-11(c), April 18, 2006

29. “CSE Approves Secure BlackBerry”, IT Security Bulletin 06, CSE, September 8, 2003

30. “Procurement of the BlackBerry Security Module”, IT Security Bulletin 12, CSE, October 29, 2003

31. “Blackberry IT Policy Manager”, Research in Motion, 2002

32. “Blackberry with the S/MIME Support Package”, White Paper, Version 4, Research in Motion, 2004

33. “Recommendation for Block Cipher Modes of Operation - Methods and Techniques”, NIST Special Publication 800-38A, December 2001

34. Yvo de Jong, “On the Implementation of Iterative Detection in Real-Time MIMO Wireless Systems”, DRDC Ottawa TR 2003-242, December, 2003

35. “MANET Neighbourhood Discovery Protocol (NHDP)”, IETF Internet-Draft, June 19, 2006, draft-ietf-manet-nhdp-00

36. Joshua Wright, “Layer 2 Analysis of WLAN Discovery Applications for Intrusion Detection”, home.jwu.edu/jwright/papers/l2-wlan-ids.pdf, November 8, 2002

37. Karygiannis, A., Antonakakis, E., and Apostolopoulos, A., "Detecting Critical Nodes for MANET Intrusion Detection Systems," 2nd International Workshop on Security, Privacy and Trust in Pervasive and Ubiquitous Computing, Lyon, France, June 29, 2006

38. Yongguang Zhang and Wenke Lee, “Intrusion Detection in Wireless ad-hoc Networks”, Proceedings of the 6th annual international conference on Mobile computing and networking, Boston, August 6-11, 2000

39. Kachirski, Oleg and Guha, Ratan, “Effective Intrusion Detection Using Multiple Sensors in Wireless Ad Hoc Networks, Proceedings of the 36th Hawaii International Conference on System Sciences (HICSS’03), 2003

40. Yongguang Zhang, Wenke Lee, Yi-An Huang, “Intrusion Detection Techniques for Mobile Wireless Networks”, Wireless Networks, Volume 9, Issue 5, September, 2003

41. Christropher Besemann et al, “Intrusion Setection System in Wireless Ad-Hoc Networks: Sybil Attack Detection and Others”, www.cs.ndsu.nodak.edu/~kawamura/doc/IDSinWirelessAdHocNetworksSybilAttack.pdf , 2004

42. Ioanna Stamouli, “Real-time Intrusion Detection for Ad Hoc Networks”, M.Sc. Thesis, University of Dublin, September 12, 2003

43. Anjum, Farooq et al, “Signature based Intrusion Detection for Wireless Ad-Hoc Networks”, Mobicom 2000

44. Bo Zhu , Feng Bao , Robert H. Deng , Mohan S. Kankanhalli , Guilin Wang, Efficient and Robust Key Management for Large Mobile Ad Hoc Networks, Computer Networks: The International Journal of Computer and Telecommunications Networking, v.48 n.4, p.657-682, 15 July 2005

45. Gustave Anderson, Donovan Artz, Vincent A. Cicirello, Moshe Kam, Nicholas Morizio, Andrew Mroczkowski, Max Peysakhov, William Regli, and Evan Sultanik, “The Secure Wireless Agent Testbed: An Integration of Mobile Agents. Security, and Ad Hoc Networking, Submitted to IEEE Transactions on Systems, Man, and Cybernetics Part C. (Under Review)

46. Constantinos Spyrou, George Samaras, Evaggelia Pitoura, and Paraskevas Evripidou, “Mobile Agents for Wireless Computing: The Convergence of Wireless Computational Models with Mobile-Agent Technologies”, Mobile Networks and Applications 9, 517-528, 2004

47. Wayne Jansen, “Intrusion Detection with Mobile Agents”, Computer Communications, Special Issue on Intrusion Detection Systems, vol. 25, number 4, September 2002.

48. Hairong Qi and Feiyi Wang, “Optimal Itinerary Analysis for Mobile Agents in Ad Hoc Wireless Networks”, The 13th International Conference on Wireless Communications, vol. 1, pp.147-153. Calgary, Canada, July, 2001

49. Evan et al, Secure Mobile Agents on Ad Hoc Wireless Networks, IEEE Intelligent Systems , Volume 20, Issue 5, September 2005

50. Kwindla Hultman Kramer, Nelson Minar, and Pattie Maes, “Tutorial: Mobile Software Agents for Dynamic Routing, Mobile Computing and Communications Review, Vol. 3, No. 2, April, 1999

51. C. K. Tham S. Marwaha and D. Srinivasan, “Mobile agents based routing protocol for mobile ad hoc networks”, Proceedings of IEEE, Globecorn,, 2002

52. Wesam Al Mobaideen, “Performance Evaluation of Mobile Agents Paradigm for Wireless Networks”, Department of Computer Science, University of Bologna, Technical Report UBKCS-2003-04, March, 2003

53. T. Lindhoim, and F. Yellin, ”The Java Virtual Machine Specification”, Addison Wesley, 1997

54. D. Horvat, D. Cvetkovic, V. Milutinovic, P. Kocovic, and V. kovacevic,”Mobile Agents and Java Mobile Agents Toolkits”, IEEE Proceeding of the 33rd Hawaii International Conference on System Sciences-2000, Pages: 3090-3099, 2000

55. R. Gray, D. Kotz, G. Cybenko, and D. Rus, ”DAgent: Security in a Multiple Language, Mobile-Agent System”, In Giovanni Vigna, Editor, Mobile Agents and Security, Volume 1419 of Lecture Notes in Computer Science, Pages 154-186. Springer-Verlag, 1998

56. D. Lange, ”Java Aglets Application Programming Interface (JAAPI)”, IBM Corp. White Paper, Feb., 1997

57. G. Glass, ”ObjectSpace Voyager Core Package Technical Overview”, Mobility: Process, Computers and Agnets, Addison-Wesley, Feb, 1999

58. C. Baumer, M Breugst, S. Choy, and T. Magedanz, ”Grasshopper- A Universal Agent Platform based on OMG, MASIF and FIPA Standards”, First International Workshop on Mobile Agents for Telecommunication Applications (MATA’99), Pages 1-18, Ottawa, Canada, October 1999

59. Sun Microsystems, ”Java Remote Method Invocation- Distributed Computation for Java”, White Paper, 1998

60. Yan Zhou, "Intelligent Agent Routing for Mobile Ad-hoc Networks", Dalhousie University MCSc Thesis, 2003

61. Wenwei Yue, “An Improved Agent-Based Routing Protocol for Mobile Ad-Hoc Networks”. Dalhousie University MCSc Thesis, 2004

Annex A – Blackberry IT Security Policy Settings

These policies are directly or indirectly related to the security of assets stored, processed, or transferred by the BES or the BlackBerry handheld. They are centrally managed on BES and cannot be changed by the BlackBerry user. The recommended values are based on sound security principles, but any application should be based on a risk assessment.

Non-Grouped Device-Only Items

Policy item	Description	Recommended Use	Recommended Values
Password Required	Use this policy item to specify whether the handheld requires a security password. Click TRUE to enable a required password on the handheld, or click FALSE to disable the password requirement on the handheld.	Typically, organizations set this option to TRUE. Note: The user still has the ability to disable the password on the handheld unless you also configure the UserCanDisablePassword policy item with a FALSE value.	**TRUE**
Allow Peer-to-Peer Messages	Use this policy item to specify whether handheld users can use PIN-to-PIN messaging on the handheld. Click TRUE to make this functionality available to handheld users, or click FALSE to exclude handheld users from using PIN-to-PIN messaging and make it unavailable on the handheld.	Typically, this policy is set to TRUE. Set the option to FALSE if you have security concerns in your organization regarding PIN-to-PIN messages.	**FALSE**
Minimum Password Length	Use this policy item to specify the minimum allowable length of the handheld security password, in characters, which must be between 4 and 14 characters inclusive. Type the minimum number of password characters in the	Typically, set this option according to your organization's password length policy. If no such policy exists, the recommendation is to set a minimum of 6 characters and a maximum of 8 characters.	**8**

Policy item	Description	Recommended Use	Recommended Values
	field provided, and then click OK.		
User Can Disable Password	Use this policy item to specify whether the handheld user can disable the specified security password. Click TRUE to enable this option, or click FALSE to disable the option.	Typically, set this option FALSE to prevent users from disabling their own passwords. In the absence of a security policy, set this option to FALSE.	**FALSE**
Maximum Security Timeout	Use this policy item to specify the maximum time in minutes allowed before a handheld security time out occurs. In the field provided, type the number of minutes until the time out occurs (a minimum value of 1 and a maximum value of 60 is allowed), and then click OK. The handheld user can select any time out value less than the maximum value.	Typically, set this option if your organization has a security policy. If you do not have a security policy, the recommended minimum value is 30.	**5**
Maximum Password Age	Use this policy item to specify how many days until a handheld user's password expires. In the field provided, type the number of days between password expiries (a minimum value of 0 and a maximum value of 65535 is allowed), and then click OK. A value of 0 disables password aging.	Typically, set this option if your organization has a password expiration policy. If you do not have a password expiration policy, the recommended minimum value is 30.	**30 to 60, depending on organization policies**
User Can Change Timeout	Use this policy item to specify whether the handheld user can change the specified security time out. Click TRUE to enable this option, or click FALSE to disable the option.	Typically, set this option to FALSE as most organizations' security policies require. In the absence of a security policy, set this option to FALSE.	**TRUE**

Policy item	Description	Recommended Use	Recommended Values
Password Pattern Checks	Use this policy item to create a pattern check on the handheld security password. The possible values are 0 to 3. Type 0 in the field provided to perform no password pattern check. Type 1 in the field provided to require that the password has at least one digit and one letter to be acceptable. Type 2 in the field provided to require that the password has at least one digit, one letter, and one special character to be acceptable. Type 3 in the field provided to require that the password mixes upper and lower case characters and has at least one digit, one letter, and one special character to be acceptable. Click OK.	To enable a high level of security, recommendation is to set this value to a minimum of 1.	**2**
Enable Long Term Timeout (Periodic Challenge Time)	Specifies whether the handheld locks after a pre-defined period of time, regardless of user activity.	Typically, organizations set this option to FALSE. If set to TRUE, the default time is one hour. Use the Set Password Timeout IT policy item to change the time until the security time out occurs.	**TRUE**
Allow SMS	Use this policy item to specify whether handheld users can use SMS messaging on the handheld. Click TRUE to make this functionality available to handheld users, or click FALSE to exclude handheld users from using SMS messaging and make it unavailable on the	Typically, organizations set this option to TRUE. This policy item is available only on the Java-enabled handhelds.	**FALSE**

Policy item	Description	Recommended Use	Recommended Values
	handheld.		
Allow BCC Recipients	Use this policy item to specify whether users can specify BCC recipients on email messages. Click TRUE to make this functionality available to handheld users, or click FALSE to make BCC recipients unavailable to handheld users.	Typically, this option is set to TRUE to enforce recipient confidentiality.	**TRUE**
Home Page Address is Read-Only	Use this policy item to specify if the URL address of the Home Page can be modified by the handheld user. Click TRUE to make the URL Read-Only (not writable); click FALSE to make the URL not Read-Only (writable).	Most organizations set this option to TRUE.	**TRUE**
Enable WAP Config	Use this policy item to disable (hide) the WAP browser icon even if the carrier has provisioned the WAP browser and the appropriate service books are present. This policy item is available only on the Java-enabled handhelds. Click FALSE to hide the WAP browser icon on the handheld; click TRUE to enable the WAP browser icon on the handheld.	Most organizations set this option to FALSE.	**FALSE**
Default Browser Configuration UID	Use this policy item to specify a unique ID for the Browser Configuration Service Record, which sets the default browser to use (for example, when opening links in email messages). Type the unique ID in the field	Typically, set this option to the unique ID of the default Browser Configuration Service Record. This policy item is available only on the Java-enabled handhelds.	**The UID of the HTML Browser associated with the BES will be entered**

Policy item	Description	Recommended Use	Recommended Values
	provided, and then click OK.		

Non-Grouped Desktop-Only Items

Policy item	Description	Recommended Use	Recommended Values
Show Application Loader	Use this policy item to specify whether the handheld user has access to the application loader in the desktop software. Click TRUE to make this functionality available to the handheld user, or click FALSE to hide the application loader from the user.	Typically, organizations set this option to TRUE. If your organization has a centralized application.	**FALSE**
Force Load Count	Use this policy item to specify how many times a handheld user is allowed to decline when prompted to update the handheld. Type a value to indicate the number of times the user can decline when prompted before a forced handheld update occurs, and then click OK. If the value is 0 or higher, and the user declines to update their handheld software the specified number of times, the BlackBerry desktop loader forces the handheld software to update. Set the value to -1 to disable the forced update and reminder messages.	Set this option to send a message reminding a user to update the handheld software.	**Not Applicable as "Show Application Loader" policy is set to FALSE**
Sync Email Instead of Import	Use this policy item to specify whether the Personal Information Manager (PIM) allows email and folder synchronization to occur instead of an import of moves and deletes on the handheld. Click TRUE to enable the	Typically, organizations set this option to TRUE.	**TRUE**

Policy item	Description	Recommended Use	Recommended Values
	email synchronization option, or click FALSE to disable the option.		
Email Conflict Desktop Wins	Use this policy item to specify what happens when a conflict occurs between the desktop and the handheld during Personal Information Manager (PIM) synchronization. Click TRUE to enable desktop information to overrule handheld information, or click FALSE to enable handheld information to overrule desktop information.	Typically, organizations set this option to TRUE.	**TRUE**
Disable Wireless Calendar	Use this policy item to specify whether the wireless calendar synchronization option (BlackBerry Wireless Sync) is available to handheld users in the calendar option of the Personal Information Manager (PIM). Click TRUE to make this functionality unavailable to handheld users, or click FALSE to allow handheld users to use the wireless calendar synchronization option.	Wireless calendar synchronization is a significant feature of the BlackBerry solution. Most organizations set this option to FALSE to enable the wireless calendar synchronization feature. Note: Wireless calendar synchronization is only available with version 2.1 or later of the handheld software and BlackBerry Desktop Software version 2.1.	**FALSE**
Auto Backup Enabled	Use this policy item to control enabling of the Automatically backup my handheld option. Click TRUE to enable prompting for automatic backups, or click FALSE to disable prompting for automatic backups.	Typically, set this option to TRUE to enable clean recovery of handheld data in the event that the handheld must be replaced.	**FALSE**
Auto Backup Frequency	Use this policy item to specify how often an automatic backup is performed. Its value is measured in days. Type the number of days to occur between automatic backups in	Typically, organizations set this value to 2 or more days, to enable changes to be made on the handheld to data stored between backups, so that users do	**Not applicable as "Auto Backup Enable" policy is FALSE**

Policy item	Description	Recommended Use	Recommended Values
	the field provided, and then click OK. The allowable range of values is 1 to 99 days. If no value is specified, a default value of 7 days will be used.	not need to wait for backups to occur when synchronizing the handheld while it is connected to the computer. Backup files should be saved to a network drive if disk space on the user's local hard drive is limited.	
Auto Backup Include All	Use this policy item to specify whether all data can be included in automatic backups. Click TRUE to enable all data to be included and to select the Backup all handheld application data option in BlackBerry Desktop Manager Backup and Restore, or click FALSE to enable some data to be excluded from backups.	Note: The policy item Auto Backup Include All must be set to FALSE if the Auto Backup Exclude Sync and Auto Backup Exclude Email keys are set to TRUE.	**Not applicable as "Auto Backup Enable" policy is FALSE**
Auto Backup Exclude Email	Use this policy item to specify whether email can be excluded from automatic backups. Click TRUE to enable email to be excluded, or click FALSE to include email in backups.	The policy item Auto Backup Include All must be set to FALSE if this key is set to TRUE.	**Not applicable as "Auto Backup Enable" policy is FALSE**
Auto Backup Exclude Sync	Use this policy item to specify whether synchronized application data (data configured for synchronization with Intellisync) can be excluded from automatic backups. Click TRUE to enable synchronized application data to be excluded, or click FALSE to include synchronized application data in backups.	Note: The policy item Auto Backup Include All must be set to FALSE if this key is set to TRUE.	**Not applicable as "Auto Backup Enable" is FALSE**
Show Web Link	Use this policy item to specify whether the handheld user has access to the Web Link icon in the desktop software. Click TRUE to make the icon available to the handheld user,	Typically, organizations set this option to TRUE.	**FALSE**

Policy item	Description	Recommended Use	Recommended Values
	or click FALSE to hide the icon from the user. This setting requires that you also specify a value for the Web Link URL setting.		
Web Link URL	Use this policy item to specify the URL for the Web Link icon, if it appears. Type a valid URL in the field provided, and then click OK. This setting requires that you also set Show Web Link to TRUE.	Typically, set the URL according to your organization's requirements.	**Not applicable as the "Show Web Link" policy is set to FALSE**
Web Link Label	Use this policy item to specify the label for the Web Link icon, if it appears in the desktop software. Type a label in the field provided, and then click OK.	Typically, set the label according to your organization's requirements.	**organization requirements**
Auto Signature	Use this policy item to specify the signature to be automatically attached to the handheld user's email messages. Type the text of the signature in the field provided, and then click OK.	Typically, the auto signature is used by organizations to add a disclaimer to the end of all outgoing email messages for specific users.	**organization Disclaimer**
Forward Messages In Cradle	Use this policy item to specify whether the handheld continues to receive messages while the handheld is connected to the computer using the cradle or a USB cable. Click TRUE to enable the handheld user to receive email while the handheld is connected to the computer, or click FALSE to prevent the handheld from receiving email when connected to the computer. The Disable handheld redirection while the handheld is in the cradle check box in the BlackBerry Desktop Manager Desktop Redirector	Typically, organizations set this option to FALSE.	**FALSE**

Policy item	Description	Recommended Use	Recommended Values
	is selected or deselected accordingly.		
Don’t Save Sent Messages	Use this policy item to specify whether a copy of each message sent by the handheld user is saved to a Sent Messages folder. Click TRUE to prevent saving sent messages, or click FALSE to save sent messages.	Typically, organizations set this option to FALSE to enable storage on the mail server of messages sent from the handheld.	**TRUE or FALSE as per organization policy**
Allow Other Email Services	Use this policy item to allow or disallow the use of other email services on the handheld. Click TRUE to allow other email service books on the handheld, or click FALSE to configure the handheld to reject all email service books other than the Desktop service book. Clicking FALSE forces all outbound email through your organization’s BlackBerry Enterprise Server.	Typically, this option is set to TRUE to enable an alternate email address for the user on the handheld.	**FALSE**
Allow Other Browser Services	Use this policy item to allow or disallow the use of other browser transport services on the handheld. Click TRUE to allow other browser transport service books on the handheld, or click FALSE to configure the handheld to reject all browser transport service books other than the Desktop service book.	Typically, set this option to FALSE to force all browser traffic through your organization’s BlackBerry Enterprise Server. If users have another browser application loaded on the handheld that they wish to use, set this option to TRUE.	**FALSE**
Force Load Message	Use this policy item to specify a string that appears (in place of the default string) when users are required to update to a later version of the BlackBerry handheld software. Type a string in the field provided, and then click OK.	—	**Not Applicable as “Show Application Loader” policy is set to FALSE**

Non-Grouped Global Items

Policy item	Description	Recommended Use	Recommended Values
Allow Phone	Use this policy item to specify whether handheld users can use the phone capabilities of the handheld. Click TRUE to make this functionality available to handheld users, or click FALSE to exclude handheld users from using the phone functionality and make it unavailable on the handheld.	This policy item is available only on the Java-enabled handhelds. Warning: Setting, modifying, or removing this policy item causes the handheld to reset upon receiving the IT policy update.	**TRUE**
Allow Browser	Use this policy item to specify whether handheld users can use the browser on the handheld. Click TRUE to make this functionality available to handheld users, or click FALSE to exclude handheld users from using the browser.	This option is typically set to TRUE unless users in your organization do not need or are not permitted to use the browser.	**TRUE**

Password Policy Group

Policy item	Description	Recommended Use	Recommended Values
Set Password Timeout	Use this policy item to specify the amount of time, in minutes, before the security timeout occurs on the handheld. The allowable range of time is between 0 and 60 minutes. Set the value to 0 to disable automatic locking of the handheld.	The value specified must be less than or equal to the value set for the Maximum Security Timeout policy item if it is set.	**5**
Set Maximum Password Attempts	Use this policy item to specify the number of security password attempts (incorrect passwords entered) allowed on the handheld before the handheld data is erased and the handheld disabled. The allowable range of attempts is 3 to 10.	If you set a maximum number of password attempts, notify handheld users of the maximum number so that they do not exceed that number when trying to recall a forgotten password.	**5**

Policy item	Description	Recommended Use	Recommended Values
Suppress Password Echo	Use this policy item to prevent password characters from printing onscreen ('echoing') after the maximum number of allowable failed password attempts.		**FALSE**
Maximum Password History	Use this policy item to specify the maximum number of prior passwords against which new passwords can be checked to prevent reuse of the old passwords. The allowable range of passwords retained in the password history is 0 to 15.	Type a number in the field provided below; entering 0 disables password reuse. Entering 5, for example, prevents reuse of the last 5 passwords used on the handheld.	**10**

SMIME Application Policy Group

Policy item	Description	Recommended Use	Recommended Values
Enable Wireless Email Reconciliation	Use this policy item to specify whether the wireless email reconciliation functionality is supported on the handheld. This also requires that the Enable Wireless Email Reconciliation on this server option is already selected on the BlackBerry Enterprise Server Properties window Email Options tab. If the server is enabled to support this functionality, click TRUE to enable wireless email reconciliation on the handheld. Click FALSE to disable wireless email reconciliation on the handheld.	Wireless email reconciliation support for the server and all its users is enabled by default. If this policy item is not added to the IT policy to which a user is assigned, wireless email reconciliation support is still enabled by default. This enables the Wireless Reconcile option on the handheld by default.	**TRUE**
Attachment Viewing	Use this policy item to enable or disable users to view attachments on the	By default, if no setting is specified for this item, attachment viewing is	**TRUE**

Policy item	Description	Recommended Use	Recommended Values
	handheld. Click TRUE to enable attachment viewing on the handheld; click FALSE to disable attachment viewing on the handheld.	enabled for all users who are on a BlackBerry Enterprise Server with attachment service installed, running, and connected to the BlackBerry Enterprise Server through an attachment connector.	

Security Policy Group

Policy item	Description	Recommended Use	Recommended Values
Force SmartCard Handheld Locking	Use this policy item to enable or disable support for smart cards to be used to lock and unlock handhelds. Click TRUE to enable smartcard locking and unlocking support; click FALSE to disable this support.	Note: This setting applies only to handhelds with the S/MIME Support Package installed.	**FALSE**
Force SmartCard To Unlock Keyboard	Use this policy item to specify whether or not a smartcard is required to unlock the handheld using a keyboard. Click TRUE to require a smartcard; click FALSE to disable this requirement.	Note: This setting applies only to handhelds with the S/MIME Support Package installed.	**FALSE**
Disable Untrusted Certificate Use	Use this policy item to specify whether outgoing email messages are encrypted with untrusted certificates. Click TRUE to prevent the user from sending a message that is encrypted using an untrusted certificate; click FALSE to warn the user that the certificate is untrusted. Clicking	Note: This setting applies only to handhelds with the S/MIME Support Package installed.	**TRUE**

Policy item	Description	Recommended Use	Recommended Values
	FALSE does not prevent the user from using a certificate that is untrusted.		
Disable Revoked Certificate Use	Use this policy item to specify whether outgoing messages are encrypted with revoked certificates. Click TRUE to prevent the user from sending a message that is encrypted using a revoked certificate; click FALSE to warn the user that the certificate is revoked. Clicking FALSE does not prevent the user from using a revoked certificate.	Note: This setting applies only to handhelds with the S/MIME Support Package installed.	**TRUE**
Disable Email Normal Send	Use this policy item to specify whether email messages can be sent as clear text (in other words, normally). Click TRUE to require a secure email package on the handheld and BlackBerry Enterprise Server, preventing email messages from being sent as clear text; click FALSE to disable this requirement.	Note: This setting applies only to handhelds with the S/MIME Support Package installed.	**FALSE**
Disable Peer-to-Peer Normal Send	Use this policy item to specify whether Peer-to-Peer (PIN-to-PIN) messages can be sent as clear text (in other words, normally). Click TRUE to require a secure email package on the handheld and BlackBerry Enterprise Server, preventing Peer-to-Peer messages from being sent as clear text; click FALSE to disable this requirement.	Note: This setting applies only to handhelds with the S/MIME Support Package installed.	**FALSE**
Disable Key	Use this policy item to	Note: This setting applies	**TRUE**

Policy item	Description	Recommended Use	Recommended Values
Store Low Security	disable or enable setting the key store security level to Low. Click TRUE to disable setting the security level to Low; click FALSE to enable setting the security level to Low.	only to handhelds with the S/MIME Support Package installed.	
Key Store Password Maximum Timeout	Use this policy item to specify the maximum number of minutes allowed before the cached keystore password times out. The allowable range of values is between 0 and 60 minutes. Enter the value in the field provided. The default value is 1. A value of 0 prevents the keystore password from timing out.	Note: This setting applies only to handhelds with the S/MIME Support Package installed.	**2**
Disallow Third Party Application Downloads	Use this policy item to disallow downloading to the handheld of third party applications (in other words, applications not authored by Research In Motion). Click TRUE to prevent downloading of third party applications; click FALSE to allow third party applications on the handheld.		**TRUE**
Force Lock When Holstered	Use this policy item to enable or disable automatic locking of the handheld when placed in the holster. Click TRUE to enable locking, requiring the user to enter a password each time the user removes the handheld from the holster; click FALSE to disable automatic locking of a holstered handheld.	—	**TRUE**
Allow Third	Use this policy item to	By default, if no setting is	**FALSE**

Policy item	**Description**	**Recommended Use**	**Recommended Values**
Party Apps To Use Serial Port	enable or disable third party applications to use the serial port, IrDA or USB ports on the handheld. Click TRUE to enable third party applications loaded on the handheld to use the serial port, IrDA or USB ports on the handheld; click FALSE to disable running third party applications using the serial port, IrDA or USB ports on the handheld.	specified for this item, third party applications are automatically enabled to run using the serial port, IrDA or USB ports on the handheld.	
Allow Internal Connections	Use this policy item to enable or disable all internal connections from the handheld. Click TRUE to enable internal connections from the handheld; click FALSE to disable internal connections from the handheld.	By default, if no setting is specified for this item, all internal connections are enabled on the handheld. Allows connection to the BlackBerry Enterprise Server Mobile Data Service	**TRUE**
Allow External Connections	Use this policy item to enable or disable all external connections from the handheld. Click TRUE to enable external connections from the handheld; click FALSE to disable external connections from the handheld.	By default, if no setting is specified for this item, all external connections are enabled on the handheld.	**TRUE**
Allow Split-Pipe Connections	Use this policy item to enable or disable applications to open both internal and external connections simultaneously. Click TRUE to enable applications to open both internal and external connections simultaneously; click FALSE to disable opening	Enabling split pipe connections presents a security issue because, when enabled, applications can surreptitiously collect data from inside the firewall and send it outside the firewall without any auditing. By default, if no setting is specified for this item, split pipe connections are disabled on the	**FALSE**

Policy item	Description	Recommended Use	Recommended Values
	both internal and external connections simultaneously.	handheld.	
Disable Invalid Certificate Use	Use this policy item to control the user's ability to send a message using a certificate that has expired or is not yet valid. Click TRUE to prevent the user from sending a message that is encrypted using a certificate that has expired or is not yet valid; click FALSE to warn the user that the certificate has expired or is not yet valid. Clicking FALSE does not prevent the user from using a certificate that has expired or is not yet valid.	Note: This setting applies only to handhelds with the S/MIME Support Package installed.	**TRUE**
Disable Weak Certificate Use	Use this policy item to control the user's ability to send a message using a certificate that has a weak corresponding public key. Click TRUE to prevent the user from sending a message that is encrypted using a certificate that has a weak corresponding public key; click FALSE to warn the user that the certificate has a weak corresponding public key. Clicking FALSE does not prevent the user from using a certificate that has a weak corresponding public key.	Note: This setting applies only to handhelds with the S/MIME Support Package installed.	**TRUE**
Trusted Certificate Thumb Prints	Use this policy item to define a string that contains a semi-colon-separated list of Hex-ASCII certificate thumbprints, generated using either SHA1 or MD5. If the string is present, the	Note: This setting applies only to handhelds with the S/MIME Support Package installed.	**Not Set**

Policy item	Description	Recommended Use	Recommended Values
	user cannot add any certificate with a thumbprint does not appear in the defined list to the trusted key store.		

TLS Application Policy Group

Policy item	Description	Recommended Use	Recommended Values
TLS Disable Weak Ciphers	Use this policy item to enable or disable the use of weak ciphers during a TLS connection. Enter a value in the field provided; enter 0 to disable weak ciphers, 1 to enable weak ciphers, or 2 to prompt the handheld when weak ciphers are used.		**0**
TLS Disable Untrusted Connection	Use this policy item to enable or disable the use of untrusted connections during a TLS connection. Enter a value in the field provided; enter 0 to disallow untrusted connections, 1 to allow untrusted connections, or 2 to prompt the handheld when untrusted connections are used.		**0**
TLS Minimum Strong RSA Key Length	Use this policy item to specify the minimum RSA key size, in bits, allowed for use in TLS connections. The valid range for this setting is 512 to 4096 bits.	A default value of 1024 is used if this value is not set.	**1024**
TLS Minimum Strong DH Key Length	Use this policy item to specify the minimum DH key size, in bits, allowed for use in the TLS connection. The valid	A default value of 1024 is used if this value is not set.	**1024**

Policy item	Description	Recommended Use	Recommended Values
	range for this setting is 512 to 4096 bits.		
TLS Minimum Strong ECC Key Length	Use this policy item to specify the minimum ECC key size, in bits, allowed for use in the TLS connection. The valid range for this setting is 160 to 571 bits.	A default value of 163 is used if this value is not set.	**163**
TLS Disable Invalid Connection	Use this policy item to enable or disable the use of connections to servers with invalid certificates during TLS connections. Enter a value in the field provided; enter 0 to disallow invalid connections, 1 to allow invalid connections, or 2 to prompt the handheld when invalid connections are used.		**0**
TLS Restrict FIPS Ciphers	Use this policy item to enable or disable the use of any cipher that is not FIPS compliant. Click TRUE to restrict use of non-FIPS compliant ciphers; click FALSE to enable use of any non-FIPS compliant ciphers.	If no setting is specified for this item, by default, use of any non-FIPS compliant cipher is disabled.	**TRUE**
TLS Minimum Strong DSA Key Length	Use this policy item to specify the minimum DSA key size, in bits, allowed for use in TLS connections. The valid range for this setting is 512 to 1024 bits.	A default value of 1024 is used if this value is not set.	**1024**

WTLS Application Policy Group

Policy item	Description	Recommended Use	Recommended Values
WTLS Disable Weak Ciphers	Use this policy item to enable or disable the use of		**0**

Policy item	Description	Recommended Use	Recommended Values
	weak ciphers during WTLS connections. Enter a value in the field provided; enter 0 to disable weak ciphers, 1 to enable weak ciphers, or 2 to prompt the handheld when weak ciphers are used.		
WTLS Disable Untrusted Connection	Use this policy item to enable or disable WTLS connections to untrusted servers. Enter a value in the field provided; enter 0 to disallow untrusted connections, 1 to allow untrusted connections, or 2 to prompt the handheld when untrusted connections are used.		**0**
WTLS Minimum Strong RSA Key Length	Use this policy item to specify the minimum RSA key size, in bits, allowed for use in WTLS connections. The valid range for this setting is 512 to 4096 bits. A default value of 1024 is used if this value is not set.		**1024**
WTLS Minimum Strong DH Key Length	Use this policy item to specify the minimum DH key size, in bits, allowed for use in the WTLS connection. The valid range for this setting is 512 to 4096 bits. A default value of 1024 is used if this value is not set.		**1024**
WTLS Minimum Strong ECC Key Length	Use this policy item to specify the minimum ECC key size, in bits, allowed for use in the WTLS connection. The valid range for this setting is 160 to 571 bits. A default value		**163**

Policy item	Description	Recommended Use	Recommended Values
	of 163 is used if this value is not set.		
WTLS Disable Invalid Connection	Use this policy item to enable or disable WTLS connections to servers with invalid certificates. Enter a value in the field provided; enter 0 to disallow invalid connections, 1 to allow invalid connections, or 2 to prompt the handheld when invalid connections are used.		**0**

Browser Policy Group

Policy item	Description	Recommended Use	Recommended values
MDS Browser Title	Use this policy item to set a name in the ribbon of the Mobile Data Service Browser window.		**Not Set**

Desktop Policy Group

Policy item	Description	Recommended use/default setting	Recommended values
Desktop Password Cache Timeout	Use this policy item to specify the time, in minutes, that the desktop caches the handheld password in memory. The allowable range of values is 0 to 720 minutes. If the value is set to 0, the cache timeout is disabled; the password cache s cleared only when the handheld is disconnected from the computer, regardless of the length of time the handheld is connected to the	The value defaults to 10 minutes.	**5**

Policy item	**Description**	**Recommended use/default setting**	**Recommended values**
	computer.		
Desktop Allow Desktop Add-ins	Use this policy item to specify whether or not the desktop enables the user to configure and execute desktop add-ins (third-party COM-based extensions that access the handheld databases during synchronization). When this policy is set to FALSE, the Configure Add-ins and Execute Add-in actions options are disabled in the desktop software.	The value defaults to TRUE if the policy is not set.	**FALSE**
Desktop Allow Device Switch	Use this policy item to control whether the Desktop software enables or disables the user switching handhelds. Click TRUE to enable the user to switch handhelds; click FALSE to disable the user switching handhelds.	By default, if no setting is specified for this item, the user is enabled to switch handhelds.	**FALSE**

Bluetooth Policy Group

Policy item	Description	Recommended Use Default	Recommended Values
Disable Handsfree Profile	Disables the use of Bluetooth handsfree peripherals.	FALSE	**FALSE**
Disable Headset Profile	Disables the use of Bluetooth headsets.	FALSE	**FALSE**
Disable Pairing	Disables the ability to establish a relationship or pair . with another Bluetooth device.	Once you have established a pairing with an approved device, (for example a headset), use this rule to prevent the user from establishing any subsequent pairings.	**TRUE**
Disable Serial Port Profile	Disables the ability to communicate with a serial port that has been Bluetooth-enabled.	FALSE	**TRUE**

Annex B – Summary of Blackberry Safeguards [32]

Security architecture

Users can use the handheld browser to access data on the Internet or corporate intranet and can use third-party applications that require secure access behind the firewall. The Mobile Data Service uses a standard Internet protocol such as HTTP or TCP/IP. The same encryption that protects data that is sent to or from users' handhelds is used to protect data from the Internet, and online corporate data and applications.

An HTTP connection can be set up over SSL/TLS (Hypertext Transfer Protocol over Secure Sockets, or HTTPS) to provide additional authentication and security if an application accesses servers on the Internet. The handheld supports HTTPS communication in one of the following modes, depending on corporate security requirements:

- Proxy mode SSL/TLS: The Mobile Data Service sets up the SSL/TLS connection on behalf of the handheld. Communication over the wireless network between the handheld and BlackBerry Enterprise Server is not encrypted using SSL/TLS, but it is still Triple-DES or AES encrypted. A point exists behind the corporate firewall where data is not encrypted.

- Handheld direct mode SSL/TLS: Data is encrypted over SSL/TLS for the entire connection between the handheld and the origin server. This type of connection is considered to be more secure than proxy mode because data remains encrypted and is not decrypted at the Mobile Data Service.

In proxy mode SSL, the user experiences faster response times, but the system administrator must be trusted with the data. Handheld direct mode SSL/TLS is appropriate when only the endpoints of the transaction are trusted (for example, with banking services).

Note: Handheld direct mode SSL is supported on BlackBerry Wireless Handhelds with handheld software version 3.6.1 or later.

Wireless Transport Layer Security

BlackBerry supports Wireless Transport Layer Security (WTLS), which provides an extra layer of security when connecting to a Wireless Application Protocol (WAP) gateway. WTLS requires a WAP gateway to provide standard WAP access to the Internet. To use a WAP gateway, a company must work with the network operator or service provider. WTLS is supported in BlackBerry Handheld Software version 3.2.1 or later.

IT policies and IT commands

In the past, personal devices, such as mobile phones and personal digital assistants (PDAs), were difficult if not impossible for system administrators to manage. Even if system administrators deployed them, devices seldom contained the technology to track or monitor them effectively. With the advent of powerful new devices that can access and store more sensitive corporate data, controlling the security of these devices becomes a much more important issue. In the wrong hands, roaming devices with remote access to sensitive data could be dangerous.

With the BlackBerry Enterprise Solution, a system administrator can monitor and control all BlackBerry handhelds from the BlackBerry Enterprise Server Management console. With BlackBerry Enterprise Server version 4.0, BlackBerry incorporates a high level of wireless IT control. This control is accomplished using wireless IT commands and IT policy.

Wireless IT commands

System administrators can control BlackBerry handhelds remotely using wireless IT commands. These commands are most commonly used on lost or stolen handhelds. The following wireless IT commands are available to system administrators:

- Erase all Application Data: This command erases all user and application data that is stored on the BlackBerry handheld. If a handheld has been stolen or cannot be found, the system administrator can erase all information and application data remotely.

- Set a Password and Lock the Handheld: With this command, the system administrator creates a new password and locks the handheld remotely. If the user is uncertain of the handheld location, the system administrator can set a password (if one has not been set) and lock the handheld. The system administrator can then verbally communicate the new password to the user when the handheld is found. The user is prompted on the handheld to accept or reject the new password change.

> Note: If content protection is enabled, the administrator will not be able to reset the user’s password remotely.

- Reset the Password and Lock the Handheld: If the user has forgotten the handheld password, the system administrator can reset the password remotely and communicate the new password to the user.

Wireless IT commands enable system administrators to immediately respond to a lost or stolen handheld and protect confidential enterprise information.

IT policies for security settings

IT policies enable system administrators to customize the features such as password, mail forwarding, and browser options that are common to all BlackBerry handheld users on a given BlackBerry Enterprise Server. IT policies provide an efficient method for managing many different users simultaneously.

With wireless IT policy, custom settings can be enabled from the BlackBerry Enterprise Server and immediately enforced on C++-based BlackBerry handhelds running handheld software version 2.5 or later and Java-based BlackBerry handhelds running handheld software version 3.6 or later.

Using the BlackBerry Enterprise Server, system administrators can set specific IT policies to define how users use the security settings that are included on BlackBerry handhelds and in the BlackBerry Desktop Manager.

• IT policies for security: The BlackBerry Enterprise Solution offers users many different security settings for the BlackBerry handheld and BlackBerry Desktop Manager. All BlackBerry user security settings can be defined by system administrators. For example, system administrators specify whether a password is required, the length of time that a password can exist before it becomes invalid, and the length and composition of a password. Encryption key details can also be specified using an IT policy.

• Wireless policy deployment: All IT policies, including security settings, can be immediately applied wirelessly. This innovative feature is extremely important, because many handheld users are mobile workers who rarely synchronize their handhelds with the enterprise network. To accomplish wireless delivery of new policies and immediate user adoption, IT policy settings are automatically written to the user configurations. To verify that the settings are always current, the BlackBerry Enterprise Server periodically transmits handheld settings to the handheld wirelessly.

• Continuous updating of IT policies: All IT policies, including security settings, are updated regularly. The BlackBerry handheld is updated periodically through wireless policy deployment. With continuous updating, BlackBerry users quickly adopt new IT policies, including security settings.

• Group policies: The IT policy feature enables a system administrator to define a policy for a group and apply it to all users in the group instead of creating a policy for each user. For example, a system administrator can create a policy for executives, and assign each executive to the group policy.

BlackBerry Router authentication protocol

The BlackBerry Router connects to the BlackBerry Enterprise Server and routes data to handhelds that are connected to the BlackBerry Handheld Manager through a serial/USB port. The handheld must authenticate itself to the BlackBerry Enterprise Server before the BlackBerry Router can send data to the handheld.

1. User connects the handheld: The user connects the handheld to a desktop computer that is running the BlackBerry Handheld Manager.

2. Handheld is authenticated: The BlackBerry Router uses a unique authentication protocol to verify that the user is a valid user. The authentication sequence uses the authentication information that the BlackBerry Enterprise Server and the handheld use to validate each other to determine whether the connection is valid. The BlackBerry Router does not learn the value of the master encryption key that passes between the handheld and the server.

3. Data bypasses the wireless network: The BlackBerry Router and the BlackBerry Handheld Manager manage all data flow to and from the handheld through the physical connection.

- Data from the handheld is sent to the BlackBerry Router through the BlackBerry Handheld Manager.
- Data to the handheld is sent from the BlackBerry Router to the handheld through the BlackBerry Handheld Manager.

All data between the handheld and the BlackBerry Enterprise Server is compressed and encrypted. When the user disconnects the handheld or closes the BlackBerry Handheld Manager, the wireless data flow is restored.

Corporate firewall or proxy

After the initial connection to the BlackBerry Infrastructure is established (over the Internet), the connection to the BlackBerry Infrastructure is persistent and used to send traffic between the BlackBerry Enterprise Server and the handheld. Outbound traffic from the BlackBerry Enterprise Server has no destination other than the BlackBerry handheld through the wireless network. Inbound traffic to the BlackBerry Enterprise Server from any source other than the handheld (through the BlackBerry Infrastructure or BlackBerry Desktop Software) or the Messaging Server is discarded.

The TCP connection through port 3101 is designed to be secure in the following ways:

The connection to the wireless network is outbound-initiated by the BlackBerry Enterprise Server and must be authenticated. No inbound-initiated traffic is permitted.

All data traffic between the BlackBerry Enterprise Server and the user’s handheld is encrypted using Triple-DES or AES encryption. All data remains encrypted along the entire path from the BlackBerry Enterprise Server to the handheld or from the handheld to the BlackBerry Enterprise Server. There is no staging location in which the data is decrypted and encrypted again. Therefore, all communications between the BlackBerry Enterprise Server and the handheld are protected by encryption from all unauthorized parties, including RIM. The BlackBerry Enterprise Server only accepts data that it can decrypt using a valid encryption key. No communication of any kind can occur between the BlackBerry Enterprise Server and wireless network or handheld unless this condition is met. Because only the handheld and server have a valid encryption key, no datagrams are accepted from any outside source.

BlackBerry Wireless Handheld

The BlackBerry Enterprise Solution uses either the Triple-DES or AES encryption algorithm to protect data while it is in transit between the BlackBerry Wireless Handheld and BlackBerry Enterprise Server. All messages that the BlackBerry Wireless Handheld sends or receives are Triple-DES or AES encrypted. This encryption verifies that a BlackBerry message remains protected in transit to the BlackBerry Enterprise Server while it is outside the corporate firewall.

Users can use a password to lock the handheld when it is not in use. The handheld password is an important feature for securing handheld data, and it can be forced by system administrators through the use of an IT policy. When creating a password, the user must create a strong password without using repetition or excessive simplicity. Passwords that consist of a natural sequence (such as 1, 2, 3, 4, 5) or identical characters are rejected by the handheld.

The handheld only stores a SHA-1 hash of the password. A hash is a function that takes a variable-length input string and converts it into a fixed-length numerical representation of the original value. The hash is known as a one-way function because it cannot be reversed easily to reveal the password value.

The user can also specify a security timeout, which indicates the number of idle minutes that occur before the handheld locks so that data stored on the handheld remains safe in the event of a theft or loss. When the handheld locks, either from a security timeout or from a user command, the owner information is immediately displayed and access to data through the keyboard or serial/USB port is prevented until the user types the correct password. In version 3.6 or later of the BlackBerry Handheld Software, users can set the handheld to lock whenever it is inserted in the holster. This locking can also be set through an IT policy.

By default, a user is limited to ten password attempts on the BlackBerry handheld. The data on the handheld is deleted after ten incorrect password attempts. If users have a current backup of the handheld data on the desktop, they can use the backup and restore tool in the BlackBerry Desktop Software to replace the data on the handheld. System administrators can change the value of the password setting through an IT policy.

Annex C – Brief Review of Mobile Agent Technologies

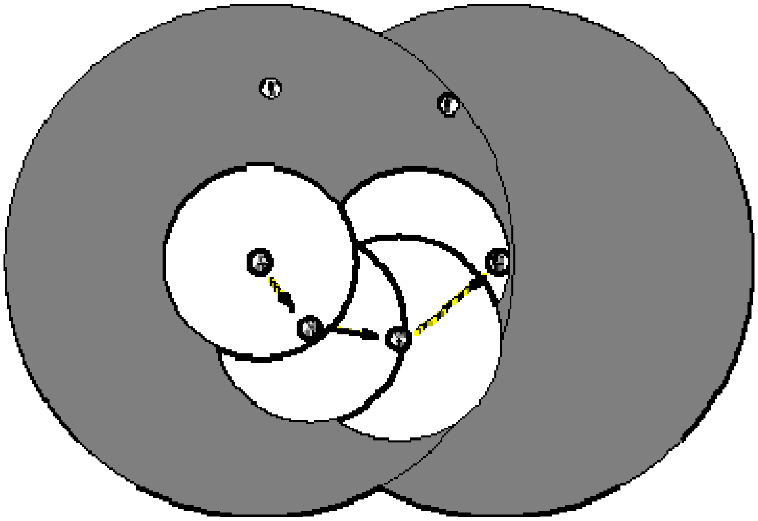
C.1 Multihop routing and mobile agents

Why use mobile agent technologies in wireless networks? The answer lies in the topologies common in most mobile ad hoc networks (MANETS). These networks generally do not communicate from A (the transmitter) to B (the receiver) in one hop.

Rather, multihop routing is used to make those networks more efficient in terms of bandwidth and nodal power requirements. But that efficiency comes at some expense[9], and mobile agents are often used to improve the “downside” of multihop routing.

In Figure 1, the shaded areas indicate a one-hop end-to-end communications connection for nodes A and B, following the illustration from [50]. If A sets up a one-hop connection, the connection would take up a bandwidth slot in the entire shaded area (prohibiting nodes ‘I’ from using the same slot), and the nodal power requirements would be greater to cover such a wide area. Management could be easily centralized, however, since a node in each of the shaded circles could readily handle channel assignments and utilization, accommodating changes in demand, link performance, or other factors.

Figure 1 – Bandwidth usage in multihop routing



[9] Such as the vulnerability of rogue intermediate nodes, increaaed end-to-end use of the bandwidth over time, and differing subnet link characteristics.

The white areas of Figure 1 illustrate a multihop connection between A and B. In this scenario, nodes ‘I’ could communicate on the same bandwidth slot as A uses, but it would take longer to set up the A-B connection. In addition, an efficient route must be selected between A and B (in this case, the route includes nodes X and Y), where intermediate nodes must have sufficient capacity, be located on a ‘least cost’ path to minimize the number of links, and/or be on a path which minimizes impairments (maximizes performance).

Some problems, of course, are that nodes X and Y must be trusted (i.e., a rogue intermediate node could hijack the connection and launch a variety of confidentiality, integrity, or availability attacks), the nodes may be moving (constantly coming into and out of range), and link characteristics of A-X, X-Y, and Y-B links may be changing due to occupancy or environmental factors. And there’s no easy way to centrally manage such a distributed connection.

Mobile agents permit coordinated decentralized management in a MANET. They can facilitate routing by adapting to network changes (even if those changes occur in widely separated links) and facilitate the timely application of safeguards by adapting to threat agent exploits and attempted exploits.

C.2 Characteristics of mobile agents

The following are some of the major characteristics of effective mobile agents [50]:

- Agents encapsulate a thread of execution along with a bundle of code and data. Each agent runs independently of all others, is self-contained from a programmatic perspective, and preserves all of its state information when it moves from one network node to another. The latter is termed strong mobility.

- Any agent can move easily across the network. The underlying infrastructure provides a language-level primitive that an agent can call to move itself to a neighbouring node.

- Agents must be small in size. Because there is some cost associated with hosting and transporting an agent, they are designed to be as minimal as possible. Simple agents serve as building blocks for complex aggregate behaviour.

- An agent is able to cooperate with other agents in order to perform complex or dynamic tasks. Agents may read from and write to a shared block of memory on each node, and they can use this facility to coordinate with other agents executing on that node and to leave information behind for subsequent visitors.

- An agent is able to identify and use resources specific to any node on which it finds itself. From an agent’s perspective, nodes are differentiated (at least) by who their neighbours are and how locally congested the network is. Certain nodes might also have access to particular kinds of information, such as absolute location derived from a global positioning system receiver, that agents could access and use.

C.3 Mobile agent technologies

Various types of and applications for mobile agents have been proposed (and tested) in a variety of MANET environments. Applications of agent technologies have been described in [7], [45], [46], [47], [48], [49], [50], [51], and [52].

This section is a brief overview of mobile agent technologies, most of which are based on the Java programming language.

C.3.1 Java Developer's Kit

Java provides a portable, general purpose, easy to learn, secure, network aware object oriented language [53]. Java is an interpreted programming language that, instead of compiling the source code into native instructions code, it compiles into a bytecode. Java bytecode is an intermediate format that can be interpreted on any platform that has a Java Virtual Machine(JVM) - the Java interpreter suitable for that platform. This design of Java platform independence ensures great portability for Java programs and makes it especially suitable for mobile agents.

Mobile agent systems implemented in Java provide its agents with two main migration mechanisms - remote method invocation (RMI[10], as used in Voyager, see section C.3.4, and is the most common mechanism), or through sockets, as used in Aglet (see section C.3.3).

RMI is a feature of the Java Developer's Kit (JDK), where an object can invoke Java public methods of another remote object. When using RMI for agent migration, the agent first sends a local message to initialize the migration process on its current local host, which then invokes the public method on another host to initialize the transfer process of the agent between them. The remote host then requests the agent object from the mobile agent's current local host. The local host serializes the agent object and sends it to the remote host. After the agent's resources and data has been transferred, the remote host informs the local one that the transfer is completed and restarts the agent execution [54].

Using sockets as the migration mechanism, the mobile agent code and data are converted to a byte array that would be protocol independent. The process begins when the mobile agent invokes a public method on the local host which causes the mobile agent to be serialized and passed to another layer to be prepared for transfer. When it is ready, the mobile agent is sent to the new host by using a standard transport protocol such as TCP.

C.3.2 D'Agents

D'Agents system, known as 'Agent Tcl', was developed at Dartmouth College. It supports agents written in Tcl, Java, and Scheme [55]. D'Agents supports strong mobility by capturing and restoring the complete state of a migrating agent. However, supporting strong mobility in

[10] Java RMI [59] aims to make communication between two objects in different virtual machines transparent and simple. Java RMI is built on top of a transport layer that usesTCP connections.

Java requires a specialized version of the Java Virtual Machine. This means that the system will work only with the modified JVM, which impacts portability, since this modified virtual machine is no longer ubiquitous.

C.3.3 Java Aglets

Java Aglets [56] was developed by the IBM Laboratory in Japan. Aglets extend Java to support mobile agents with weak mobility. Two migration primitives are supported: dispatch, an asynchronous and immediate mechanism of shipping the code of the Aglet to the specified context, and retract, which fetches the Aglet stand-alone code and is used to bring the Aglet back to it's home context. Sockets is the migration mechanism used.

C.3.4 Voyager

Voyager [57] is an advanced, Java-based Object Request Broker (ORB) that supports universal communication between Voyager, SOAP, CORBA, Remote Method Invocation (RMI) and Distributed Component Object Model (DCOM) objects. Voyager enables dynamic and static proxy generation and offers a built-in distributed 'garbage collection system'.

To enable autonomous mobile agent movement, Voyager loads the agent classes by searching the Classpath in the destination machine, and if that class does not exit, it uses the classloaders that have been registered either by the targeted server or by the mobile agent itself to load the required classes from the machine that is declared as the source of these classes. However, Voyager does not load the agent's thread state to the new location. Instead, it restarts the code execution on the new location.

Agent migration in Voyager is done using RMI to transfer the mobile agent object to a destination specified in the destination address.

C.3.5 Grasshopper

Grasshopper [58] is an agent technology that conforms to the OMG MASIF (Object Management Group's Mobile Agent System Interoperability Facility). Implemented in Java, it allows agents to talk to each other via an Agent Communication Language (ACL).

The agent environment consists of regions, places, agencies, and agents. A region facilitates the management of other distributed components such as places, agencies, and agents. The region's registry keeps information about the currently hosted distributed components. When an agent moves, it's registered information is updated automatically in the correspondent registry.

Two parts constitute an agency - the Core Agency and one or more Places. Places enable logical groupings inside the agency. The core agency offers the following minimal functionality required to execute an agent:

- Communication Service deals with distributed components' interaction and creates the illusion of transparent communication, so that there is no difference between remote and local method invocation. Communication service can be used internally to send or receive agents or for locating entities within the distributed agent environment.

- Management Service allows a human user to monitor and control places and agents of an agency.
- Registration Service allows an agency to record information about all currently hosted places and agents.
- Security Service protects the agency resources and remote communication from unauthorized interaction.
- Persistent Service enables recovery after a system crash by storing agents and places on a persistent medium.

C.3.6 Mole

Mole [59] is implemented in Java and supports strong and weak mobility. Mole places, i.e., Mole's computational environment, enable agents to run as threads of the Java virtual machine. Through what is termed Service Agents (actually, stationary agents), places provides Mole's mobile agent with access to the underlying operating system's functionality.

Agents in Mole can communicate among them either by a remote procedure call (RPC) or session based communication. Every agent has to be identified by an identifier called badge in order to set up a session to another mobile agent. After session set up, agents can communicate either by remote method invocation or by message passing. The session method of communication can be considered a synchronous way of communication among agents that allows them to coordinate and cooperate among themselves. An agent is not allowed to move to a different host during a session.

C.4 Application to SA

The application of mobile agent technology to support situational awareness was described in section 7.2.4. From a MANET perspective, mobile agents can provide more efficient routing (and routing information to JNDMS). But of equal importance, mobile agent tools will give more opportunity to safeguard vital information and infrastructure by providing ways to specify trust relationships that can be verified in real time. That verification (or lack thereof) is important SA data.

C.5 Future work in mobile agent technologies

There is much current research on improving mobile agent functionality and efficiency. Some areas of current research are briefly discussed in this section.

C.5.1 Mobile Agent Specialisation

Mobile agent populations need not be homogeneous. Research is ongoing[11] into a diverse collection of interacting mobile programs, which can form an agent ecology. Human network managers can manage the diversity of the agent ecosystem, monitoring the state of a sub-network and adjusting the agent population to match changing circumstances. Or agent populations can be designed to regulate themselves. For example, a very simple self adjustment strategy would be for each agent belonging to a certain class to monitor the resources that it and its peers consume, and to die off or spawn new copies of itself depending on supply and demand.

Different agents in an ecology could fill different roles. Several distinct kinds of specialization are possible:

- Agents can specialize with regard to usage patterns across the network.
- Specialized agents could work to manage requirements in specific areas of a network.
- Agents can adapt the network infrastructure to changing needs over time.
- Agents can specialize on behalf of specific users.

This last type of specialization points at perhaps the most distinctive new feature of mobile agent architectures: the ability for individual users to inject code into a system that changes how local infrastructure works. Collections of agents could be dispatched to serve a particular user's (or the network’s) needs.

C.5.2 Accommodation of Future Networks

Mobile agents must admit a wide variety of network models, data rates, and node types. They must use common bandwidth very efficiently, because thousands of nodes may be deployed in a small area. Low power operation is extremely important, as battery life tends to be a limiting resource for much hardware, especially in military operations. And the communications links and mechanisms need to be abstract or transparent enough that researchers will find it easy to incorporate into standard communications components. Finally, mobile agents must be inexpensive to build, easy to deploy, and simple to maintain.

[11] See [7], [45], [46], [47], [48], [49], [50], and [51].

List of symbols/abbreviations/acronyms/initialisms

ACL	Access Control List, Agent Communication Language
AES	Advanced Encryption Standard
AODV	Ad Hoc On Demand Distance Vector
ATM	Asynchronous Transfer Mode
BER	Bit Error Ratio
BES	Blackberry Enterprise Server
bits/s	bits per second
b/s	bits per second
BSPK	Binary Phase Shift Keying
BSSID	Basic Service Set Identifier
CA	Collision Avoidance
CCK	Complementary Code Keying
CDMA	Code Division Multiple Access
CF	Canadian Forces
CHE	Complex Humanitarian Emergency
CIA	Coalition Information Assurance
C, I, and/or A	Confidentiality, Integrity, and/or Availability
CN	Computer Network
CND	Computer Network Defence
CoABS	Control of Agent-Based Systems

COMSEC	Communications Security
COP	Common Operating Procedure
CORBA	Common Object Request Broker Architecture
CRC	Cyclic Redundancy Check
CSE	Communications Security Establishment
CSMA	Carrier Sense Multiple Access
DAMA	Demand Assignment Multiple Access
DARPA	Defence Advanced Research Projects Agency
DCOM	Distributed Component Object Model
DES	Data Encryption Standard
DLPC	Downlink Power Control
DND	Department of National Defence
DQPSK	Differential Quadrature Phase Shift Keying
DRDC	Defence Research and Development Canada
DSR	Dynamic Source Routing
DSSS	Direct Sequence Spread Spectrum
EAP	Extensible Authentication Protocol
EEPC	End-to-End Power Control
EGP	Exterior Gateway Protocol
EHF	Extremely High Frequency
FCAPS	Fault, Configuration, Accounting, Performance, and Security
FDMA	Frequency Division Multiple Access
FHSS	Frequency Hopping Spread Spectrum
FSK	Frequency Shift Keying

G	giga (prefix)
GMSK	Gaussian Minimum Shift Keying
GPRS	General Packet Radio Service
GPS	Global Positioning System
GSM	Global System for Mobile Communications
HF	High Frequency
HOLSR	Hierarchical Optimized Link State Routing
HRHM	High Rate High Mobility
Hz	Hertz, cycles per second
IA	Information Assurance
IDM	Information Dissemination Management
IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronic Engineers
IETF	Internet Engineering Task Force
IGP	Interior Gateway Protocol
IIS	Information and Intelligent Systems
IP	Internet Protocol
IR	Infrared
ISM	Industrial, Scientific, and Medical; IP Service Monitor
IT	Information Technology
ITI	Information Technology Infrastructure
ITM	Irregular Terrain Model
ITU	International Telecommunications Union
IV	Initiation Vector

JDK	Java Developer’s Kit
JVM	Java Virtual Machine
JNDMS	Joint Network Defence and Management System
k	kilo (prefix)
LMCS	Local Multipoint Communications System
LORAN	Long Range Navigation
M	mega (prefix)
m	metres
MAC	Media Access Control
MANET	Mobile Ad Hoc Network
MIC	Message Integrity Code
MIMO	Multiple Input – Multiple Output
MOE	Measure of Efficiency
MOP	Measure of Performance
MPR	Multipoint Relay
M&S	Modelling and Simulation
NETOPS	Network Operations
NIO	Network Information Operations
NIST	National Institute of Standards
OBBS	On-Board Beam Shaping
OFDM	Orthogonal Frequency Division Multiplex
OLSR	Optimized Link State Routing
OMG MASIF	Object Management Group’s Mobile Agent System Interoperability Facility
OODA	Observe-Orient-Decide-Act

ORB	Object Request Broker
OSPF	Open Shortest Path First
PDA	Personal Digital Assistant
QAM	Quadrature Amplitude Modulation
QOLSR	Quality Optimized Link State Routing
QoP	Quality of Protection
QoS	Quality of Service
QPSK	Quadrature Phase Shift Keying
RADIUS	Remote Authentication Dial In User Service
R&D	Research and Development
RIM	Research in Motion
RIP	Routing Information Protocol
RF	Radio Frequency
RMI	Remote Method Invocation
RPC	Remote Procedure Call
RSA	Rivest, Shamir, and Adelman
SA	Situational Awareness
SAT	Situational Awareness Tool
SCPC	Single Channel Per Carrier
SHA	Secure Hash Algorithm
S/MIME	Secure Multipurpose Internet Mail Extensions
S&NM	Systems and Network Management
SNMP	Simple Network Management Protocol
SOAP	Simple Object Access Protocol

SSID	Service Set Identifier
SSL	Secure Sockets Layer
SUCV	Statistically Unique and Cryptographically Verifiable
TC	Topology Control
TCP	Transport Control Protocol
TDM	Time Division Multiplex
TDMA	Time Division Multiple Access
TDP	Technology Demonstration Project
TKIP	Temporal Key Integrity Protocol
TLS	Transport Layer Security
UDR	Usage Data Record
UHF	Ultra-High Frequency
ULPC	Uplink Power Control
WEP	Wired Equivalent Privacy
WiFi	Wireless Fidelity
WPA	WiFi Protected Access

DOCUMENT CONTROL DATA

(Security classification of title, body of abstract and indexing annotation must be entered when the overall document is classified)

1. ORIGINATOR (the name and address of the organization preparing the document. Organizations for whom the document was prepared, e.g. Establishment sponsoring a contractor's report, or tasking agency, are entered in section 8.)

TRM Technologies Inc.
151 Slater St Suite 100 Ottawa ON
K1P5H3

2. SECURITY CLASSIFICATION (overall security classification of the document, including special warning terms if applicable)

UNCLASSIFIED

3. TITLE (the complete document title as indicated on the title page. Its classification should be indicated by the appropriate abbreviation (S,C or U) in parentheses after the title.)

Considerations for Wireless Network Situational Awareness (U)

4. AUTHORS (Last name, first name, middle initial)

Gort, James

5. DATE OF PUBLICATION (month and year of publication of document)

November 2006

6a. NO. OF PAGES (total containing information. Include Annexes, Appendices, etc.)

90

6b. NO. OF REFS (total cited in document)

61

7. DESCRIPTIVE NOTES (the category of the document, e.g. technical report, technical note or memorandum. If appropriate, enter the type of report, e.g. interim, progress, summary, annual or final. Give the inclusive dates when a specific reporting period is covered.)

Contractor report

8. SPONSORING ACTIVITY (the name of the department project office or laboratory sponsoring the research and development. Include the address.)

Defence R&D Canada – Ottawa
Network Information Operations Section
3701 Carling Ave, Ottawa, ON K1A 0Z4

9a. PROJECT OR GRANT NO. (if appropriate, the applicable research and development project or grant number under which the document was written. Please specify whether project or grant)

15br01

9b. CONTRACT NO. (if appropriate, the applicable number under which the document was written)

W7714-6-3307

10a. ORIGINATOR'S DOCUMENT NUMBER (the official document number by which the document is identified by the originating activity. This number must be unique to this document.)

10b. OTHER DOCUMENT NOS. (Any other numbers which may be assigned this document either by the originator or by the sponsor)

DRDC Ottawa CR 2006-238

11. DOCUMENT AVAILABILITY (any limitations on further dissemination of the document, other than those imposed by security classification)

(x) Unlimited distribution
( ) Distribution limited to defence departments and defence contractors; further distribution only as approved
( ) Distribution limited to defence departments and Canadian defence contractors; further distribution only as approved
( ) Distribution limited to government departments and agencies; further distribution only as approved
( ) Distribution limited to defence departments; further distribution only as approved
( ) Other (please specify):

12. DOCUMENT ANNOUNCEMENT (any limitation to the bibliographic announcement of this document. This will normally correspond to the Document Availability (11). However, where further distribution (beyond the audience specified in 11) is possible, a wider announcement audience may be selected.)

13. ABSTRACT (a brief and factual summary of the document. It may also appear elsewhere in the body of the document itself. It is highly desirable that the abstract of classified documents be unclassified. Each paragraph of the abstract shall begin with an indication of the security classification of the information in the paragraph (unless the document itself is unclassified) represented as (S), (C), or (U). It is not necessary to include here abstracts in both official languages unless the text is bilingual).

Within the realm of information operations, computer network defence (CND) focuses on managing the vulnerabilities and risk inherent in all computer networks. While much of the current research in the field of CND situational awareness (SA) is focusing on a bottom-up approach of how to define meaning out of the abundance of sensor information, DRDC has done work in defining the information requirements for CND SA from a top-down approach. The Joint Network Defence and Management System (JNDMS) is a Technical Demonstrator Project (TDP) implementation of a service that will provide this situational awareness; however, the focus is on wired networks. The question which this report addresses is: What is important for situational awareness in a wireless network and how does it differ from that of a wired network?

14. KEYWORDS, DESCRIPTORS or IDENTIFIERS (technically meaningful terms or short phrases that characterize a document and could be helpful in cataloguing the document. They should be selected so that no security classification is required. Identifiers such as equipment model designation, trade name, military project code name, geographic location may also be included. If possible keywords should be selected from a published thesaurus. e.g. Thesaurus of Engineering and Scientific Terms (TEST) and that thesaurus-identified. If it is not possible to select indexing terms which are Unclassified, the classification of each should be indicated as with the title.)

wireless network situational awareness, computer network defence, vulnerabilities, safeguards