Security Challenges for Swarm Robotics

Fiona Higgins, Allan Tomlinson and Keith M.Martin

Technical Report
RHUL-MA-2008-19
October 2008

Department of Mathematics
Royal Holloway, University of London
Egham, Surrey TW20 0EX, England
http://www.rhul.ac.uk/mathematics/techreports

Abstract

Swarm robotics is a relatively new technology that is being explored for its potential use in a variety of different applications and environments. Previous emerging technologies have often overlooked security until later developmental stages, when it has had to be undesirably (and sometimes expensively) retrofitted. We identify a number of security challenges for swarm robotics and argue that now is the right time to address these issues and seek solutions. We also identify several idiosyncrasies of swarm robotics that present some unique security challenges. In particular, swarms of robots potentially employ different types of communication channels; have special concepts of identity; and exhibit adaptive emergent behaviour which could be modified by an intruder. Addressing these issues now will prevent undesirable consequences for many applications of this type of technology.

1 Introduction

Swarm robotics is a relatively young area of research, which is growing rapidly and comprehensive reviews of the state-of-the-art may be found in [1, 2, 3]. As with many technologies, there is no formal definition for swarm robotics that engenders universal agreement, however there are some characteristics that have been generally accepted. These include robot autonomy; decentralised control; large numbers of member robots; collective emergent behaviour and local sensing and communication capabilities. From our security perspective it is reasonable to consider swarm robotics as a special type of computer network with the aforementioned characteristics.

It has often been the case that the security of a new technology is an afterthought rather than an upfront design objective, leading to many security issues. This was the case with, for example, mobile phone technology. The first generation of mobile phones were analogue, and easy to clone since they broadcast their identity clearly over the airwaves. It was also easy to eavesdrop on them by simply tuning a radio receiver to pick up conversations. Subsequently the underlying technology had to be expensively modified in order to address these threats. In the case of swarm robotics research, the particular security requirements of swarm robotic networks do not appear to have been investigated in any detail so far. Thus we believe that this is an opportune time to consider these issues, before any wide-scale deployment. Deferring security research until later in the technology's evolution could, depending on the application, be a risky strategy and lead to undesirable consequences.

As far as we are aware, this is the first attempt to categorise security challenges to swarm robotics. Very little prior work appears to have been done. A notable exception to this is the work of Winfield and Nembrini [4] who identify several threats to a swarm of robots, which they classify as hazards. We hope that our identification of the main security challenges will result in the development of robot swarm technology that is reliable and safe to deploy even in potentially hostile environments.

In Section 2 we briefly review technologies that are similar to swarm robotics, highlighting the key differences. In Section 3 we discuss security, commencing with a short high level overview of security, providing examples of swarm robotic deployment where security is required, and then cataloguing aspects of the swarm robotic environment which present challenges to security. Finally in Section 4 we draw some conclusions.

2 Related Technologies

Before considering the security of swarm robotic networks it will be useful to review how similar technologies, some of which have been subjected to a degree of security analysis, relate to robotic swarms. This will allow us to identify the unique features of robotic swarms that may benefit from closer scrutiny in terms of security.

2.1 Multi-Robot Systems

Swarm robotics differs from more traditional multi-robot systems in that their command and control structures are not hierarchical or centralised, but are fully distributed, self-organised and inspired by the collective behaviour of social insect colonies and other animal societies [5]. Self-organisation means that sometimes the collective behaviour, even if unpredictable, may well result in solutions to problems that are superior to ones that could have been devised in advance. The parallel drawn with social societies in the animal world extends to communication interactions between the robots can be indirect as well as direct. *Fault-tolerance*, which is related to security, has already been extensively researched within the context of multi-robot systems with hierarchical command and control, notably in the work of Parkers ALLIANCE control architecture [6].

2.2 Mobile Sensor Networks

Sensor networks consist of collections of devices (or *nodes*) with sensors that typically communicate over a wireless network. A *mobile* sensor network is a sensor network where the nodes are either placed on objects which move [7] or where the nodes may move themselves [8]. In the latter case they are sometimes known as *robotic sensor networks*.[1] Hybrid systems also exist [9], where mobile robots work in conjunction with static sensors. Although mobile sensor networks exhibit many similarities to swarm robotic networks, there are distinct differences. For example, robotic swarms may utilise a wider range of communications technologies, which extend to indirect communication such as stigmergy. Additionally, individual identity may be more important in a sensor network if it is important to determine exactly where some sensed data originated. Furthermore, and importantly, a sensor network is not designed to have the collective emergent behaviour of a robotic swarm.

2.3 MANETs

Mobile Ad-hoc Networks *(*MANETs*)* consist of wireless mobile nodes that relay each others traffic, with the nodes spontaneously forming the wireless network themselves. The special properties of MANETs, such as the lack of infrastructure, absence of trusted third parties, as well as possible resource constraints, make implementing security a very challenging task. MANETs can consists of many types of mobile devices and there is considerable existing work on their security [10, 11]. Although MANETs do not exhibit the emergent behaviour of swarms, some MANET security techniques could have relevance to swarm robotics depending on the communication method used by the swarm.

2.4 Software Agents

There is no universally agreed definition of a software agent, but we take one proposed by Wooldridge [12]: An *agent* is a computer system that is situated in some environment, and that is capable of autonomous action in this environment in order to meet its design objectives. A *multi-agent system* (MAS) [13, 12] is a system composed of multiple autonomous agents, where each agent cannot solve a problem unaided; there is no global system control; data is decentralised; and computation is asynchronous. A *mobile* agent is a particular class of agent with the ability during execution to migrate from

[1] http://rsn.cs.rpi.edu

one host to another where it can resume its execution [13]. Thus *mobile multi-agent systems* may share many features with swarm robotic systems, but in a virtual world.

Corresponding to the active interest in mobile software agents and their rapid adoption, there has been much interest in their security [13]. However this does not always translate easily to robotic swarms because of the particular characteristics of robotic swarms which differentiate them, such as their physical nature, diverse communication mechanisms and control structure.

3 Security of Swarm Robotics

3.1 Basic Security Terminology

Security in any environment, including swarm robotics, is fundamentally about the provision of core *security services*, some of the most important of which are as follows. The service *confidentiality* is about keeping data secret. An *integrity* service prevents prevents data from being altered in an unauthorised or unintended way. *Entity authentication* (sometimes called *identification*) is the process whereby one entity is assured of the identity of another entity. *Data origin authentication* is the assurance that data came from its reputed source. Finally, *availability* is the property of being accessible and useable upon demand by an authorised entity. The term *denial of service* is often used in reference to loss of availability.

A *threat* is a potential violation of the provision of a desired security service. Threats that are not mitigated leave *vulnerabilities* in the system that may be exploited. Such exploitative actions are often called *attacks* and those that initiate their execution are *attackers*. An example of a threat could be that an unauthorized person might see top secret information; a vulnerability could be that trust is misplaced in a courier; an attack could be that someone steals the data and publishes it in the media. Information may also be *accidentally* lost. The impact of a document theft or loss will depend on the content of the document. The process of *risk assessment* takes this into consideration along with the probability of the threat being realised.

In any system, the provision of security is a holistic process. This requires careful management processes that oversee the use of specific security technologies that can be applied to devices and networks. These include *firewalls*, *access control mechanisms* and *network security protocols*. At the heart of most security technologies is the deployment of specific *cryptographic primitives*, which are mathematical tools that can be applied to data to provide the core security services. These normally rely on the careful protection and maintenance of *cryptographic keys*, which are critical data items that must be stored securely.

3.2 Scenarios Demonstrating the Need for Security in Swarm Robotic Applications

Military:

Swarm robotic networks may be used in military applications[2] where the need for security is perhaps self evident. However, circumstances may arise in non-military applications where the system may be vulnerable to particular threats.

Environment: Robot swarms may be used to maintain the environment by detecting environmental pollutants such as oil spillages and cleaning them up [14]. Although exchanged data may not be sensitive in such applications, data integrity and availability are of high importance. Furthermore, the swarm may accidentally encounter a 'rogue' device perhaps from a swarm with a different goal. Unless the 'intruder' is detected the emergent behaviour of the swarm may be affected. In the military scenario, of course, the rogue may indeed be malicious.

Disaster Relief: Robot swarms could be deployed during disaster relief operations in environments where traditional communication networks have broken down.[3] Availability then becomes a primary security requirement, as well as authentication/identification in the case where multiple swarms are in joint operation.

Healthcare: The European I-Ward project uses swarms of robots to provide assistance to healthcare workers.[4] Entity authentication is likely to be the most important security requirement in such scenarios. Moreover, authentication and confidentiality may be important when robots are deployed in multiple applications, to prevent data from previous application sessions being disclosed.

Commercial Applications: As the technology develops robotic swarms may find commercial use. In any commercial application the motivation to steal data and services will lead to threats to the service. If commercial applications are to be successfully deployed then some consideration should be given beforehand to the potential security risks.

[2] http://www.challenge.mod.uk/

[3] http://www.shu.ac.uk/mmvl/research/guardians/

[4] http://www.iward.eu/cms/index.php

3.3 Challenges to Security

It is appropriate therefore to consider the challenges to providing security in swarm robotic networks. It is clear that some security issues are similar to other related technologies and that some solutions from these technologies may apply to swarm robotics. However, not all of these shared problems have been fully solved. Furthermore, the swarm robotic environment introduces particular security challenges that do not exist in other technologies.

Resource Constraints: The smaller a device is, the greater the challenge to providing security due to resource constraints (storage, communication bandwidth, computational restrictions and most importantly energy). Attacks on the provision of resources can lead to the device becoming inoperable, permanently so if the resource is not renewable. This leads to a loss of availability. Resource constraints also restrict the types of existing security technologies that can be deployed.

Physical Capture and Tampering: Physical capture of a robot leads to loss of availability. Worse, capture of security credentials could harm other members of the swarm. If a robot is tampered with and reintroduced into the swarm, an attacker might influence the swarm behaviour. This attack would be unique to swarm robotic technology.

Control: Systems employing swarm intelligence do not have a hierarchical structure with points of control. The individuals within these systems take decisions autonomously, based on local sensing and communications. With such systems it is evident that there could be many risks if they went out-of-control, including many security violations such as loss of confidentiality or availability. Control presents an interesting challenge to security within swarm robotics.

Communication: Swarm robots can interact either explicitly, or implicitly [15]. *Explicit* communication can be achieved via broadcast or directed messages. Radio-frequency (RF) and infra-red (IR) technologies have been widely for explicit communications within swarms. Other technologies include coloured LED display, body-language or sign-language, colour patterns on a robots body, coil induction, haptics, audible sounding, combination of LED display and audio signalling and acoustic signalling in an underwater environment. *Implicit* communication includes interaction via sensing other robots and their behaviours, and interaction via the environment, which acts as a sort of shared memory and is known as *stigmergy* [16, 5, 17].

From a security perspective, any open implicit or explicit communication method can be jammed, intercepted or otherwise disturbed relatively easily by an attacker. The security of RF and IR has been well researched but the security of the remaining more exotic interaction methods needs to be thoroughly investigated and presents a fascinating security challenge.

Swarm Mobility: Security is difficult to provide in any mobile environment, however the mobility of robot swarms is quite unusual and has some interesting characteristics that might make some security services easier to implement than for related technologies. One example is entity authentication, discussed below, which could be provided through visual sensing and physical data exchange. However any constraint on the movement of swarm members, for example to remain in the bounds of the swarm could present additional security issues.

Identity and Authentication: As discussed in section 3.2, it may be very important for a swarm robot to determine if it is interacting with a legitimate entity or not. Data origin and entity authentication require some notion of identity, which is a particular problem where individual identity within a swarm is undesirable [18]. Other work has used *group identity* [19]; or individual identity which is broadcast regularly [20]. If identity can be assumed or changed then attacks can be launched on entity authentication, confidentiality, integrity and availability. The notion of identity within a robotic swarm thus presents an interesting challenge from a security standpoint.

Key Management: Security services deployed in a robot swarm inevitably require the need to manage cryptographic keys [21]. These keys define which pairs (or groups) of robots can apply security services. As robots join and leave a swarm, it may be necessary to alter this keying material. Thus the dynamic and interactive nature of a swarm presents sophisticated key management challenges.

Intrusion Detection: When a foreign entity joins a network it is sometimes called *intrusion.* One means of detecting intrusion is based on network *Intrusion Detection Systems.* The autonomous nature of robots and collective emergent nature of the behaviour of the swarm will make any anomalous behaviour difficult to detect. If undetected, one or more foreign robots could infiltrate the swarm, either maliciously or accidentally, and ultimately affect the desired emergent behaviour.

Once an intruder is detected, an appropriate response will need to be formulated according to an *Intrusion Protection System.* Depending on the application the response could be to simply ignore the rogue device, or to monitor its behaviour, or to find a way to either disable it or remove it from the system. Intrusion detection and protection looks to be particularly challenging in a swarm of robots, and will need a specifically tailored approach.

Managing Learning: Robots can learn and react to environmental changes by means of adaption. A malicious entity might present changes in the environment which will cause a robot to adapt in an undesired way.

For example, if anomaly detection is used to detect intrusion based on learning typical behaviour, then a malicious entity could change the pattern of typical behaviour in order to gain entry to the network.

4 Conclusions

The development of swarm robotic technology has reached a point where many new applications are emerging. Therefore, we believe that this is an opportune moment to take a closer look at the security of swarm robotic systems - before widespread deployment. Although the security of related technology has been investigated, robotic swarms are different due to factors such as their autonomy, distributed control, and emergent behaviour. Bearing this in mind, we have identified a number of significant challenges to robotic swarm security, some of which are unique to this technology. For example, the challenges presented by more esoteric communication methods than straightforward RF or IR, the question of identity, and the potential for modification of emergent behaviour if a malicious entity manages to infiltrate the swarm. It is likely that some of these challenges will require new security techniques to be developed, and we will aim to investigate these in our future work.

References

[1] L. Bayindir and E. ahin, "A review of studies in swarm robotics," *Turkish Journal of Electrical Engineering*, vol. 15, pp. 115–147, 2007. [Online]. Available: http://journals.tubitak.gov.tr/elektrik/issues/elk-07-15-2/elk-15-2-2-0705-13.pdf

[2] E. ahin and W. Spears, Eds., *Swarm Robotics Workshop: State-of-the-art Survey*, ser. Lecture Notes in Computer Science. Berlin Heidelberg: Springer-Verlag, 2005, vol. 3342.

[3] E. ahin, W. Spears, and A. Winfield, Eds., *Swarm Robotics. Revised Selected Papers from the Second International Workshop, SAB 2006. Rome. Italy.* Springer Berlin/Heidelberg, 2007, vol. 4433/2007.

[4] A. Winfield and J. Nembrini, "Safety in numbers: fault-tolerance in robot swarms," *International Journal of Modelling, Identification and Control*, vol. 1, pp. 30–37, 2006. [Online]. Available: http://www.ias.uwe.ac.uk/ a-winfie/WinNemIJMIC06.pdf

[5] E. Bonabeau, M. Dorigo, and G. Theraulaz., *Swarm Intelligence: from natural to artificial systems (Santa Fe Institute Studies in the Sciences of Complexity).* Oxford University Press, 1999.

[6] L. E. Parker, “ALLIANCE: An architecture for fault tolerant multi-robot cooperation,” *IEEE Transactions on Robotics and Automation*, vol. 14, no. 2, pp. 220–240, April 1998. [Online]. Available: http://www.cs.utk.edu/ parker/publications/TRA.pdf

[7] T. Wark, C. Crossman, W. Hu, Y. Guo, P. Valencia, P. Sikka, P. Corke, C. Lee, J. Henshall, K. Prayaga, J. O’Grady, M. Reed, and A. Fisher, “The design and evaluation of a mobile sensor/actuator network for autonomous animal control,” in *Proceedings of the 6th international conference on Information processing in sensor networks.* ACM, 2007, pp. 206–215.

[8] K. Dantu, M. Rahimi, H. Shah, S. Babel, A. Dhariwal, and G. Sukhatme, “Robomote: Enabling mobility in sensor networks,” in *Proceedings of Fourth International Symposium on Information Processing in Sensor Networks*, 2005, pp. 404–409.

[9] J. Reich and E. Sklar, “Toward automatic reconfiguration of robot-sensor networks for urban search and rescue.” in *Proceedings of the 1st International Workshop on Agent Technology for Disaster Management*, 2006. [Online]. Available: http://users.ecs.soton.ac.uk/sdr/atdm/ws34atdm.pdf

[10] E. Hansson, A. Bengtsson, and A. Vidstrm, “Security solutions for mobile ad hoc networks.” Swedish MOD, FOI Defence Research Agency Command and Control Systems P.O. Fox 1165 SE-581 11 Linkping Tel 013-378086, Technical Report FOI-R–1694–SE ISSN 1650-1942, August 2005. [Online]. Available: http://www2.foi.se/rapp/foir1694.pdf

[11] L. Buttyn and J.-P. Hubaux, *Security and Cooperation in Wireless Networks: thwarting malicious and selfish behaviour in the age of ubiquitous computing.* Cambridge University Press, 2007. [Online]. Available: http://secowinet.epfl.ch/fulltext/SeCoWiNetV1.5.1.pdf

[12] M. Wooldridge, *An Introduction to MultiAgent Systems.* Wiley, 2002.

[13] N. Borselius, “Multi-agent system security for mobile communication,” Ph.D. dissertation, Department of Mathematics, Royal Holloway, University of London., 2003.

[14] D. Fritsch, K. Wegener, and R. Schraft., “Control of a robotic swarm for the elimination of marine oil pollutions,” in *IEEE Swarm Intelligence Symposium (SIS 2007)*, 2007, pp. 29–36.

[15] L. Parker, “Current state of the art in distributed autonomous mobile robotics,” *Distributed Autonomous Robotic Systems*, vol. 4, pp. 3–12, 2000. [Online]. Available: http://www.cs.utk.edu/ parker/publications/DARS$_2$000$_o$*verview.pdf*

[16] P.-P. Grass, “La reconstruction du nid et les coordinations inter-individuelles chez bellicositermes natalensis et cubitermes sp. la thorie de la stigmergie: Essai d’interprtation du comportement des termites constructeurs.” *Insec. Soc.*, vol. 6, pp. 41–80, 1959.

[17] T. White, “Expert assessment of stigmergy: A report for the department of national defence,” School of Computer Science, Carleton University, Ottawa, Ontario, Canada, Tech. Rep., 2005. [Online]. Available: http://www.scs.carleton.ca/ arpwhite/stigmergy-report.pdf

[18] P. Flocchini, G. Prencipe, N. Santoro, and P. Widmayer, “Gathering of asynchronous robots with limited visibility.” *Theoretical Computer Science*, vol. 337, no. 1-3, pp. 147–168, 2005. [Online]. Available: http://dx.doi.org/10.1016/j.tcs.2005.01.001

[19] R. A. Russell, “Visual recognition of conspecifics by swarm robots,” in *2004 Australasian Conference on Robotics & Automation*, 2004. [Online]. Available: http://www.araa.asn.au/acra/acra2004/papers/russell.pdf

[20] J. Fredslund and M. Matari, “A general algorithm for robot formations using local sensing and minimal communication,” *IEEE Transactions on Robotics and Automation*, vol. 18, pp. 837–846, 2002.

[21] S. Dolev, L. Lahiani, and M. Yung, “Secret swarm unit. reactive k-secret sharing,” in *Proc. of the 8th International Conference on Cryptology in India.* Springer Verlag, 2007, pp. 123–137.