A Flock-Based Model for Ad Hoc Communication Networks

Christian Carling[1], Pontus Svenson[2], Christian Mårtenson[2], Henrik Carlsen[1]
[1]Division of Defence Analysis
[2]Division of Command and Control Systems

Swedish Defence Research Agency
S-172 90 Stockholm, Sweden
E-mail: carling@foi.se, ponsve@foi.se,
cmart@foi.se, hencar@foi.se

Abstract

We introduce a model for simulating the movement of semi-autonomous mobile units that exhibit swarm-based behaviour and collectively form a mobile ad-hoc communication network. The mobility model is used to study how the topological properties of the resulting communication network change over time. The connectivity graphs are determined by allowing each unit to communicate with others inside a given radius. By varying the free parameters of the mobility model, qualitatively different regimes of movement can be emulated. A number of properties of the graphs (*e.g.*, the size of largest connected component, overall network efficiency and the number of isolated units) are calculated and compared for the different regimes. Finally, we present several directions for future work, both in terms of further applications and extensions of the present model.

1. Introduction

The approach of the information age has made command and control (C2) systems more and more important. What we here call the information age implies not just new possibilities for superior C2 systems – the entire character of conflicts will change. The new spectrum of conflicts includes network centric warfare [1], cyberwar [2] and netwar [3]. Moreover, the armed forces will to an even larger extent be faced with operations other than war such as peace keeping and peace enforcement operations.

In contrast to current C2 systems, future systems cannot be characterized by words such as rigidity, homogeneity and stability. Key characteristics will instead be heterogeneity, variable connection topology and lack of complete knowledge of the architecture at any instant of time. Modern methods for information fusion [4] can be used to determine an accurate situation picture of a battlefield, but they require fast and reliable communication paths between sensor platforms and operators. Since every platform and ultimately even every soldier can be seen as both a sensor and a recipient of (part of) the situation picture, the amount of data that must be transmitted will be large.

These characteristics call for new methodological approaches for designing reliable communication networks. These networks must be analysed thoroughly to determine their attack vulnerability and weaknesses. In this paper we describe work in progress undertaken at the Swedish Defence Research Agency, aimed at modelling topological features of C2 systems that take the complexity of future tasks for the armed forces into consideration [1].

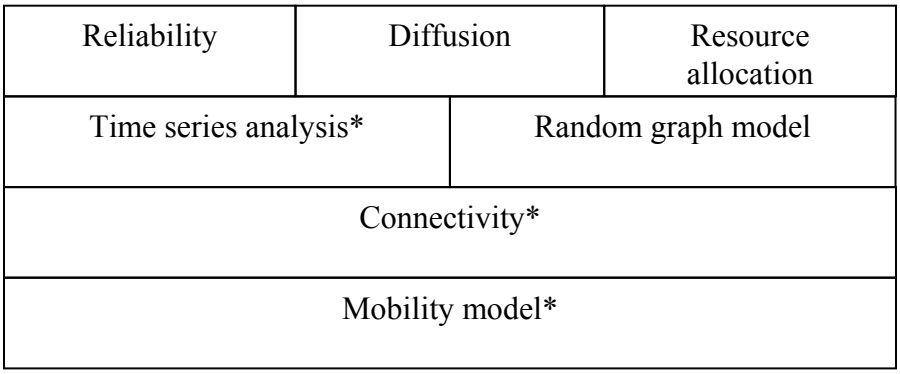

Figure 1: Modelling framework

The issues to analyse for current and future systems largely coincide. Performance, quality of service and reliability, for example, continue to be of vital importance. However, the environment in which future C2 systems will operate is radically different. Therefore, the issues have to be analysed from a different perspective.

The work presented here is part of a larger framework, a schematic picture of which is shown in figure 1. We are interested in communication networks emerging from complex conflict dynamics. Therefore, the mobility model is the point of departure for our work. The connectivity of the communication network is then derived from the underlying dynamics. At the next layer, two parallel and complementing tracks are developed. The straight-forward approach for analysing the connectivity graphs is time-series analysis. Random graph modelling is an indirect, albeit powerful, approach that is more computationally feasible when dealing with large networks. On top of the framework are the various applications of the underlying results. Here, we mention the three most interesting applications: reliability, diffusion (spread of information in the network), and resource allocation.

Results achieved so far derive from the two first layers and time series analysis, as indicated by the asterisks in figure 1. This provides the foundation for the remaining stages. Reliability concerns itself with robustness of C2 systems against attacks and malfunctions. Resource allocation is closely related to efficiency of communication. Nodes in the network will have different specialities. A sensor node that detects a target must communicate information about it to a classifier node, which will transmit its output to a command node. If the target is hostile, the command node may order an attack against it. If so, the nodes that are selected to execute the attack must quickly receive relevant information about the target.

[1] The present work is a continuation of an earlier paper, see Carling, C. and H. Carlsen. *Project Metanet: Methods for Analysis of Complex Networks*, in *7th International Command and Control Research and Technology Symposium*, 2002. Quebec City, Canada: CCRP.

Communication efficiency is also related to diffusion of information. Since the nodes of the network are non-stationary, information can be transmitted also by moving nodes. Transmitting information in this way would be a good alternative when radio communication is dangerous or impossible.

The paper is organized as follows. In the next section we introduce a model of communication between mobile units that aims at capturing some key characteristics of a broad range of conflicts. Section three contains an analysis of the connectivity properties of the dynamically changing communication network. We conclude with directions for future work and a more thorough discussion of the top layer of figure 1 in section 4.

2. **Model of Mobile Communications Networks**

The present study is limited to topological features of C2 systems, *i.e.* we omit issues such as routing and energy consumption. For this purpose we need a model of conflict rich enough to capture key characteristics of a wide range of modes of conflicts.

At the microscopic end of the spectrum of war modelling, analysis often starts with the sets of differential equations put forward by Lanchester in 1916[2]. These equations, which can be deterministic or stochastic, represent attrition in combat. Over the years, these models have been refined to include effects of interaction between forces, game theoretical considerations on decisions, terrain models via three dimensional movements in space and time, and so on.

A Lanchesterian view of war is thus focused on attrition and force size. In our case, we are mainly interested in the ability of units to communicate, and hence focus on the dynamics of movement. A Lanchester based model is not well suited to incorporate the complex dynamics that can arise in the case of small autonomous units (perhaps working in concert) continuously adapting to changing conditions. A key characteristic for this situation is the absence of a central command that dictates the action of each unit; hence the ability to self-organize is vital. This is the kind of behaviour that can be expected in operations with highly trained special units, in guerrilla warfare, violent demonstrations and conflicts at the edge between peace and war.

Traditionally, the vast majority of work has been devoted to modelling in the military domain. While we acknowledge this highly valuable work, we think there are reasons for going beyond studying the isolated domain of military conflicts. The reasons for this are twofold. First, it has become harder to maintain a sharp distinction between what is defined as being a military conflict and what is considered some kind of irregular mode of conflict. This is further underlined by the September 11th attacks and their aftermath. Future forces must be able to meet a broader range of challenges; modelling must keep pace with this development.

[2] At roughly the same time, a Russian officer, M Osipov, published a similar set of equations. For an English translation see Helmbold and Rehm, in Bracken, Kress and Rosenthal (eds.), *Warfare Modelling* (1995).

Second, military operations other than war (such as peace keeping) are an increasing activity for the armed forces in a number of countries. These kinds of operations pose new challenges to modelling efforts. Here, the dynamics differ substantially from those of traditional conflicts. For example, the interaction with civilian society and authorities is a key component in these operations. Furthermore, attrition is no longer a key parameter.

During the last decade or so, a number of alternative models for conflicts have been proposed. To a large extent, these approaches are influenced by developments of complex systems studies. A corner stone of this approach is a "bottom-up" philosophy to the effect that interactions via simple rules on a micro scale can result in complex behaviour on an aggregated level. "Agent based modelling" is an acronym used to describe this line of research. Work in this tradition include models based on cellular automata (*e.g.*, Woodcock *et al.* [7]).

Here, we analyse implications for certain properties of C2 systems in the light of complex systems modelling of conflicts. A model originally proposed for simulating flocking behaviour of animals is used for mobility movement simulations.

2.1 ***A Flocking-Based Mobility Model***

In this work we are interested in capturing the collective behaviour that results from the movement of autonomous units. We want to find behaviour that on large scales seems intentional and under the control of a steering body. This kind of behaviour must be the aim of operations where a high degree of self-organization is permitted on a low level. Self-organization on the micro level must go hand in hand with the ability to focus on a common task.

The behaviour of shoals and herds of land animals is fascinating in its seemingly unpredictable, yet coordinated motion. The dynamics resemble some of the key features above. This makes models of flocking interesting candidates for simulation of the types of conflict that we are interested in. In one of the more successful attempts to model flocking behaviour, Reynolds had an idea in mind that resembles these characteristics [9]. Reynolds suspected that flocking was a decentralized activity, and created a computer model to investigate his theory.

Reynolds model is based on an "individual unit hypothesis", meaning that the units act according to a set of rules that are applied in their neighbourhoods. In addition to being governed by the external state, *i.e.* the neighbours in the vicinity, the particles internal state also govern the motion. Here, the internal state of a particle is just its velocity. The particle neighbourhood is defined by two parameters, θ and r, see figure 2.

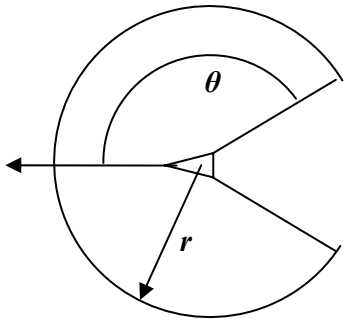

Figure 2: The neighbourhood of a unit is defined by the angle θ and the distance r.

To participate in a flock each unit strives to stay close to the flock while avoiding collision with other units. Stated simply, the rules that determine the movement of a unit are (see figure 3):

(i) avoid collisions with nearby units,
(ii) attempt to match velocity with nearby units, and
(iii) attempt to stay close to nearby units.

In each case "nearby" is interpreted as those units that are within the sector defined by r and θ.

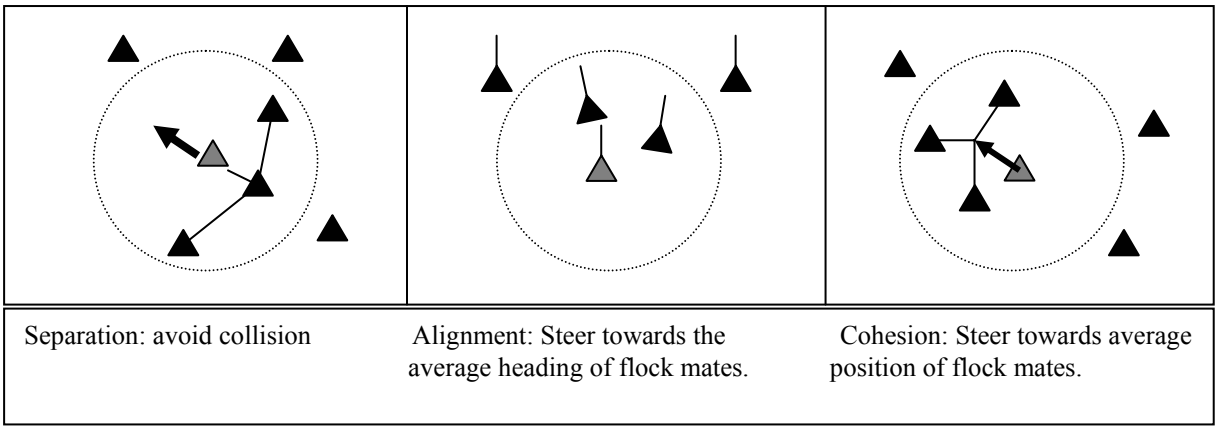

Figure 3: Flocking rules.

With no loss of generality and to assure physically reasonable motion, we limit the speed and acceleration of each unit by given maximum values. In addition to θ and r, each of the three flocking rules is also assigned a weight.

In addition to the three basic rules producing flocking behaviour, we include two other simple steering rules: one is a pure random walk and the other is a constant motion in a fixed direction. All these are finally combined (through weighted vector addition) to produce an "interesting" overall behaviour. Adding a small component of random walk introduces noise into the system, producing more dynamic patterns. The fixed translation gives the flock "somewhere to go" as a

whole, which also affects the resulting mobility pattern. Hence, the mobility model, as formulated here, has eight free parameters[3].

For the sake of simplicity, the units are moving on a flat ground and influence of terrain is neglected. Our aim is not to find a set-up that in detail can mimic all the dynamical aspects of a certain type of warfare or conflict. Instead, we seek a single model that is rich enough to capture a wide range of characteristic dynamical behaviour.

A typical situation of interest for the study consists of a rather large number of units, acting without (or under minor influence of) a central command. In the future, we foresee a rising number of conflicts that include this kind of tactical situations. First, a major line of development is different forms of unmanned vehicles, either A(ir), G(round), W(ater) or U(nderwater).
With further downsizing, the prospects for joint operations with a large number of autonomous units will increase. On the other hand, a number of different tactical situations still include – and will continue to include – only the individual soldier or other combatant as the basic unit. Here, improved communication techniques, *e.g.,* on a peer-to-peer basis, dramatically change the rules of the game. Recent examples include the use of SMS messaging to synchronize actions undertaken by activists in street fights in Prague, Gothenburg and Genoa. Special operations forces operations are also included along this line. In the middle, we find the more conservative set-up of platform-based operations, although enhanced with massive network capability through sophisticated C2 systems.

Among the many possible set-ups, we have chosen three different military behaviours for generation of connectivity graphs. The examples should not be justified on their ability to exactly mimic some specific behaviour or tactical situation. Rather, they are chosen as instructive illustrations of the mobility model. However, when configuring the model inspiration from tactical situations has played a vital role, and hence we label the examples according to conventional ground forces, special operations forces with a preferred direction and special operations forces without preferred direction.

In all examples 200 units are involved and the initial configuration is randomized inside a given region. To achieve the different behaviours three parameters where changed: the amount of directional drift, the flocking range and the cohesion weight. The conventional ground forces are characterised by strong directional drift, small cohesion and large flocking range. The two special operations forces configurations have smaller vicinity ranges and stronger cohesions. This encourages the formation of smaller groups. For undirected special operations forces there is no directional drift, but the units are placed within a potential well; this keeps them from drifting off to infinity.

Figure 4 shows snapshots of the dynamical evolution of the three examples. The initial coherent behaviour in the case of conventional ground forces and special operations forces with preferred direction is evident from the figure. Later, the special operations forces organize in a more spread out behaviour compared to the conventional forces. In the case of special operations

[3] The original model as formulated by Reynolds, allows for separate definitions of the neighbourhood of each of the three steering rules, giving a total of nine parameters (a range, an angle and a weight for each).

forces without preferred direction, the initial random configuration is spread over a somewhat larger area. This resembles a situation when an operation has failed: the troops are spread out and try to organize for survival. After a short time interval, the troops have indeed self-organized into a number of smaller groups of typically 5 to 15 members. Later, some groups break apart and new groups form.

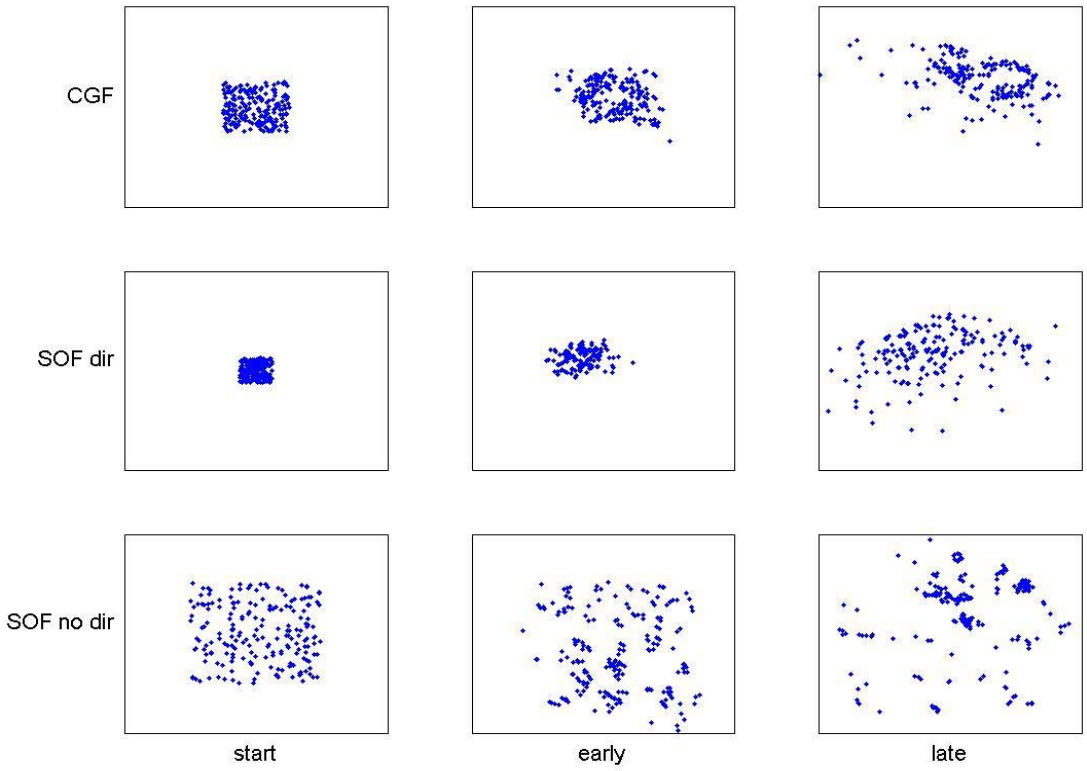

Figure 4: Snapshots of simulations of the three different types of military behaviour. From top to bottom, configurations for conventional ground forces (CGF), special operations forces with a preferred direction (SOF dir) and special operations forces without preferred direction (SOF no dir) are shown. Left column shows initial configurations at time 0. In the middle column, the configurations for times 500 (CGF and SOF dir) and 100 (SOF no dir) are plotted, while the right column displays configurations at times 5000 (CGF and SOF dir) and 1000 (SOF no dir).

2.2 ***Connectivity Graphs From the Flocking Model***

The connectivity graph is built up from instantaneous time-slices of configurations of the units. Each unit has a range of connectivity described by the radius *d;* all other units within distance *d* of it are connected to it. Since all units are constantly moving, new units will enter and others will leave the vicinity region. In this way a connectivity network of nodes and links is created

with units identified as nodes and possible communications by links, see figure 5. As a result of the units being constantly moving, the connectivity topology will change over time.

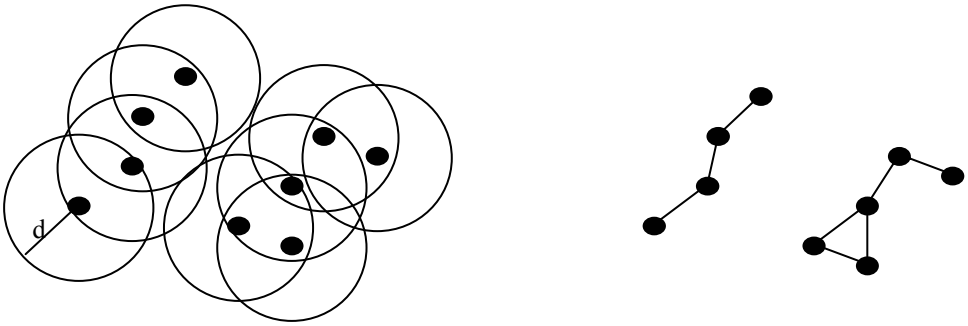

Figure 5: A snapshot of the configuration of a fraction of the units and the corresponding connectivity graph.

The resulting model shares many features with so called mobile ad hoc networks[4]. The idea behind mobile ad hoc networks originated in the 1970's, but it is only lately that the field has gained momentum. As already mentioned, the communication network lacks a central administration; the nodes act as end systems and routers at the same time. This has far reaching consequences for the characteristics compared to a static network. First, routing is more challenging due to the changing topology and the problem of proper management of address databases. Second, the position of the nodes must be distributed among the nodes themselves [11]. Other problems include power management and security [12]. In this project we leave these issues aside and concentrate on the topological characteristics of the resulting graphs.

3. **Properties of the Connectivity Graph**

A graph is a collection of nodes, usually numbered from 1 to n, and a list of edges (i,j). In general, each edge can also have a cost or weight associated with it, but this will not be used in this paper.

In recent years, many new graph models have been introduced. Among the most interesting are the so-called small world and scale-free graphs [14-18]. In order to distinguish between different graph models, it is necessary to measure several different quantities.

A graph can consist of several connected components; two nodes i and j are in the same component if there is a path between them. The size (number of nodes) of the largest component is interesting to study in for example disease spreading applications. We define $p(k)$ as the number of neighbours of node k. Those nodes that have no neighbours (*i.e.*, $p(k)=0$) are particularly interesting.

[4] For a review, see Hubaux, J.-P., et al., *Towards Self-Organized Mobile Ad Hoc Networks: The Terminodes Project.* IEEE Communications Magazine, 2001(January): p. 118-124.

A useful measure of network connectivity is the global efficiency introduced by Latora and Marchiori [19]. They define the efficiency between two nodes as

$$\varepsilon_{ij} = \frac{1}{d_{ij}},$$

where d_{ij} is the shortest distance, measured in number of hops, between nodes i and j and $d_{ij} = \infty$ if there is no path between the nodes. The global efficiency is then the average of this over all pairs of nodes in the graph,

$$E_{glob} = \frac{1}{n(n-1)} \sum_{i \neq j} \varepsilon_{ij}.$$

The advantage of this measure over for instance measuring just the mean distance is that it works even when the graph is not connected, as will often be the case for our simulations.

Another important aspect of connectivity is robustness of communication. A fail-safe network should be able to lose some communication nodes with little or no influence on the communication as a whole. Such behaviour corresponds to a highly clustered network, with a large clustering coefficient. For a node i, the local clustering coefficient is defined as the number of pairs (j,k) such that there are edges (i,j), (i,k), and (j,k); the total clustering coefficient is the normalized average of this over all nodes.

In figure 6, we show the full degree distribution $p(k,t)$ for various times t for the case labelled "special operations forces, with a specified direction to its target". The z-axis displays the number of units that have exactly k neighbours at time t. Two things are readily apparent from this figure. After a quick transient behaviour, the distribution seems to stabilize. This stabilization coincides with a significant increase in the number of isolated nodes. This is easily understood as the units drifting away from each other, out of communication range (see also figure 7 below). Using a larger communication range d would produce a similar initial transient, but stabilize at a higher average degree.

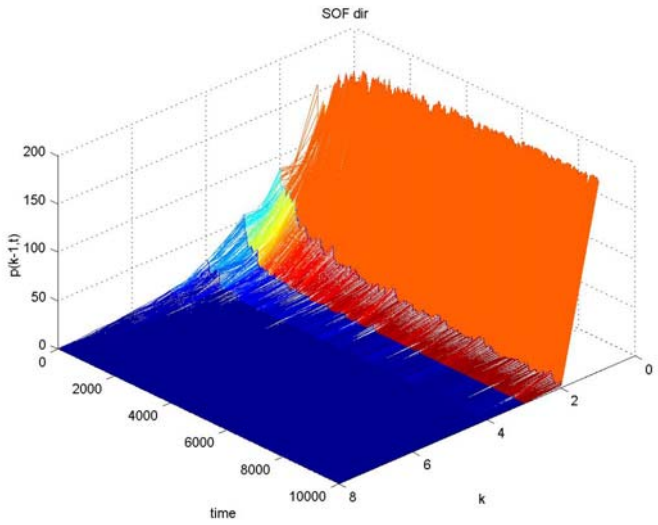

Figure 6: The degree distribution *p(k,t)* for a SOF dir-case.

Our conclusions from figure 6 are confirmed by examining other properties of the connectivity graph. Figure 7 shows the global efficiency for the same case. We see a quick, almost exponential decay up to time approximately 10000, thereafter the system stabilizes at a value that is characteristic for the phase.

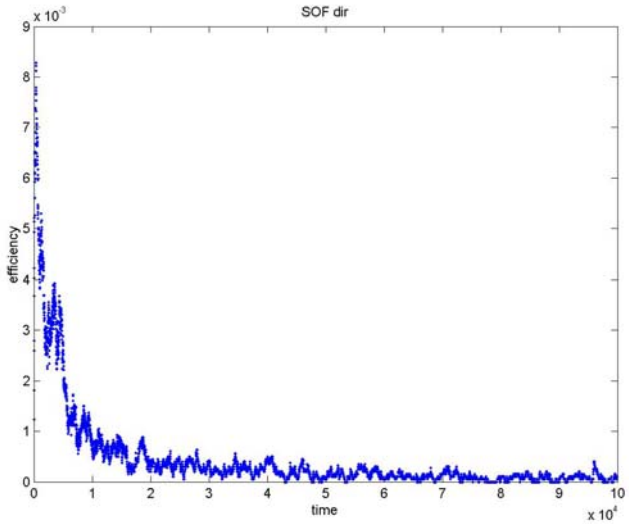

Figure 7: Global efficiency as defined by Latora and Marchiori for the case SOF dir. Note the quick decay until stabilization at a value an order of magnitude smaller than at the start (where all units are close together and hence can communicate efficiently).

Figure 8 shows the number of isolated units, *i.e.*, those that have lost contact with the others completely. This number fluctuates strongly in the stationary phase – many units are periodically out of contact for a short while before they reconnect.

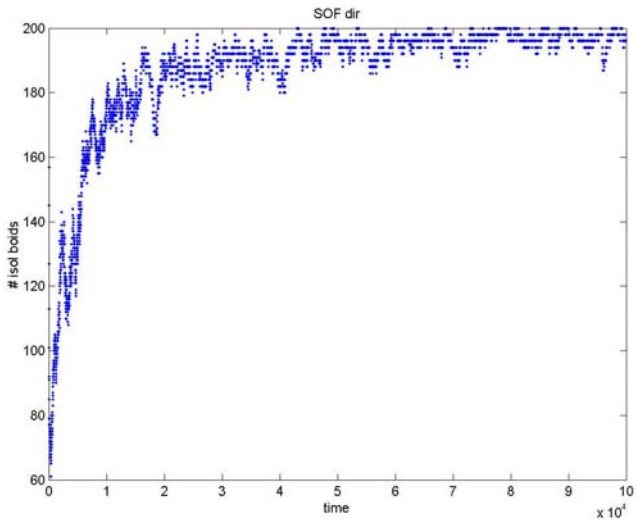

Figure 8: Number of isolated units as a function of time for SOF dir. This quantity reaches its stationary behaviour somewhat slower than the global efficiency.

In order to be able to share a situation picture efficiently, it is important that all units can communicate quickly with each other. The global efficiency, plotted above in figure 7, is one measure of this. Another is the size of the largest connected cluster at each time interval, shown in figure 9. The difference between the efficiency and maximum cluster size is that the former takes into account also the time needed to propagate information. This is important when transmitting large amounts of information, but for other types of information (*e.g.*, an order to cease fire), the maximum cluster size is more relevant.

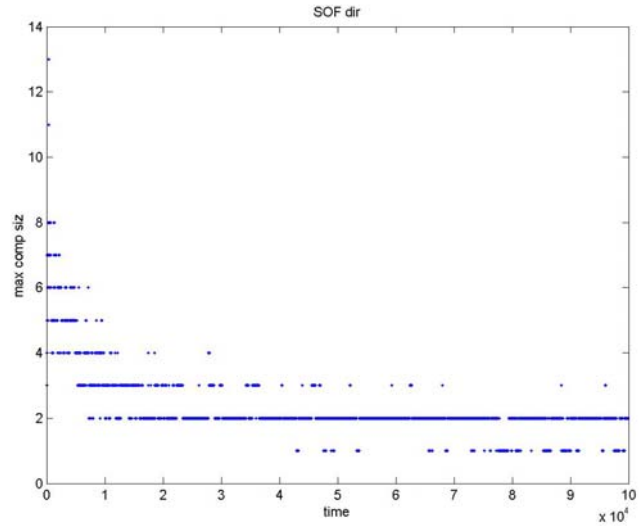

Figure 9: Size of the largest connected cluster of units as a function of time. This quantity is interesting since it determines the number of units that can be reached by a short message immediately.

When constructing the connectivity graph, different radii *d* can be used. Using a very large *d* of course leads to a connectivity graph that is almost the complete graph, while a too small *d* gives a graph consisting of only isolated units. In figure 10 we compare the global efficiency for *d=0.5 r* and *d=2r* using the "SOF dir" mobility pattern. The difference in efficiency is more than an order of magnitude. This shows the importance of being able to communicate just a little bit further. Increasing *d* in a real situation would however also lead to an increased risk of detection by enemy signal surveillance.

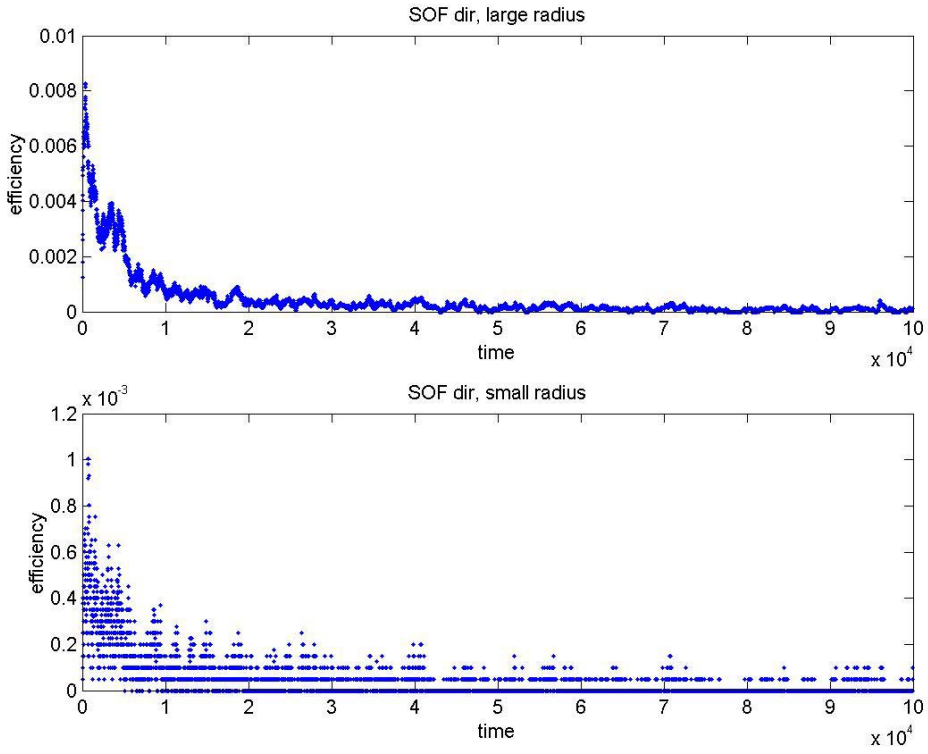

Figure 10: Global efficiency for different communication ranges *d*. Note the increase by more than an order of magnitude when increasing *d* by a factor 4.

We also analysed two other important cases of flock behaviour. Results for the global efficiency, number of isolated nodes and size of largest component for SOF no dir and CGF are shown in figure 11.

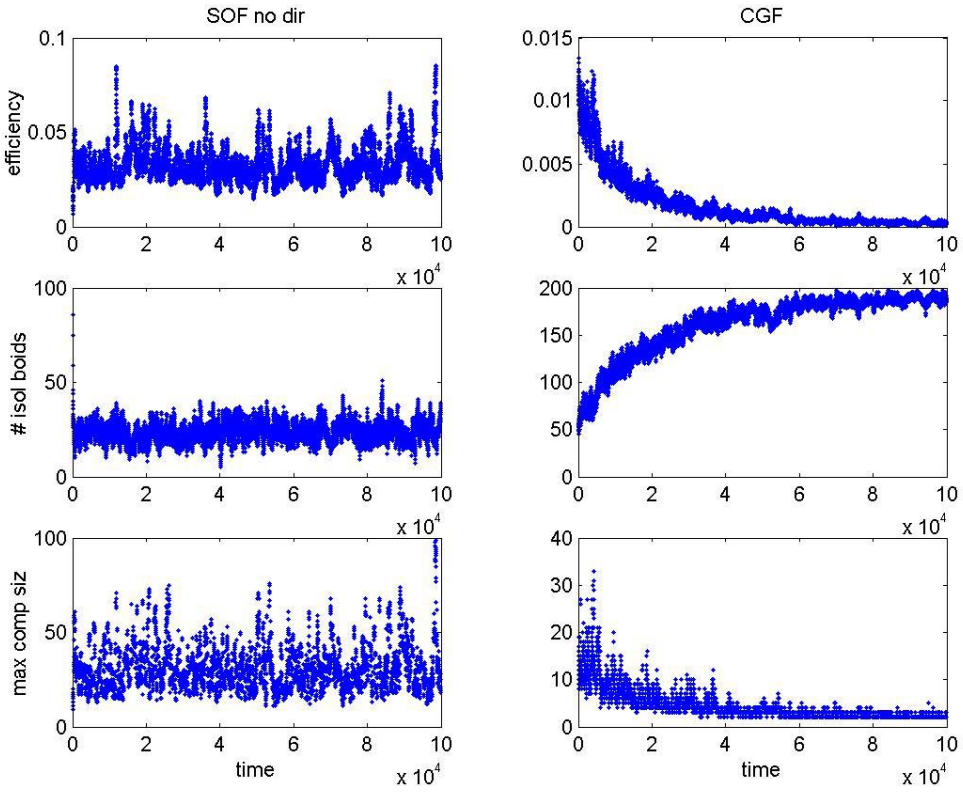

Figure 11: Global efficiency, number of isolated nodes, and size of largest component for SOF no dir and CGF. Note the differences – SOF no dir is basically random, while CGF looks very similar to SOF dir.

The figure clearly shows that the addition of a preferred direction to the flocking model leads to a completely different behaviour. Note the similarity between CGF and SOF dir – this means that the direction is a relevant parameter for this problem, while the distinction between SOF and CGF is irrelevant, at least for the quantities that we have calculated.

We have performed several more computer experiments using flocking parameters that are close to those analysed above. Most of these display the same properties as discussed above – the flocking model thus seems to possess a remarkable stability against small perturbations. This will be investigated further in a future publication.

4. **Discussion and Directions for Future Work**

In conclusion, we introduced a flocking model that captures the qualitative features of moving individuals, and manned or unmanned platforms. By varying the flocking parameters, we obtained different regimes of movement. For each regime we determined a time series of connectivity graphs using a radius of communication d that would correspond to, *e.g.*, using a low-power radio or line-of-sight laser communication. The connectivity graphs were analysed and shown to possess different characteristics depending on the mobility pattern. We noted in particular the dynamic nature of these graphs. At each instant, there are many unconnected units

and the size of the largest connected component is small. But since the units move, the connection pattern changes, hence they are able to exchange information quickly.

The most important result of this paper is the large effect on the global efficiency of increasing the radius of communication. When planning an operation, this increase must be weighted against the increased danger posed to the troops if their communication equipment operates at higher power levels.

4.1 Extensions of the basic model

In this paper, we took a "minimalist" approach, trying to keep our modelling framework as simple as possible. The basic model described above can however be modified and extended in many ways, to allow for more complex situations:

Heterogeneous units
The fundamental mobility parameters (mass, maximum speed and force, flocking neighbourhood definition) are the same for all units in the simulation. It is trivial to let mobility parameters vary between individual units, allowing us to simultaneously model very agile and more slow-moving units. One obvious limiting case is inclusion of fixed installations that do not move at all, but serve as base stations/gateways for communication.

Adversarial units
Several authors have implemented flock-based models of adversarial behaviour through simultaneous modelling of red and blue forces, which coordinate their motions and pursue and attack members of the opposing force. This produces much more dynamic movement than our one-sided simulations.

Extended flocking neighbourhoods
The flocking model we have implemented closely follows Reynolds original work. Since his primary intention was to model animal behaviour, the restriction to narrowly defined local neighbourhoods for coordinating movement is essential, since it captures an element of reality. However, swarms of unmanned vehicles (flying, floating, rolling or whatever) could coordinate their movement over larger distances, using the emergent ad-hoc communication network to broadcast position and speed of each unit across the swarm. There is however no point in pushing this to any extreme, trying to achieve "perfect situational awareness", since such global coordination would likely take away most of the fluidity and adaptive behaviour of the swarm.

4.2 Network reliability

When discussing network reliability, it is instructive to make a distinction between structure, function and content. Following Libicki [21], there are three different kinds of attacks against a network: physical, syntactical and semantic. A physical attack destroys or denies individual nodes or links, through physical means (blast or radiation). Syntactical attacks target the operating logic within nodes, disrupting their function but otherwise leaving them unharmed. Semantic attacks target the information *content* that flows across the network.

It is thus possible to disturb the network by other means than changing the topology. One can think of several schemes with the effect of changing the functionality. The lack of centralised command implies a need for decentralised cooperation. As a result, it will be an easy task for a malicious node to cause severe harm to the performance of the network. By taking over a node, an antagonist has the possibility to alter the functionality of the network while keeping its topological properties constant. By letting the node advertise that it knows the shortest path to a target of important, it can reroute traffic to itself. Another approach is to let the hijacked node fill the network with traffic, *i.e.,* a type of denial of service attack. One can think of still other means of disturbing the network, once one has the control of a node. In future work, we will concentrate on topological aspects of reliability. Both random failure and deliberated attacks will be studied. In both cases, the nodes ability to participate in the communication network can either cease to exist forever or it can be unable to communicate over a period of time.

Topological failure can be modelled by removal of either links or nodes. Node removal implies the loss of all links belonging to the node. Taking out terminal nodes that only have a single connection obviously does not affect the rest of the network. The loss of bridging nodes or hubs can severely affect the connectivity of remaining nodes, possibly decomposing the network into several smaller disconnected components. The mobile network setting destroys the clear-cut distinction between terminal, bridging and hub nodes. The continuous relative motion implies that individual nodes will change roles over time: at one instant a node is a terminal node, shortly thereafter, it may be in a more central role, serving as a temporary bridge or hub for the communication between several other nodes. This also makes the concept of targeted attacks against mobile communication networks hard to define: As an outside observer, how do you determine which units, or group of units, to attack for maximum effect?

The effect of internal failures is studied via removal of nodes and links at random. In the case of external attacks, the antagonist who wants to cause as much harm as possible to the network can act from geographical information. This is due to the fact that in our simple model there is a simple correspondence between geographical configuration and connectivity. The antagonist can use two different strategies. In the first case, they choose to knock out a fixed number of the most centrally localized units. This is based on the assumption that these units contribute to a larger number of communication paths. The second strategy is to eliminate nodes in a line perpendicular to the aggregate path traced out by the flock. In this case, the antagonist seeks to cut off the front group from the stragglers.

4.3 Random graph modelling

Even though we have strived to build a fast-running model, the generation of connectivity graphs is time consuming. For large numbers of units, it is not feasible to generate exact connectivity graphs. Another interesting approach is to use some properly defined random graph model that approximates the global characteristics of the communication network generated via the mobility model. The two approaches should match each other in a statistical sense: the ensemble average of the random graph model should approximate the time average of the simulated connectivity graphs. This approach permits us to use several standard methods from random graph theory when studying the properties of the communication network.

4.4 Resource allocation

The next issue of interest is resource allocation. From the myriad of possible configuration in the network, we develop methods for extracting useful functional chains of nodes and links. A functional chain can be any meaningful combination of nodes (sensor, information processing, decision support, shooter) for performing a task; a typical example being a sensor-to-shooter chain. Since there is not a one-to-one relationship between any service and a functional chain (a sensor-to-shooter chain can be realized via many different combinations) a method for translation is needed.

4.5 Diffusion of information

In order to get a complete picture of the communication properties of the flock, we must consider the dynamical nature of the system as a whole. Since the units move, each edge has a certain lifetime. This means that information can spread not only through the connections, but also via physical movement of the nodes, that brings previously unconnected nodes within direct communication range: unit 1 transmits interesting information to unit 2, these then move apart and unit 2 can transmit the information to unit 3, which was perhaps several links away at first.

In future work, we will investigate this by giving information to one unit and measuring the number of units that have received the information as a function of time and their distance from the original receiver[5]. Other possible extensions of this idea include having red and blue teams searching for information in the terrain and distributing it among their teams, while exposed to enemy attack.

5. **References**

1. Alberts, D.S., J.J. Garstka, and F.P. Stein, *Network Centric Warfare: Developing and Leveraging Information Superiority*. 1999, Washington DC: DoD/CCRP.
2. Denning, D.E., *Activism, Hactivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy*, in *Networks and Netwars*, J. Arquilla and D. Ronfeldt, Editors. 2001, RAND: Santa Monica.
3. Arquilla, J. and D. Ronfeldt, *Networks and Netwars*. 2001, Santa Monica: RAND.
4. Hall, D.L. and J. Llinas, eds. *Handbook of Multisensor Data Fusion*. 2001, CRC Press.
5. Carling, C. and H. Carlsen. *Project Metanet: Methods for Analysis of Complex Networks*. in *7th International Command and Control Research and Technology Symposium*. 2002. Quebec City, Canada: CCRP.
6. Sheldon, B., *Comparing the Results of a Nonlinear Agent-Based Distillation to Lanchester's Linear Model*, in *Manoeuvre Warfare Science 2002*, G. Horne and S. Johnson, Editors. 2002, USMC Project Albert: Quantico, VA.
7. Woodcock, A.E.R., L. Cobb, and J.T. Dockery, *Cellular Automata: A New Method for Battlefield Simulation.* Signal, 1988(January): p. 41 - 50.
8. Ilachinski, A., *Irreducible Semi-Autonomous Adaptive Combat (ISAAC): An Artificial-Life Approach to Land Combat*. 1997, Center for Naval Analyses.
9. Reynolds, C.W., *Flocks, Herds, and Schools: A Distributed Behavioral Model.* Computer Graphics, 1987. **21**: p. 25 - 34.

[5] This is very similar to models for disease spreading and voter models.

10. Hubaux, J.-P., et al., *Towards Self-Organized Mobile Ad Hoc Networks: The Terminodes Project.* IEEE Communications Magazine, 2001(January): p. 118-124.
11. Mauve, M., J. Widmer, and H. Hartenstein, *A Survey on Position-Based Routing in Mobile Ad Hoc Networks.* IEEE Network, 2001(November/December): p. 30-39.
12. Hongmei, D., W.L. Wei, and D.P. Agrawal, *Routing Security in Wireless Ad Hoc Networks.* IEEE Communications Magazine, 2002(October): p. 70-75.
13. Bollobas, B., *Random Graphs*. 1985, New York: Academic Press.
14. Watts, D.j., *Small Worlds*. 1999, Princeton, NJ: Princeton University Press.
15. Barabási, A.-L. and R. Albert, *Emergence of Scaling in Random Networks.* Science, 1999. **286**: p. 509-512.
16. Albert, R. and A.-L. Barabási, *Statistical Mechanics of Complex Networks.* Reviews of Modern Physics, 2002. **74**: p. 47-94.
17. Newman, M.E.J., *Models of the Small World: A Review.* Journal of Statistical Physics, 2000. **101**: p. 819.
18. Newman, M.E.J., S.H. Strogatz, and D.J. Watts, *Random Graphs With Arbitrary Degree Distribution and Their Applications.* Physical Review E, 2001. **64**: p. 026118.
19. Latora, V. and M. Marchiori, *Efficient Behavior of Small-World Networks.* Physical Review Letters, 2001. **87**: p. 198701.
20. Adamic, L.A., et al., *Search in power-law networks.* Physical Review E, 2001. **64**: p. 046135.
21. Libicki, M.C., *The Mesh and the Net: Speculations on Armed Conflicts in a Time of Free Silicon*. 1996: National Defence University.