EVO-SCHIRP: Evolved Secure Swarm Communications

Shaya Wolf
University of Wyoming
Laramie, Wyoming
swolf4@uwyo.edu

Rafer Cooley
University of Wyoming
Laramie, Wyoming
rcooley2@uwyo.edu

Mike Borowczak
University of Wyoming
Laramie, Wyoming
mike.borowczak@uwyo.edu

Nicholas Cheney
University of Vermont
Burlington, Vermont
ncheney@uwyo.edu

***Abstract*—CHIRP (Communication for Heterogeneous IoTs with Round-robin Protection), an optimal communication protocol, performs poorly in networks with multiple agent groups (cliques). Research began on modifying and securing CHIRP with a project called S-CHIRP(Secure CHIRP). However, S-CHIRP still provides sub-optimal multi-clique communication. We created an evolutionary protocol, EVO-SCHIRP (Evolutionary S-CHIRP) and compare results against CHIRP and S-CHIRP based on communication efficiency and information security. This research took place in two phases. First, EVO-SCHIRP was compared to CHIRP by implementing an efficient communication protocol with one clique. Second, EVO-SCHIRP was compared to S-CHIRP by considering communication security. This research opportunity extends research in many fields such as swarm intelligence, evolutionary robotics, information security, autonomic systems, and decentralized communication. The CHIRP protocols have many applications such as drone communication, infrastructure inspection, and biomedical sensors.**

I. Lightweight Communications

As intrusion threats grow, autonomous systems depend on information security for intrusion detection and secure communication [1] [2]. Further, swarms rely on efficient and lightweight communication to organize their behavior and accomplish goals. Given specific communication rules assigned to autonomous agents, this research applies evolutionary algorithms to communication protocols between heterogeneous agents in groups (or cliques) of networks. Current networking and communication protocols rely on default TCP/IP-based methods. However, autonomic communications generate complex systems with a reduction in human intervention and simplify system management.

Introduction

This research evolves secure communication protocols between groups of independent agents within clustered networks. Previous work revealed an optimal communication protocol, called CHIRP (Communication for Heterogeneous IoTs with Round-robin Protection), which schedules communications efficiently within a single swarm of agents. An ideal protocol, S-CHIRP (Secure Communication for Heterogeneous IoTs with Round-robin Protection), would secure swarm communications within environments which contain multiple cliques. However, S-CHIRP does not currently guarantee that nodes will only communicate with agents within their clique. This research considers an evolutionary approach; it compares communication efficiency with CHIRP and compares security assurances with S-CHIRP. By creating an efficient communication protocol for resource-constrained agents, the CHIRP and S-CHIRP protocols demonstrate systems that are more suitable for swarm communications than methods utilized by current network infrastructures. More specifically, the first phase of this research evolves communication protocols within a single clique and compares those results to CHIRP. The second research phase compares protocols evolved in multi-clique environments to the benchmarks set by S-CHIRP.

Motivation

Once swarms are deployed, they rely on their programming to be flexible and account for the unexpected. Therefore, the scalability and adaptability of evolutionary robotics lends itself nicely to improving swarm communications. Evolutionary approaches to swarm optimization have led to promising results due to the biologically inspired nature of swarm communications and strict limitations on resources[3].

This research also provides crucial communication algorithms necessitated by swarm technology. Drawing from biological inspirations, evolutionary robotics can optimize these types of communications and further research for countless applications. Further, it can optimize communications when faced with large networks. This solution keeps overhead low and ensures feasibility of swarm communication across large scale networks [4].

Further, exploring research avenues comparable to the CHIRP and S-CHIRP protocols extends research on decentralized communication systems which are gaining popularity due to their inherent security benefits. Free from third party interests, decentralized algorithms fit many more applications than just swarm communications. They have applications in economy, business, information security, and many other large distributed environments of agents. CHIRP, S-CHIRP, and EVO-SCHIRP utilize these security benefits to ensure more secure swarm communications.

Finally, cybersecurity applications could also stem from this research. Secure-by-design systems have the potential to secure our information from malicious or intrusive third parties. CHIRP, S-CHIRP, and EVO-SCHIRP aim for a secure-by-design system.

Importance

Current swarm research efforts explore efficient processing of sensor information, goal completion, and communication between neighboring agents. Furthering research on autonomous systems requires solutions that provide for these self-managing services on resource budgets. This often means that encryption techniques aren't feasible and secure-by-design communication protocols are the only possible option.

Infrastructure systems require regular inspection and maintenance. However, manual inspection is costly, dangerous, and subject to human error. Autonomous monitoring systems avoid system failures with inspections that minimize cost, maximize safety, and provide exceptional precision [5]. The ARIA project, from Carnegie Mellon University's Robotics Institute, utilizes lightweight bots to assess structural integrity of bridges and other aging constructions [6]. Bots like these could benefit from networking and data sharing protocols, limiting the data storage and analysis required by any one particular bot. Companies also utilize drones as a risk-management solution for remote structural inspection of mineshafts [7].

Finally, this research can benefit sensor technology. Medical technology demands comprehensive and proactive detection of health risks that may not be apparent to a traditional health care provider [8]. The space constraints on biomedical sensors exemplify the necessity for an efficient communication protocol. In addition, cross communication between the sensors in two different bodies pose high security risks, demonstrating the necessity for secure-by-design communication systems.

Background

CHIRP's decentralized communication protocol can be implemented by virtually any device due to the extremely small amount of necessary stored data and minimal computations [9]. This research extends S-CHIRP by evolving unique protocols for communication and comparing the results with the CHIRP and S-CHIRP metrics. Because CHIRP is an optimal solution, less-fit evolved protocols are to be expected in the first phase of research. The second phase looks at multiple cliques in one network, where the evolved swarms are expected to see higher-fit protocols than the S-CHIRP model.

In CHIRP, each node communicates with every other node in their clique bidirectionally in as few communication rounds as possible. The CHIRP communication pattern is based on a simple equation calculated by each node during each round. This solution allows a node to use the round (R), their index (I), and the number of nodes in their clique (N), to calculate the index of their next target communication partner (T).

$$T = (R - I)\ mod\ N$$

Although this solution achieves the fewest number of communication rounds necessary for each node to talk to every other node, it still has other issues. Namely, when cliques overlap, there are a few different problems that can occur. Inactive communications occur when nodes don't have anyone to communicate with during a specific round. Other errors occur when nodes calculate the target node and accidentally speak to the node with that index in a different clique. If there is a two-sided communication error (where both nodes send a message to the wrong target), it is considered to be an invalid communication. If there is a one-sided communication error (where one node sends a message to the wrong target), it is considered to be a collision. These different communication types can be seen in Figure 1.

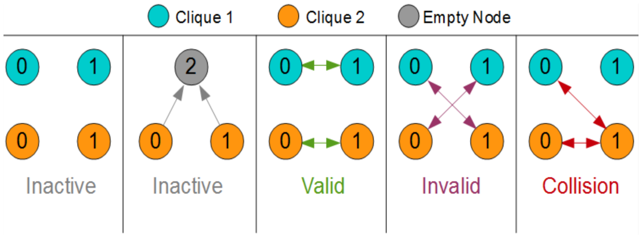


Fig. 1. Different communication scenarios for agents.

II. Experimentation Details

This research considers full cycles of communication. This means that N nodes fully communicate in N rounds during each cycle. Although this is technically suboptimal for even-numbered clique sizes, it provides for a more consistent ground for measurement from EVO-SCHIRP to S-CHIRP.

Experiment Description

This problem resembles the handshake problem. In this problem, a room full of people (agents) must shake hands with every other person at least once. The classic problem asks how many handshakes are possible. Similarly, we want to know how many rounds are necessary to complete all of the possible handshakes. After each agent has finished shaking hands with every other agent, they begin another communication cycle and the round number is reset. In addition to this, there may be overlapping swarms/cliques and cross-clique communication must be minimized. In order to replicate this behavior in experiments agents are encoded with three goals.

1) Communicate with every other node
2) Communicate with only one other node at a time
3) Do not communicate with any node from another clique

If agents maintain their three main goals, they will obtain high fitnesses. Therefore, their fitness values will follow from these goals. The number of:

1) distinct agents handshakes with worst performing node
2) distinct agents communicating per round
3) correctly paired bidirectional communications

The first phase of this research only considers the first two goals listed above. The second phase of the experiment factors in the security aspect by including all three goals listed above in attempts to to find a solution that rivals S-CHIRP. By considering multiple swarms, this research shed light on intrusive agents, the integrity of overlapping decentralized systems, and strategies to strengthen the S-CHIRP protocol.

Method Description

Protocols were arranged into matrices with two separate encodings. Both encodings set each column as the communication schedule for a particular agent and each row as the round within the communication cycle. Therefore, for matrix M, M[i][j] returns who the jth agent will talk with on the ith round. The first encoding, unique encoding, lists the index of the node that a particular agent will communicate with. For example,

$$M[1][0] = 2$$

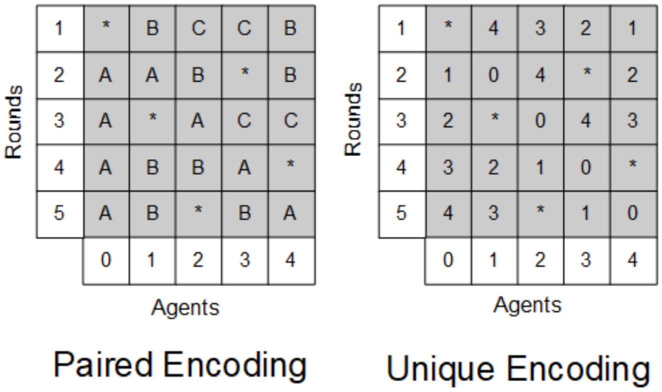
$$M[1][2] = 0$$

means that agent 0 will speak with agent 2 during round 1. The second encoding, paired encoding, each node outputs a symbol each round and those with matching symbols will communicate for that round. So,

$$M[1][0] = A$$

$$M[1][2] = A$$

again means that agent 0 will talk with agent 2 during round 1. These are illustrated in Figure 2 and an example is given in the caption. We also employ algorithms to convert protocols from one encoding to the other.



Paired Encoding

Rounds					
1	*	B	C	C	B
2	A	A	B	*	B
3	A	*	A	C	C
4	A	B	B	A	*
5	A	B	*	B	A
Agents	0	1	2	3	4

Unique Encoding

Rounds					
1	*	4	3	2	1
2	1	0	4	*	2
3	2	*	0	4	3
4	3	2	1	0	*
5	4	3	*	1	0
Agents	0	1	2	3	4

Fig. 2. In a paired encoding, the agents are paired based off of the symbol they output. So in round 1, Agent 1 communicates with Agent 4 because they both output a ”B”. In unique encoding, agents are paired based off of the agent ID they output. So in round 1, Agent 1 communicates with Agent 4 because Agent 1 is outputting a ”4” and Agent 4 is outputting a ”1”. A ”*” indicates that that agent is not communicating with anyone in that round.

CPPNs (Compositional Pattern-Producing Networks) were used with each of these encodings to evolve the data over differing numbers of generations, CPPN layers, and clique sizes. The CPPNs utilized neurons that propagate based on many different activation functions. By instituting a fully connected CPPN, communication protocols were evolved after 25 generations (or epochs), where the input to the network was the previous rounds communication matrix(random for round 0) and the network output represents the current rounds communication matrix. Multi-clique scenarios were simulated using groups of CPPNs who shared a simulated transmission space, meaning each networks communication patterns were evaluated with every other network.

The CPPN’s were evolved with a Pareto Front tournament-style evolutionary algorithm. The algorithm selects parents from a collection of possible CPPN’s, allows each of those parents to produce a child and uses tournament selection with elitism to pick survivors each epoch for 25 generations. The tournament selection process selects 50 individuals, each one being the best of a group of uniformly and randomly picked individuals from the total population.

There are two basic fitness functions, one for single cliques and one for multiple cliques. The single-clique fitness was calculated based off of how well all of the nodes talk to one another during a single round of communication. On top of that, the fitness function makes sure that agents are talking to each other bidirectionally. To achieve this for a unique encoding, the function finds, the number of:

- distinct elements in the lowest performing column/agent
- distinct elements in the lowest performing row/round
- correctly paired bidirectional communications

These numbers are summed together to obtain a fitness comparable to the maximum possible fitness (different for each clique size). To achieve this for paired encodings, the protocols are converted to unique encodings and then the same function is applied as above. In future iterations of this work, the fitness will be scaled to a number between zero and one to create one comparable maximum possible fitness across clique sizes.

The second fitness function, for multiple clique scenarios, considers both the fitness of each clique as well as invalid communications, collisions, and inactive nodes (nodes that speak with themselves). This is achieved by looking at the:

- average score of cliques using the first fitness function
- distinct elements in corresponding cells across matrices

Note that looking at the number of distinct elements in corresponding cells will count a collision once (since it is a one-sided error in communication) and an invalid communication twice (since it is a two-sided error in communication).

Experiment Distinctions

Clique sizes of five, ten, and twenty-five were considered in the final results. During each run, different numbers of layers in each CPPN were considered, running with five and ten for each clique size. The mutation rates within the network were maintained at relatively low levels, with a value of 0.1 set for both connections and neurons. Each time the fitness was considered, fitness values were stepped through a network equal in size to the number of agents. Then, when overlapping cliques were considered, three uniform possibilities were tested, each with the number of cliques being 40% of each clique size:

1) 2 cliques of size 5
2) 4 cliques of size 10
3) 10 cliques of size 25

III. Current Results

Phase 1: CHIRP (Single Clique)

In single clique generations, CHIRP outperforms EVO-SCHIRP. EVO-SCHIRP does not benefit from longer generational evolution. This is observed in the random-walk of the fitness score over time. Although some individuals had high fitness scores, this occurred randomly throughout generations. These results are shown in Figure 3. In the graphs, the fitnesses is averaged across the population at each generation and the top performers in each generation are plotted as gray dots as well.

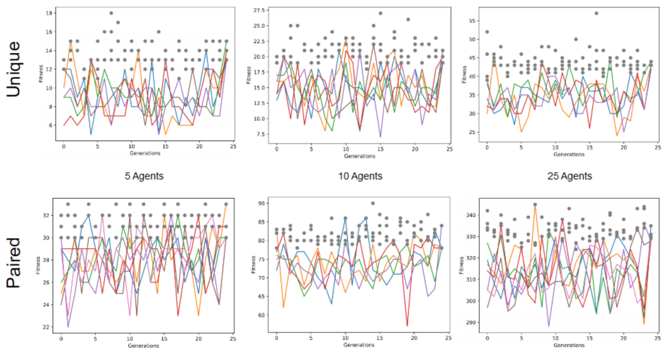


Fig. 3. The top row depicts fitness results from experiments using unique encodings with population sizes of 5, 10, and 25. The bottom row depicts fitness results from experiments using paired encodings, also with population sizes of 5, 10, and 25.

In future iterations of this work, mutation rates will be lowered to gain more control of the fluctuations in fitness. To increase the fitness of a communication schedule, different fitness functions that better incentivise correct pairwise communications are necessary. Paired encoding worked much better than unique encodings, so future experimentation will utilize paired encodings.

Phase 2: S-CHIRP (Multi-Clique)

The experiment was centered around three multi-clique scenarios. Each scenario has a uniform distribution in clique size while prior work normal and gamma distributions were also considered. In this experiment only the size of the cliques in the network were varied.

These experiments revealed that both EVO-SCHIRP and S-CHIRP result with approximately .5 fitness, or 50% fit when the fitness was scaled against the maximum possible fitness. This was not surprising for S-CHIRP, since it guarantees overlapping between cliques. In EVO-SCHIRP however, the resulting cliques are all different and therefore shouldn't experience as much overlap. In future work, a security metric other than cross-clique communications must be designed to indicate how secure a protocol is. This metric will likely be based on number of collisions and invalid communications. Future work will also include looking into normal and gamma distributions of clique sizes in the network as well.

IV. Conclusion

The research done here shows progress towards finding a secure-by-design communication protocol for overlapping cliques of agents. By using a Pareto Front tournament selection algorithm, we simulated swarms and flocks of virtual agents as they evolve, attempting to communicate with one another until the next generation. Through this research we were unable to evolve a communication pattern which performed worse than CHIRP in a single clique environment but the same as S-CHIRP in multi-clique environments.

Future Research

In addition to the future research avenues explained throughout the paper, single-hop network protocols can be extended to include multiple hops which would align with other routing research efforts in the field. Especially since agents must use minimal resources, developing a multi-hop version of EVO-SCHIRP would progress the field of swarm routing by working to minimize the required resources. Further, integration of malicious agents can demonstrate how each protocol performs with adversaries.

References

[1] S. Ganapathy, K. Kulothungan, S. Muthurajkumar, M. Vijayalakshmi, P. Yogesh, and A. Kannan, "Intelligent feature selection and classification techniques for intrusion detection in networks: a survey," *EURASIP Journal on Wireless Communications and Networking*, vol. 2013, no. 1, p. 271, Nov 2013. [Online]. Available: https://doi.org/10.1186/1687-1499-2013-271

[2] S. Dobson, S. Denazis, A. Fernández, D. Gaïti, E. Gelenbe, F. Massacci, P. Nixon, F. Saffre, N. Schmidt, and F. Zambonelli, "A survey of autonomic communications," *ACM Trans. Auton. Adapt. Syst.*, vol. 1, no. 2, pp. 223–259, Dec. 2006. [Online]. Available: http://doi.acm.org/10.1145/1186778.1186782

[3] S. Nolfi, J. Bongard, P. Husbands, and D. Floreano, "Evolutionary robotics," *Springer Handbook of Robotics*, p. 20352068, 2016.

[4] F. Dressler and O. B. Akan, "A survey on bio-inspired networking," *Computer Networks*, vol. 54, no. 6, pp. 881 – 900, 2010, new Network Paradigms. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1389128610000241

[5] M. R. Jahanshahi, W.-M. Shen, T. G. Mondal, M. Abdelbarr, S. F. Masri, and U. A. Qidwai, "Reconfigurable swarm robots for structural health monitoring: a brief review," *International Journal of Intelligent Robotics and Applications*, vol. 1, no. 3, pp. 287–305, Sep 2017. [Online]. Available: https://doi.org/10.1007/s41315-017-0024-8

[6] B. Guldur and J. F. Hajjar, "Automated classification of detected surface damage from point clouds with supervised learning," vol. 33. Vilnius: Vilnius Gediminas Technical University, Department of Construction Economics and Property, 2016, pp. 1–6, copyright - Copyright Vilnius Gediminas Technical University 2016; Document feature - ; Tables; Diagrams; Last updated - 2016-10-01. [Online]. Available: https://doi.org/10.22260/ISARC2016/0038

[7] "Hovering over opportunities," Oct 2015. [Online]. Available: https://www.zurichcanada.com/en-ca/canada/knowledge-hub/articles/2015/10/hovering-over-opportunities

[8] C. Bachmann, M. Ashouei, V. Pop, M. Vidojkovic, H. Groot, and B. Gyselinckx, "Low-power wireless sensor nodes for ubiquitous long-term biomedical signal monitoring," *IEEE Communications Magazine*, vol. 50, no. 1, p. 2027, 2012.

[9] M. Borowczak and G. Purdy, "S-chirp: Secure communication for heterogeneous iots with round-robin protection," in *2018 IEEE International Conference on Consumer Electronics (ICCE)*, Jan 2018, pp. 1–6.

[10] D. Karaboga, B. Gorkemli, C. Ozturk, and N. Karaboga, "A comprehensive survey: artificial bee colony (abc) algorithm and applications," *Springer Science+Business Media*, March 2012.