2011

Security aspects of sensor-based defence systems

Michael N. Johnstone
Edith Cowan University

DOI: 10.4225/75/57b5397ecd8c2
Originally published in the Proceedings of the 9th Australian Information Security Management Conference, Edith Cowan University, Perth Western Australia, 5th -7th December, 2011

SECURITY ASPECTS OF SENSOR-BASED DEFENCE SYSTEMS

Michael N. Johnstone
School of Computer and Security Science
Edith Cowan University, Perth, Western Australia
m.johnstone@ecu.edu.au

Abstract

The Australian Defence Force (ADF) has IMAP and JMAP to perform planning prior to the deployment of forces, but there is a knowledge gap for on-ground forces during the execution of an operation. Multi-agent based sensor systems can provide on-ground forces with a significant amount of real-time information that can be used to modify planning due to changed conditions. The issue with such sensor systems is the degree to which they are vulnerable to attack by opposing forces. This paper explores the types of attack that could be successful and proposes defences that could be put in place to circumvent or minimise the effect of an attack.

Keywords
Wireless Sensor Network, Vulnerability, Multi-Agent System, Information Systems Security.

INTRODUCTION

Bishop (2005, p4) defines a threat as "a potential violation of security.", whilst a vulnerability, according to the Internet Engineering Task Force is "A flaw or weakness in a system's design, implementation, or operation and management that could be exploited to violate the system's security policy." (RFC 2828, 2000, p190). Thus it follows that an exploit is an attack that takes advantage of a vulnerability therefore realising a threat. The purpose of this paper is to identify likely threats before they become attacks (or exploitable vulnerabilities) in wireless sensor network systems.

The key building blocks of information security are confidentiality, integrity and availability. Confidentiality refers to the idea that only authorised users have correct access to assets (assets in this case means the data transmitted over a wireless network). The guarantee of integrity means that only authorised users can alter data in clearly defined ways. Availability means that authorised users are able to access data in a timely fashion within operational constraints. Whilst there are well-known attacks for each of these building blocks (e.g. denial-of-service is clearly an attack on availability), it is an attack on integrity, specifically the classical "man in the middle" attack that is the focus of this paper.

This is an issue for modern combat systems. Sensor-based intelligence gathering has some advantages over more traditional forms (of intelligence gathering), specifically in the areas of ease of deployment, camouflage and redundancy. Sensors are small-footprint in terms of size and weight and therefore many can be deployed at once as part of reconnaissance, prior to an engagement. Also, their small size means that sensors can be disguised easily for a range of environments. Further, sensors can overlap which provides redundancy if one or more are rendered inoperative. This reliance on sensors comes at a cost, however. Potok et al. (2003) point out that in such systems information must be transmitted securely under often sub-optimal network conditions, otherwise their value is severely negated.

The structure of this paper unfolds in three dimensions: current thinking in technology-assisted defence operations, which is the problem domain (although 'defence' is a broad term and much of what is said here can apply to other domains where defence is the primary objective); multi-agent systems as a model of interaction that can replicate (military) group action; and wireless sensor networks as a means to collect and disseminate information for the agents.

COMMAND AND CONTROL IN MILITARY OPERATIONS

To say that the military environment is dynamic is something of an understatement. Whilst entities such as the Australian Defence Force have strategic planning tools such as the Joint Military Appreciation Process (JMAP) and its equivalent for individual input - the I(ndividual)MAP, neither of these tools can foresee every possible event or predict all outcomes in the complex scenario that is a battlefield situation.

The Australian Defence Forces command and control (C2) philosophy stresses flexibility. Control covers protocols, processes and equipment-it is the last of these that is the primary subject in this paper, although there are certainly processes and protocols for data transfer (ADF, 2003).

Alberts and Hayes (2003) consider that military organisation structures created during the industrial age (their phrase) worked because they a) used a hierarchical command structure with task specialisation for human resources; and b) split a large problem into simpler sub-tasks which could be achieved, thus attaining the overall operational goal. This is not dissimilar to "Tayloristic" project management which works for the same reasons. Alberts and Hayes then go on to point out the inevitable failure of such structures in what they call the information age, mainly due to a lack of flexibility and inertia.

In terms of network-centric warfare, the movement of C2 power and decision-making responsibility from a central command to the field is crucial. Alberts and Hayes (2003) identified six different approaches to command and control, viz: Cyclic, Interventionist, Problem-Solving, Problem-Bounding, Selective Control and Control Free. It is the last (least control-centric) approach that is of interest here because it the one where a headquarters issues directives, but defers decisions as to how those directives are carried out to lower echelon forces.

Alberts and Hayes (2003, p.27) note that the control free approach gives a commander significant autonomy, an approach that has been extremely successful in the past. However, this approach is not with its detractors who fear that the loss of control would lead to a high-risk chaotic situation. Alberts and Hayes conclude that such a situation will not occur because of the assumptions of self-synchronisation followed in network-centric warfare, viz:

- *Clear and consistent understanding of command intent;*
- *High quality information and shared situational awareness;*
- *Competence at all levels of the force; and*
- *Trust in the information, subordinates, superiors, peers, and equipment*.

Clearly, it is the second and fourth of these assumptions (that is, those relating to information) that are of significance here. As will be seen in the next section, multi-agent systems also share situational awareness amongst their peers and, at some level, trust in the information relayed by those same peers (agents).

A common extension to command and control systems is the notion of command, control and communication (C3) systems. In this context, C3 refers to technology-based systems as opposed to human communication systems. A further extension that is useful is C3I or C3+intelligence. This is not a new idea. In the 1980s, Orr (1983, p105) stated that "*Determination of the current power distribution and its evolution involves C3I capabilities most directly. Global surveillance is most important in this phase. Detection and identification of enemy units, combined with friendly force status information, determines the geometric force distribution. Estimates of capability and intent provided by the intelligence function help convert this geometric force distribution into a power distribution*". This power distribution provides an assessment of the outcome of an engagement prior to the operation, which is critical to a successful outcome.

Obviously the detection of enemy units via the nodes of a wireless sensor network and resulting decisions made by agents from the intelligence provided by the sensors can provide a tactical advantage. It would be more correct to say that the sensors provide data, which is placed in context (that is, is transformed into information) by the agents who then decide on a course of action using an appropriate strategy (that is,. transforms the information into intelligence). This notion shares some commonality with the traditional idea of the data—information—knowledge--wisdom continuum, but also recognises an alternative model, data + knowledge = information.

Potok et al. (2003) envision network-centric warfare to encompass fire control, targeting, reconnaissance and surveillance and sensor-based data acquisition (see figure 1 for an example). Such a system is somewhat more complex than that considered here but there are common elements no matter what the scale of the system. For example, global time-stamping of data is just as important for a targeting system as it is for a sensor system. In the case of the latter, erroneous time stamps leads to faulty intelligence which breaks the second assumption of Alberts and Hayes (2003).

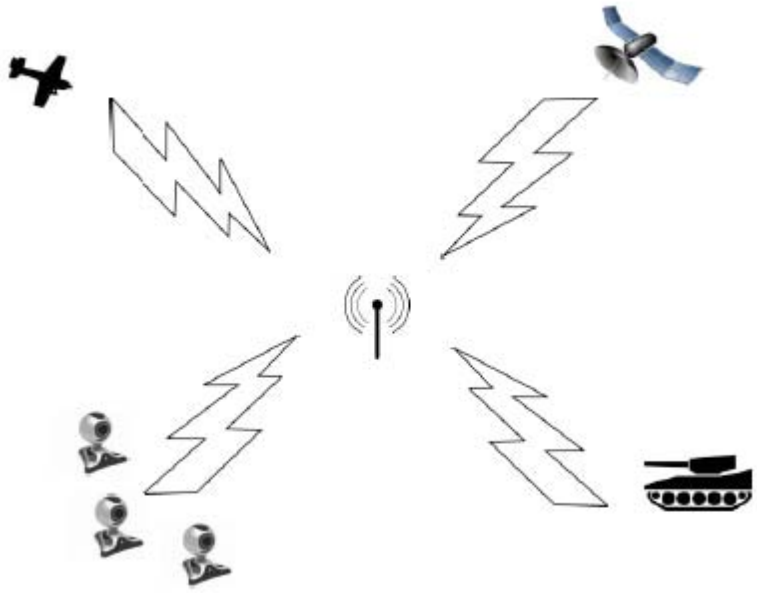

Figure 1: Potential Future Combat System Interconnections.

In summary, this section has shown that modern warfare is increasingly reliant on high-quality, reliable and timely information. The next section introduces the basic concepts of software agents and shows how agents, linked with appropriate data gathering devices, can provide that high-quality, reliable and timely information.

AGENTS AND MULTI-AGENT SYSTEMS

Agents are essentially autonomous software systems that behave as a peer-to-peer network. Agents have several useful properties that, to some extent, mimic human behaviour and thought processes, thus giving them significant utility in solving certain classes of problems.

Agents can perceive their environment (through sensors). They can also respond to changes in the environment reported by the sensors. Figure 2 shows that an agent receives sensory input from its environment and then takes action based on this input, which appears to be a simple model that suggests an agent is no more than a background software process such as a print server or a hardware device such as a thermostat. The properties that set agents apart from traditional AI systems are not perception and response, but the ability to initiate their own behaviour in order to satisfy a goal. Further, agents are capable of interacting with other agents to achieve their goal.

Agents can take the initiative, that is, they are non-deterministic (to some extent) within the constraints of their design objectives. Agents are also goal-directed and communicate with other agents in furtherance of that goal. Thus, agents are not simply objects or artificial intelligence systems. Another way to describe an agent is by its components, thus an agent consists of a sensor network which receives data from the environment, a memory structure which stores the data and a decision-making "engine" that makes choices to maximise the goal-seeking behaviour of the agent based on both current sensor input and stored memory of previous experiences with the environment. Usually, agents are considered to be 'selfish' in that they are completely autonomous and act to satisfy their goal. Without a doubt, in a military engagement, such behaviour would lead to chaos and the mission objective would not be attained. Therefore agents need a cooperative strategy which maximises not just a personal utility function, but links to an awareness of the mission goal and recognises that cooperation is a safer and more effective strategy. It is however, beyond the scope of this paper to elucidate further on the types of strategies used in multi-agent systems or the modal logic used to reason about the memory structures. By extension, a multi-agent system is one where autonomous, but connected agents cooperate to achieve a common goal. To do this the agents need to communicate, negotiate (cooperate) and coordinate their behaviour in some way.

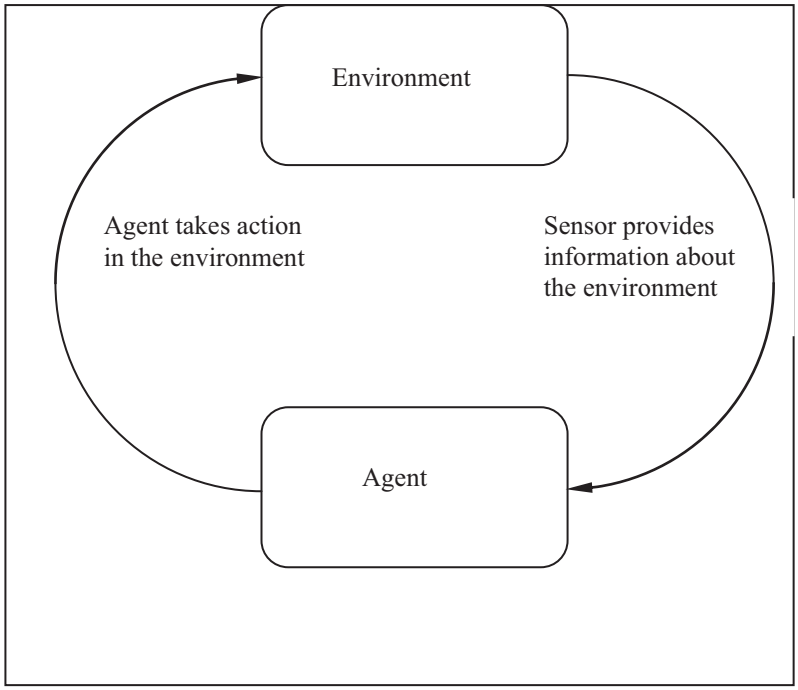

Figure 2: An Agent in its Environment (Adapted from Wooldridge, 2002).

Having briefly defined the nature of an agent it is useful to examine the types of problems that agents and multi-agent systems can be used to solve.

Beautement et al. (2005, p2), after Jennings and Wooldridge (1998) consider that domains which are open to solution with multi-agent systems can be categorised as:

- *open systems : systems with structures that evolve over time, are unknown in advance and are heterogeneous (the result of the actions of different actors independently and dependently)*
- *complex systems : characterized by Jennings and Wooldridge as systems that are too complex to understand without modularisation*
- *ubiquitous computing systems : which require interaction with all other actors in their environment in various contexts. Systems of this sort require interaction interfaces that go beyond the enumeration of the required behaviour and instead co-operate with users to achieve goals.*

Agent-based systems have certainly been proposed and used in a military context (Pohl et al., 2001; Potok et al., 2003), but it is constructive to consider military operations in the light of these categories. A military operation is partially an open system. The structures evolve over time and are potentially heterogeneous; however, the structures (plans) are known in advance (essentially the initial state). It is certainly possible to argue that military operations are complex systems as the traditional (as opposed to information age) method for planning such operations uses a hierarchical model and task decomposition because of the complex nature of such operations as discussed in a previous section. The issue of military operations as ubiquitous (computing) systems can be dealt with simply by considering them as systems qua systems, rather than having a specific computing orientation. With that assumption treated as valid, in a military operation interaction (communication and cooperation) is essential to attaining a mission objective (and thus achieving goals).

Tynan et al. (2005) consider that an architecture where each agent controls a number of wireless sensor nodes (see next section) offers advantages in terms of scalability and lower coordination cost when compared to a one agent per sensor model. Fro a military operation where potentially hundreds of sensors are distributed, this seems an efficient and balanced architecture.

Given the above (admittedly brief) analysis, it seems that military operations are a domain well-suited to solution with the aid of multi-agent systems. How, then, do the agents sense the physical environment? This is the subject of the next section.

WIRELESS SENSOR NETWORKS

Wireless networks typically have dynamic topologies, are unprotected from other signals sharing the medium and communicate over a medium that is significantly less reliable than their wired counterparts (IEEE, 2007). A wireless sensor node consists of a microprocessor, a radio frequency transmitter/receiver, a power supply (usually a battery or possibly a solar cell) and a sensor of some type. The types of sensors that can be used to provide data are traditionally microphones and cameras (still and video). Other types of sensors that would also provide valuable information are certainly available, for example, pressure, temperature and movement sensors. Such sensors could also be coupled together in that a movement sensor might trigger a dormant camera. This would have benefits in terms of power consumption as the low power device (the movement sensor) is on continuously, but the high power consumption/high bandwidth device is only activated when there is possibly something of interest to detect.

Two important properties of a wireless network are the data transfer rate and the maximum distance between transmit/receive nodes. IEEE 802.11a has a transfer rate of approximately 54Mbps and a range of 120m under ideal conditions (outdoors, few obstructions). 802.11n has a transfer rate of approximately 248Mbps and a range of 250m-not surprising as 802.11n was designed to address the speed limitations of prior 802.11.x standards. By comparison, 802.15.4 has a transfer rate of between 40-250Kbps and a range of 75m, again under ideal conditions. It would appear that 802.15.4 is at a significant disadvantage compared to 802.11.x, but this is not so as the shorter range requires less power.

Following the development of the 802.15.4 standard, several bodies, for example, the ZigBee Alliance, were formed to champion the development of low-power networks in various application areas. The Zigbee standard is not the same as 802.15.4 (with which it is often confused), but is a protocol stack built on top of the IEEE standard (see figure 3). Strictly speaking, Zigbee now uses the 802.14.5 standard, but the distinction is not significant for this discussion. Zigbee-based devices offer a potential solution where many sensors will be deployed in sub-optimal conditions, however they suffer from two drawbacks. First, power consumption is an issue as the devices are often small and powered by batteries and second, security is a potential issue. It would not be a suitable outcome if an enemy were to be able to inject false data into the communications stream.

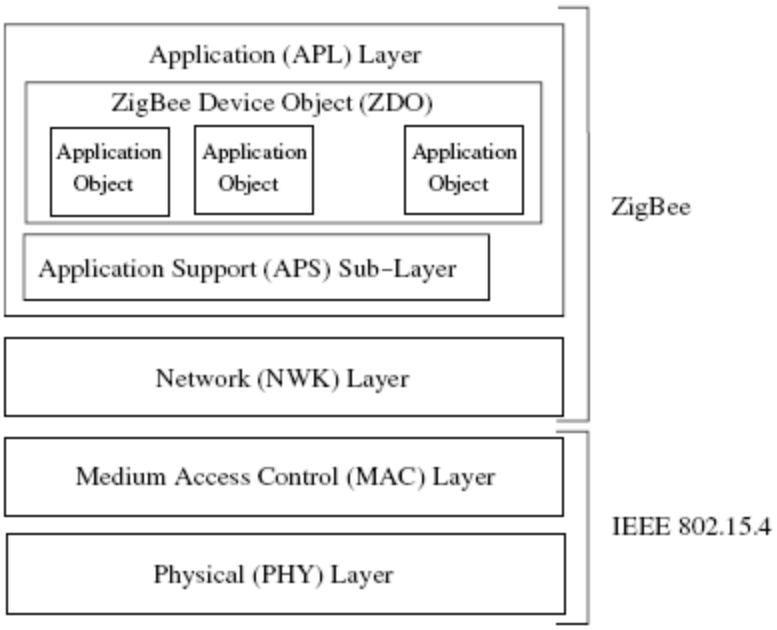

Figure 3: The Relationship between 802.15.4 and Zigbee (Akyildiz and Vuran, 2010, p6).

Most wireless sensors operating in idle mode consume power at a rate approximately equal to the power consumed in receive mode due to increased communication with a base station therefore power consumption is a significant issue for these low-power devices. Shutting down a sensor may optimise power use compared to leaving it in idle mode when it is not transmitting or receiving. Unfortunately, once a sensor is turned off, it cannot receive any messages from its neighbour sensors (because it is effectively disconnected from the network). Further, continually turning the transceiver on and off also has an energy overhead. It might be more efficient for a sensor to be able to adjust its sampling rate and communications frequency to save power.

The 802.15.4 standard handles security at the MAC layer (see figure 3). This in itself is not necessarily a problem, however it must be enabled and is disabled by default. Figure 4 shows that two bytes are reserved for a CRC which is computing on the data bytes. This suggests that the datagrams are safe from tampering because the CRC would not match when recomputed at the endpoint. This is not necessarily so. Sastry and Wagner (2004) point out that 802.15.4 networks can suffer from security breaches in three areas, viz: IV (nonce) management, key management and integrity protection. Considering just the last area for brevity's sake, Sastry and Wagner claim that CRCs are insufficient for integrity protection and favour strong encryption instead (which is available on 802.15.4 devices). The main issue, according to Sastry and Wagner (2004, p39) is that all "*...of the attacks center on the fact that in the course of modifying the ciphertext, the adversary can construct appropriate modifications to the CRC so that the receiver accepts the packet. Researchers have discovered unauthenticated encryption vulnerabilities in...802.11...that compromise not only integrity but also confidentiality.*". This was still a problem five years later as noted by Aggélou (2009).

1 byte	2 bytes	1 byte	0-10 bytes	0-10 bytes	variable	2 bytes
Len.	Flags	Seq. #	Dest. Address	Source Address	Data	CRC

Figure 4: An IEEE 802.15.4 Datagram (Adapted from Sastry and Wagner, 2002).

Clearly this is an issue for operating in a battlefield environment. If the integrity of the datagrams can be compromised, then it might be possible for an opponent to provide false data that is accepted by the network, the agents and ultimately, an on-ground commander as legitimate intelligence. A simple example of the classic man-in-the-middle attack would be a subverted video camera sensor which transmits the image of a wall of a building instead of and image of an opponent crouching beside the wall. Wireless sensor networks can be coupled to multi-agent systems, thus providing the agents with environmental data on which to base decisions; however, there are some security problems to be solved in terms of power consumption of the network nodes (availability) and the integrity and potentially confidentiality of the data sent across the network.

DISCUSSION

Potok et al., (2003, p13) after Abadi (1999) state that it is practically impossible to construct a truly secure information system. Communications are secure if transmitted messages can be neither affected nor understood by an adversary, likewise, information operations are secure if information cannot be damaged, destroyed, or acquired by an adversary. They go on to define software challenges for a future combat system including (but not limited to) network security and accessibility; fault tolerance; and information analysis and summary of large data streams from the network.

Further, Shostack and Stewart (2008) claim that that most software is insecure. This could be because, as Wysopal et al. (2007) have observed, security requirements are often omitted from requirements specifications altogether. This has been noted as being particularly problematic in other safety-critical domains such as automotive control software-recall that figure 1 contained a land-based vehicle (Koscher et al., 2010).

In terms of the problem domain (military operations), wireless sensors of various types can be distributed on-ground before a battle, whilst being connected to autonomous software agents in a multi-agent system to give an on-field tactical advantage, provided that the communications between the sensors cannot be subverted. A public key infrastructure is an obvious solution to the integrity problem, however issues of secure storage for the private key and over-the-air transmission of either public or private keys will still prove problematic. The issue of key management is perhaps further complicated by the ever-decreasing cost of the hardware required to conduct a brute-force attack. For example, a multi-TeraFLOP GPGPU cluster can be purchased for as little as AUD$10,000.

Another area of concern is whether the agents themselves can be subverted. As noted above, whilst truly secure software is almost impossible to create, it may be that security-oriented software development methods that place security requirements at the forefront of all stages of the development lifecycle will reduce or eliminate vulnerabilities in this area.

CONCLUSIONS AND FURTHER WORK

This study sought to explore how multi-agent systems coupled with low-power wireless sensor networks could provide a tactical advantage for a modern army operating in the information age. The complex nature of modern warfare was unveiled and reasons why existing command structures would prove ineffective were put forward.

Specifically, this study examined security issues in wireless sensor networks. It was suggested that the benefits of such systems, when connected to multi-agent systems outweighed the costs, provided that the sensor network could not be compromised. Some solutions were proposed for the wireless sensors (strong cryptography) and the software agents (development methods that reduce vulnerabilities).

The next step in this research programme is to simulate a multi-agent based sensor network. The simulation could then be attacked in the manner described in the previous section. The results of the simulation and attack could then be used to field-test a physical sensor system and attempt to subvert real wireless nodes.

REFERENCES

ADF. (2003). Australian Army, Land Warfare Doctrine, LWD 0-0 Command, Leadership and Management, Canberra: Commonwealth of Australia.

Aggélou, G. (2009). Wireless Mesh Networks. New York, NY: McGraw-Hill.

Akyildiz, I.F. and Vuran, M. C. (2010). Wireless Sensor Networks. Chichester: John Wiley.

Alberts, D.S. and Hayes, R.E. (2003). Power to the Edge. Washington, DC: CCRP Publication Series.

Beautement, P., Allsopp, D., Greaves, M., Goldsmith, S., Spires, S., Thompson, S.G. and Janicke, H. (2005). Autonomous Agents and Multi-agent Systems (AAMAS) for the Military ─ Issues and Challenges. Proc. DAMAS 2005, S.G. Thompson and R. Ghanea-Hercock (Eds.): pp. 1-13.

Bishop, M. (2005). Introduction to Computer Security. Boston, MA: Addison Wesley.

IEEE (2007). IEEE Standard for Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. New York: IEEE Computer Society.

Koscher, K., Czeskis, A., Roesner, F., Patel, S., Kohno, T., Checkoway, S., McCoy, D., Kantor, B., Anderson, D., Shacham, H. and Savage, S. (2010). Experimental Security Analysis of a Modern Automobile. Proc. IEEE Symposium on Security and Privacy, Oakland, CA, May 16–19, 2010.

Orr, G.E. (1983). Combat Operations C3I Fundamentals and Interactions. Research Report No. AU-ARI-82-5. Maxwell Air Force Base, AL: Air University Press.

Pohl, J., Porczak, M., Pohl, K.J., Leighton, R., Assal, H., Davis, A., Vempati, L. and Wood, A. (2001). IMMACCS: A Multi-Agent Decision-Support System. Technical Report CADRU-14-01. CAD Research Center, Cal Poly, San Luis Obispo, CA.

Potok, T., Phillips, L., Pollock, R., Loebl, A. and Sheldon, F. (2003). Suitability of Agent-Based Systems for Command and Control in Fault-tolerant, Safety-Critical Responsive Decision Networks. Proc. 16th Int'l Conf. On Parallel and Distributed Computing Systems, Aug. 13-15,2003 Reno NV.

RFC 2828 (2000). Internet Security Glossary. Internet Engineering Task Force. Retrieved September 22, 2009, from http://www.ietf.org/rfc/rfc2828.txt

Sastry, N. and Wagner, D. (2004). Security Considerations for IEEE 802.15.4 Networks. ACM Workshop on Wireless Security (WISE 04), pp. 32–42.

Shostack, A. and Stewart, A. (2008). The New School of Information Security. Upper Saddle River, NJ: Addison Wesley.

Tynan, R., O'Hare,G., Marsh, D. and O'Kane, D. (2005). Multi-agent System Architectures for Wireless Sensor Networks. Lecture Notes in Computer Science, 2005, Volume 3516/2005, pp37-58.

Wooldridge, M. (2002). An Introduction to Multi-Agent Systems. Chichester: John Wiley.

Wysopal, C., Nelson, L., Dai Zovi, D. and Dustin, E. (2007). The Art of Software Security Testing. Upper Saddle River, NJ: Addison Wesley.