ANTI-SWARMING FROM THE SWARM ROBOTICS PERSPECTIVE

Jan Carlo Barca

Monash Swarm Robotics Laboratory
Faculty of Information Technology, Monash University, VIC, Australia
Email: jan.barca@monash.edu

Abstract - This study represents the first known attempt to formulate a template for a complete anti-swarming strategy that can be employed against adversary robotic swarms. This research is important as swarm robotics technology will be widely available in the near future and it would be naïve to assume that this highly capable technology exclusively will be employed in “constructive contexts”. The proposed strategy was devised by means of the Grounded Theory Method and building on state-of-the-art methods, which have been successfully employed against destructive natural swarms. A series of future directions of research and activities, which ensure that required safeguards can be implemented are also proposed.

INTRODUCTION

Natural swarms consist of large groups of individuals which interact locally to achieve shared goals. The term refers to all forms of collective behaviors even though it frequently is associated with coordinated movement in space [1]. Studies on natural swarms have recently given rise to Swarm Intelligence (SI) where groups of simple autonomous individuals interact in virtual space to reveal solutions to problems that are difficult to resolve with traditional engineering methods. The original Ant Colony Optimization [2] and Particle Swarm Optimization [1] algorithms represent two of the earliest attempts to formulate SI technology inspired by the path seeking behaviors observed in ants and the flocking behavior of birds. A broad range of advanced SI techniques have been formulated since then, including the Firefly [3, 4], Wolf Pack [5] and Locust Swarm [6] algorithms. Strategies that enable multiple swarms to coordinate their activities [7] have also been proposed. The reader can refer to [8, 9] for comprehensive overviews of recent advancements in the field.

Over the last decade Swarm Robotics (SR) has emerged from the application of SI concepts to multi-robot systems. SR focuses on “physical embodiment and realistic interactions among the individuals themselves and also between the individuals and the environment”, while the use of low cost expendable individuals is encouraged [10]. SR systems are scalable, flexible and robust towards system failure [11], which makes them attractive in a broad range of high impact application areas including exploration, maintenance and search & rescue. SR research is therefore expected to progress rapidly in the coming years [12].
A variety of machines have already been employed in SR systems including unmanned ground vehicles (UGVs), unmanned aerial vehicles (UAVs) and climbing robots [13, 14, 15]. Traditionally SR systems have been homogenous, however recent years have seen a shift towards heterogeneity as it is expected that this will enable groups of robots to tackle a broader range of tasks [16].

One of the side effects of these advances is that SR technology, which largely is being developed by universities and the commercial sector, will be accessible to a broad range of state and non-state actors [17, 18]. To uncover how this game changing technology can be suppressed if it ends up “in the wrong hands” is therefore vital to ensure global security. However, to this day methods that can halt adversary SR systems are largely unexplored. The presented research attempts to address this issue by formulating an anti-swarming strategy and associated tactics, which prevent and suppress adversary robotic swarms.

PRELIMINARIES

When large natural swarms perform tasks that have significant negative impact they frequently progress through five phases referred to as: i) recession, ii) outbreak, iii) upsurge, iv) plague, and v) plague decline [19]. As control mechanisms employed by SR systems have been formulated by seeking inspiration from natural swarms it can be expected that similar high level phases will be observed in the robotic equivalents even if some distinct differences, which will be discussed below, do exist.

The term recession refers to periods when no swarms are present [19]. The aim of an anti-swarming strategy should be to maintain this state, or to revert back to this state, if undesirable swarm activity unfolds.

Outbreaks occur when the number and density of individuals increase in a manner that enables them to coordinate their activities and operate as swarms [19, 20]. Outbreaks can be predicted via observations of higher than normal numbers of solitary individuals and the availability of resources that facilitate swarming [20, 21, 22, 23]. The population increase can occur across regions initially, where separate populations eventually merge into dense cohesive swarms.

A transiens process where solitary individuals begin to behave less as individuals and more as a unified entity unfolds throughout the outbreak. Behavior change occurs rapidly and plays a dominant role in the formation of swarms [20]. In desert locusts numbers must rise to $10^9$ to give rise to high density swarms that move in unison [19]. This number is significantly lower in SR systems as it has been demonstrated that only five robots are required for self-organized movement in groups of UGVs [24].

At the end of transiens the individuals gregarize into a collective state that can cause extensive economic damage [25, 26, 27, 28, 29]. Higher densities and frequent interaction between individuals affect the rate of gregarization [19]. Unless checked, the process will proceed until the swarm migrates to other areas or the number of individuals and densities decrease below a gregarization threshold [20].
Natural swarms gregarize via distributed processes. This may not always be the case in SR systems as it is difficult to predict behaviors that emerge solely from local interactions. Collective phenomena in SR systems designed for real world tasks will therefore more likely be a result of careful planning or indirect control by purposive actors.

Upsurges can be recognized via widespread and significant increase in numbers, which trigger simultaneous outbreaks and enable swarms to occupy expanding areas in complimentary or neighboring regions [19]. During upsurges several swarms may operate simultaneously where the first swarm can be termed the prime swarm and the remaining swarms can be referred to as “extra swarms” or “after-swarms” [30]. Upsurges can only occur when multiplication is allowed to progress and one should therefore pay extra attention when sufficient resources to support large population growths are available [19].

Plagues occur when swarms are widespread and they affect extensive areas [21, 31, 32, 33]. Numbers must rise to $10^{11}$ for desert locust plagues to arise. The number of individuals in SR plagues will most likely be significantly lower due to cost constraints. A single locust swarm can cover regions between 0.1 and 20 km$^2$ [19, 34] and a medium size infected region can cover 2500 to 100 000 km$^2$. However, infected areas as large as 200 000 km$^2$ have been observed [35, 36]. To achieve peak plague levels swarms must spread. The best approach to prevent plagues is therefore to check populations early on [19].

Plagues decline when the number of individuals and densities are reduced to pre-plague levels. When plagues “flare up” one should therefore significantly reduce population numbers and densities.

**Task Execution**

Intelligent groups such as large scale SR systems can be expected to carry out tasks as a part of a three stage process (Figure 1) when they are likely to face countermeasures. These stages are referred to as: i) convergence, ii) task execution, and iii) dispersal [37, 38, 39, 40]. Convergence involves massing sufficient numbers of individuals to carry out tasks according to plan. This stage is required as intelligent swarms frequently are distributed throughout environments to maximize their situational awareness and reduce their vulnerability to concentrated countermeasures. Once sufficient resources have been assembled the swarm will execute designated tasks and quickly re-disperse. Swarms can also disperse as a response to emergencies or be forced to scatter. If the swarm disperses prematurely the three stage process is likely to repeat until all tasks have been completed, or the swarm is pushed back to a pre-plague level. If several swarms exist, the stages may occur at different rates across swarms [7].
Fig. 1 Intelligent swarms that may face damaging countermeasures can be expected to perform tasks as a part of a three stage process which involves convergence, task execution and dispersal. Unless the swarm is checked the process will repeat until all tasks are completed. Modified after [37].

ANTI-SWARMING

Strategies that can be employed against adversary robotic swarms have not been well studied to date due to the relatively few large scale SR systems in existence. However, the Grounded Theory Method [41] and parallels drawn between natural swarms and SR systems can be exploited to provide a sound theoretical foundation for methods that can be employed against adversary robotic swarms. This research has therefore sought inspiration from well-studied methods that have been successfully employed against desert locusts (which are regarded as one of the world’s most destructive natural swarms) to formulate the proposed anti-swarming strategy [19, 25, 26, 42, 43]. An overview of the strategy is provided in Figure 2, while in-depth discussions of associated tactics are provided below.

Fig. 2 Proposed anti-swarming strategy. Modified after [19].

Plague Prevention

Plague Prevention aims to control populations before they reach numbers and densities required to form swarms. Major campaigns are required if initial halting fails and Plague
Prevention should therefore be in place to reduce the risk of facing full scale "plagues" [19, 26]. Plague Prevention consists of: i) Outbreak Prevention, ii) Upsurge Prevention, iii) Upsurge Suppression, and iv) Upsurge Elimination.

Outbreak Prevention

Successful Outbreak Prevention requires:
- Identification of pre-plague population dynamics
- A plague prevention scheme
- Pre-planning
- Monitoring
- Sufficient funds and infrastructure

The dynamics of pre-plague populations should be identified as this will offer insights into when anti-swarming control measures are worth the expense and effort [43]. These studies should be performed by analyzing the behaviors of state-of-the-art small scale SR and distributed multi-robot systems. Both homogenous and heterogeneous systems with varying composition should be studied to determine how different robots affect the system performance. Thresholds required for self-organization should also be determined.

In addition to studying scholarly literature first hand insights obtained via red teemed simulations and real world experiments such as the ones reported in [44, 45] are also encouraged, as this will assist in broadening perspectives and increasing understanding of technological requirements [37]. Simulators such as Repast Symphony [46] and Mason [47] can be utilized to evaluate alternative methods. The evaluation process can be made efficient via crowd sourcing where external researchers and students conduct experiments via game play and report their findings. Insights gained from these studies should be stored in a knowledge management system and be utilized in the process of designing novel prevention and suppression schemes. The information should also be used for education and training. To be effective the lessons learned must include both successes and failures [37].

Plague prevention and suppression schemes can be formulated by drawing on insights from the knowledge management system and seeking inspiration from anti-swarming strategies formulated for natural swarms. To seek inspiration from existing anti-swarming strategies is important in SR contexts as few large scale SR systems have been tested in real world experiments to date.

Pre-planning begins well ahead of the incident and involves strategic planning, assigning responsibilities, organization, training, preparations, operational procedures and specifying rules of engagement [37]. This planning should be based on the prevention and suppression schemes formulated earlier and should emphasize on early prevention and crisis-decision making.

Successful outbreak prevention must be aided by appropriate monitoring as early detection of population sources, estimates of population sizes and their movements are invaluable in the process of inhibiting swarm growth [20, 38, 43, 48]. However, adequate monitoring is challenging when the areas to be surveyed are large. Efficient monitoring tools are therefore
required to detect populations at an early stage in these instances. Remote sensing technology capable of spotting planes or ships that can transport and support SR systems will aid in addressing this problem [26]. Large scale monitoring can also be supported by means of predictive maps, which indicate where swarms are likely to appear, along with decision support mechanisms that balance the costs and risks associated with dispatching anti-swarming teams [26].

An alternative is to focus monitoring efforts on high value sites. In these contexts, advanced radar systems can be employed [49]. Another alternative is to detect SR systems via microphones [49]. However, it is difficult to detect small robots in windy conditions and such systems will not be capable of detecting incoming fixed-wing UAVs that dive silently towards their target location while unpowered. There is also the possibility of detecting small robots via the radio signals some of them produce, but again this will not be possible if the robots follow preprogrammed routes without making use of radio uplinks or downlinks [49]. A carefully designed repertoire of sensors must therefore be employed to maximize the chances of successful and timely detection.

To formulate, implement and improve plague prevention and suppression schemes funds and infrastructure, which makes it possible to permanently employ adequately equipped anti-swarming teams with permanent mandate to find and suppress swarms must be available [19]. Prevention will be compromised if adequate financing cease as it has been shown that a lack of resources, inefficient logistics and organization has led to major invasions of natural swarms [50, 51]. Finances that can be used to train reserve teams must also be available well ahead of an outbreak as core teams quickly will become incapable of countering swarms by themselves during large scale outbreaks.

**Upsurge Prevention**

Once an outbreak is underway the focus should be on information gathering, trapping and confinement to prevent an increase in numbers and simultaneous outbreaks in expanding areas. The information gathering process should be initiated without delay and should investigate: i) who sent the swarm, ii) the composition of the swarm, iii) the number of individuals and the spatial distribution, iv) what resources the swarm has access to, v) how fast the swarm can move, vi) what the swarm is capable of doing, vii) where and when the swarm is likely to converge, viii) what are other possible objectives, ix) what is the worst case scenario, and x) where the swarm will disperse [19, 37].

Escape proof traps can be employed to collect information about the composition of the swarm, population numbers and distributions [43, 52]. Trapped individuals can also provide insights into when SR systems will collapse. This information can be obtained by analyzing the average failure rate of the worst components in the robots [24].

Trapping can be carried out with a single trap, multiple traps in one region or multiple traps across regions. It is difficult to accurately estimate population sizes and densities with one trap only. However, captured individuals will still provide valuable information about the robots and the composition of the swarm. One can obtain more accurate estimates of numbers and
densities when multiple traps are employed [43]. This is particularly important in situations where the formations employed by the swarm are unknown. When multiple traps are distributed across regions one can investigate the interplay between populations and thereby determine when and where swarms are likely to merge. It should also be noted that information collected at different scales can be used to improve estimates at other resolutions. Integrated analysis of trap counts from all three scales should therefore ideally be performed. However, in practice one must balance the number of traps required to obtain satisfactory accuracy and the associated cost.

The most appropriate trap design depends on the locomotory mechanisms and the size of the robots. When trapping UGVs a circular hole in the ground is likely to be sufficient, but the size of the trap should be significantly larger than the robots. A factor of $10^2$ the body size has proven sufficient against insects [43]. Robots that move across or temporarily land on surfaces can be captured by means of adhesive materials, while electrically charged netting or escape proof collecting bags may be employed to capture flying units [52]. Individuals or groups may also be immobilized by means of electromagnetic pulses. If the swarm requires access to GPS signals or a base station to operate successfully one can “lure the swarm” into communication restricted environments and take out the anchor node/s if some individuals remain outside. In situations where trap servicing is difficult or dangerous automated counting and identification mechanisms should be incorporated in the trap designs [53].

Traps can be baited when there are tight time constraints and it is acceptable to disturb the natural behavior of the swarm [30, 52]. The bait type depends on the sensors used by the robots and the sort of stimuli the robots are attracted to. E.g. if the robots are attracted to acoustic signals, then acoustic bait can be employed [53]. In crisis situations friendly units can be used as bait with the aim of trapping significant portions of the swarm between the bait and the main body of friendly units as demonstrated by Alexander the Great [38].

To confine the swarm and prevent it from spreading is important to reduce the risk of massive swarm invasions. The swarm should ideally be confined until a large number of robots run out of energy or fail due to deteriorating system components [37]. Confinement zones can be generated by preparing countermeasures along natural or manmade barriers [19]. However, it should be noted that this approach may only be applicable for relatively small swarms as large swarms will be capable of swamping barriers and defenses. In a crisis situation an alternative approach is to encircle the adversary swarm with a blue teemed SR system, which consist of larger numbers of more agile individuals with longer expected lifetime and better protective covering [38, 45, 54]. Anti-swarming swarms are currently being investigated by [45].

Upsurge Suppression

Upsurge Suppression is an extension of the previous schemes and should aim to break down SR systems without direct confrontation. To achieve this one should:

- Get backup
- Inhibit multiplication
- Disrupt the swarm’s ability to coordinate its activities
- Exhaust the swarm
• Continuously evaluate the effectiveness of countermeasures

During upsurges infected areas rapidly increase and permanent anti-swarming teams will quickly be unable to find and treat all affected areas. Reserve teams must therefore be called in without delay to prevent the swarm from spreading further [19]. It is also important to inhibit multiplication to prevent the swarm from growing. This can be done by identifying and eliminating the sources that emit robots. These sources can be naval vessels or flying vehicles, but one or more hidden stationary robots. These sources may also exist if the robots have been pre-placed in the environment.

By disrupting the swarm’s ability to coordinate its activities one target the “heart of the swarm”. Coordination can be disrupted by intercepting communication, systematically influencing quorum sensing thresholds or reducing exteroceptive sensing and communication ranges [17, 55, 56]. When intercepting communication one should exploit weaknesses in mechanisms that facilitate confidentiality, entity authentication, origin authentication and authenticity [57].

Quorum sensing thresholds can be influenced by intercepting intra-swarm communication. By decreasing these thresholds, it is possible to trick the swarm into making collective decisions prematurely, or to paralyze the swarm by significantly raising these thresholds [29, 55, 58, 59]. Quorum sensing can also be affected by introducing “controlled” individuals into the swarm as recent studies demonstrate that one can “take over” a swarm by ensuring that 10% of the individuals are controlled by an external source [60].

An alternative is to introduce noise on the intra-swarm communication channels in a manner that makes the swarm fail to distinguish between good and bad solutions [61]. If more than 30% noise is introduced the lifetime of the swarm can be reduced. This can potentially also drive the swarm to stagnation. To prevent the swarm from overcoming the problem by calculating the mean over multiple evaluations different noise distributions can be introduced in quick succession. If a swarm is hierarchical and requires interaction with a base station one can intercept communication between the base and the highest ranking individual in the swarm, and thereby hijack the swarm and potential sub-swarms [17]. This could be achieved by direct communications hacking, replacing high ranking individuals or spoofing signals to deceive the swarm into performing desirable actions. The latter is the best approach as one can increase blue teamed resources at minimal cost.

By reducing communication and sensing ranges one can affect the number of individuals that are allowed to interact, and thereby the time it takes for information to propagate through the swarm [25]. It has been proven that a neighborhood size of 10 supports strong interaction in swarms [62]. The aim should therefore be to reduce the neighborhood size significantly below this threshold to ensure that the individual elements are no longer able to coordinate and cooperate, but are instead fighting as individual uncoordinated elements. Ideally no individuals should be capable of interacting with any of its neighbors as the swarm will be capable of operating as a cohesive unit as long as some individuals are connected, albeit at a slower pace when connectivity levels are low [63]. If this approach is chosen it is also important to note that both communication and sensing ranges must be “jammed” to ensure that desired
results are obtained as it has been shown that groups of robots are capable of coordinating their activities by means of exteroceptive sensing alone [64]. Exteroceptive sensing can be “jammed” by means of visual obscurants or the equivalent in whatever spectrum the swarm functions. In the above context it is important to note that it may be difficult to interfere with communication in advanced SR systems due to the availability of effective anti-jamming techniques [65]. It is therefore imperative that additional means of halting the swarm are available.

Swarms can be exhausted by means of decoys which resemble the targets the swarm has been employed to pursue. By introducing a sufficient number of these decoys and placing them at strategic locations the swarm will run out of energy before it has completed anything of value. One can also use weather to one’s advantage to exhaust the swarm. E.g. by forcing it to move against the wind.

To ensure that the most appropriate countermeasures are employed one must continuously evaluate the effectiveness of employed anti-swarming schemes. This can be done by estimating the number of individuals in the swarm via trap counts. Without this information, managers will be unable to determine the effectiveness of campaign tactics and to adapt accordingly [19].

Upsurge Elimination

Upsurge elimination refers to the control of fully gregarious populations at the end of an upsurge and the beginning of a plague [66]. Direct elimination at earlier stages would easily leave sufficient non-scattered individuals operative to continue the upsurge. Targeted elimination is therefore only initiated as a part of the upsurge elimination scheme, which involves:

- Elimination of important sub-populations
- Determining when to move on to full scale plague suppression

Targeted elimination of sub-populations can be performed by removing elements that hold the swarm together. In hierarchical swarms the focus should be on individuals at the top of the hierarchy and highly connected members of the swarm. If the swarm is fully distributed “block attacks” against high density areas should be carried out first [19]. The idea is to break connectivity and maximize elimination rates in a cost effective manner. Post-1989 campaigns against locust swarms demonstrated that when this approach is correctly employed it also reduces adverse side effects on the environment. However, it should be noted that small populations can be expected to disperse to avoid annihilation when being attacked and thereby scatter over vast areas, which then causes an even greater challenge. Individuals in SR systems can also hide and return once they have recovered [30, 67]. It is therefore important to continue to confine the swarm whenever possible.

The second important part of the upsurge elimination scheme involves determining when full scale plague prevention is necessary. This requires the ability to determine when a population explosion is underway and depends on having access to accurate monitoring technology [68].

04-Oct-16
Plague Suppression

Full scale plague suppression should be implemented in conjunction with the above schemes and involve:

- Pushing the swarm back to a pre-plague phase
- “Wipe out”
- Implementing protective measures to limit causalities

As pointed out in [69] little is known about the mechanisms that underlie phase reversal, but it is important to reduce population numbers, densities and the degree of connectivity to levels that do not support plagues [25, 24]. It should also be noted that hysteresis is expected while numbers, densities and connectivity levels are being pushed back [25].

“Wipe outs” can be performed by flooding areas such that UGVs and other robots which operate close to the ground are immobilized. Water can also be used to force swarms out of their hiding places [52, 70]. Projecting large numbers of low cost oscillating objects into the swarm which result in collisions, is an alternative approach. Standoff tools with high energy emission radius (such as high powered microwaves or magnetic pulse emitters) can ultimately also be employed. However, to minimize unwanted side effects in these latter cases it is important to first measure the diameter of the swarm and then use this insight in the process of selecting the appropriate tool. In any case, one should aim to damage at least 40% of the swarm to ensure that it breaks down, otherwise it is likely that the swarm will reorganize and thereby self-repair [24]. If the swarm is small it may reorganize quickly. Larger swarms will repair at a slower rate and can in extreme cases even collapse and die “under their own weight” due to the relatively longer travel distances required for reorganization. General guidelines for self-repair in SR systems are as follows: i) the average travel distance required for self-repair equals \( \frac{\text{swarm diameter}}{2} \), ii) self-repair time equals \( \frac{\text{swarm diameter}}{2} \times \text{velocity} \), and iii) the time taken for self-repair increases linearly with the size of the swarm [24].

If blue teamed SR systems are employed in “wipe outs” it is important that the swarms are more agile (ideally faster than the attack speed of the adversary swarm), have more effective weapon systems (ideally longer range), are larger (ideally three to one), have longer endurance and have better armor to maximize chances of success [71, 72, 73]. It may also be advantageous to attack the adversary swarm from the back or the top, and this should therefore be taken into consideration when deploying blue teamed swarms [74].

To reduce causalities protective measures should be implemented throughout the Plague Suppression Scheme. Encirclement by adversary swarms should be avoided by means of effective use of surrounding terrain or available infrastructure [38, 54, 70, 75]. When encirclement cannot be prevented the anti-swarming box formation described in [38] can be employed, or one may use a blue teamed SR system as a protective circle or sphere while ensuring that vulnerable individuals are located at the center of the protective formation [76]. This tactic is commonly observed in musk-oxen and prevents predators from getting hold of the weaker individuals at the center of the group [77, 78].
Fountain splitting tactics where the group splits and regroups at the original location or coordinated flash expansion tactics, which makes it difficult for the adversary swarm to focus on one target, may also be initiated to reduce casualties [54]. If this proves to confuse the adversary swarm then it is best to stay together and proceed with collective evasive tactics, otherwise it is advantageous to disperse [76].

An alternative is to attempt to escape the hyper-sphere, which resembles the total sensing area of the swarm and hide to promote overshoot [7, 54]. However the ability to move fast, preferably in small groups, is then required.

FUTURE DIRECTIONS
A series of issues must be addressed to achieve this paper’s strategic vision. We should:

- establish expert anti-swarming and backup teams with access to required financing, infrastructure and equipment to facilitate rapid and effective responses to SR threats
- determine when anti-SR control measures should be initiated
- study the mechanisms that underpin phase reversal
- formulate monitoring, target identification and assignment tools for large regions and high value sites
- produce traps to collect information about adversary SR systems
- investigate how effective confinement zones can be established
- produce advanced counter SR jamming and hijacking methods
- investigate a suite of methods for exhausting SR systems
- formulate targeted elimination mechanisms which enable us to remove elements that hold SR systems together
- formulate methods for wiping out large numbers of SR nodes
- produce large scale, agile and durable counter swarms with standoff weapon systems capable of operating when faced with advanced countermeasures
- formulate effective protective formations, evasive tactics and methods that enable us to hide from SR systems
- develop metrics for assessing the effectiveness of employed counter measures
- establish a knowledge management system where gained insights are stored and shared amongst institutions and groups that should have access to the information

Details relating to the above and a more comprehensive depiction of the presented strategy will be given in an anti-swarming manual which currently is being articulated by the author.

CONCLUSIONS
In conclusion, an attempt to formulate a complete anti-swarming strategy that can be employed against adversary robotic swarms has been presented. The proposed strategy is important as natural swarms have proven capable of inflicting significant economic damage and
advanced SR technology is likely to be widely available in the near future. Adversary SR systems are likely to be employed with little warning. Timely and thorough preparation is therefore required. To ensure that the proposed strategy has a solid theoretical foundation it is built on state-of-the-art schemes, which have been successfully employed against destructive natural swarms. A series of future directions of research and activities, which ensures that required safeguards are put in place were also presented.

ACKNOWLEDGEMENTS

The author would like to thank Paul Scharre from Center for a New American Security for his input and for connecting me with Timothy Chung from DARPA, which gave me access to literature that provided insights into current swarm vs. swarm research.

REFERENCES


