Algorithms for Operating Self-organizing Swarms of UAVs Implementing Full Exchange of Information

Suren Poghosyan
Institute for Informatics and Automation Problems of NAS RA
Yerevan, Armenia
e-mail: psuren55@yandex.ru

Yeghisabet Alaverdyan
Institute for Informatics and Automation Problems of NAS RA
EKENG CJSC
Yerevan, Armenia
e-mail: ealaverdjan@gmail.com

Vahagn Poghosyan
Institute for Informatics and Automation Problems of NAS RA
Xilinx Armenia LLC
Yerevan, Armenia
e-mail: povahagn@gmail.com

Artyom Lazyan
Institute for Informatics and Automation Problems of NAS RA
Xilinx Armenia LLC
Yerevan, Armenia
e-mail: artyomlazyan@gmail.com

Davit Hayrapetyan
Institute for Informatics and Automation Problems of NAS RA
Xilinx Armenia LLC
Yerevan, Armenia
e-mail: hayrapetyan96@gmail.com

Yuri Shoukourian
Institute for Informatics and Automation Problems of NAS RA
Yerevan, Armenia
e-mail: shouk@sci.am

***Abstract* —The article is devoted to the introduction of methods and appropriate algorithms aimed at information full exchange in self-organizing swarms of logically linked UAVs. Scientific approaches to enable surveilled areas dynamic snapshotting and full exchanging of captured images during the swarm quasi-random walk (rotor-router model) are given in terms of our relevant theorems and results obtained in this direction. Besides, our methods and algorithms for constructing optimal and fault-tolerant schemes (gossip/broadcast models) have been involved and adapted accordingly, thus creating premises for operating decentralized and self-organizing swarms of logically linked UAVs.**

Strong authentication of the swarm UAVs, also mechanisms for secure and reliable data transfer based on proven principles of threshold cryptography, are accordingly presented.

***Keywords* — self-organizing systems; swarm of UAVs; information full exchange; fault-tolerant schemes; data and transfer security.**

I. Introduction

Recent development of unmanned aerial vehicles (UAV) has led to rapidly increased demand on decentralized and self-organizing systems for which information full exchange plays a significant role. Nevertheless, dynamically reconfigurable and self-organizing networks face the challenge of connecting nodes and systems not only in terms of technical deployment, but also in terms of collecting, conveying and integrating relevant information. Besides, organizational issues arise in promoting models, methods and software tools enabling real-time decision making based on collective intelligence of ad-hoc substructures. Operation of swarms of UAVs within this particular context points out to the need for adaptive methodologies of building a timely and resource efficient information exchange model. Among other concerns, secure data transfer is another major issue given the wide spectrum of targeting tasks.

Set of UAVs with relatively simple structure and logic (as a cellular automaton defined on a connected graph) stands for a collective decision-making environment with the following distinguishing feature: collective intelligence of a group is greater than the sum intelligence of its individual members. With this regard, modeling of self-organizing swarms of UAVs with the ability of collective decision-making fairly ensures overcoming uncertainties and errors of the entire system; also, failures or loss of individual UAVs are covered up without compromising the swarm mission.

The dynamic uncertain environment and complex tasks determine that the UAV system is bound to develop towards clustering, autonomy, and intelligence. In this context, the work [15] presents a comprehensive survey of UAV swarm intelligence from the hierarchical framework perspective. Particularly, classification of UAV swarm intelligence into the following layers are given: decision making layer; path planning layer; control layer; communication layer, and application layer.

II. Mathematical Preliminaries And Models For Obtaining Information Full Exchange

Aimed at targeting tasks performance, also at operational management of swarms of UAVs, we have already introduced and approved decentralized and fault-tolerant optimal schemes and communication algorithms [5]. Taking into account the fact that swarms operate in a computational and resource limited environment, lightweight algorithms resilient against network ad-hoc reconfiguration have been

designed and implemented accordingly thus ensuring the overall system operability against any single point of failure. Fulfillment of the above requirements implied involvement of gossip algorithms along with the design and development of appropriate schemes providing the uniform distribution of computing power among the nodes of the system. For the swarms of UAVs, it is also important for each of the single UAV to have only a localized view of the system and be able to communicate only with the specified subset of logically linked UAVs.

Definition. A Knödel graph with $n \geq 2$ vertices (n is even) and $1 \leq \Delta \leq \lfloor \log n \rfloor$ degrees is denoted by $W_{\Delta,n}$, where vertices are pairs of type (i,j), $i = 1,2;\ 0 \leq j \leq n/2-1$. For each of j and i, $0 \leq j \leq n/2-1$, $i = 1,\ldots,\Delta$, there exist a 1-weighted edge between $(1,j)$ and $(2, j + 2^{l-1} - 1 \bmod n/2)$ nodes.

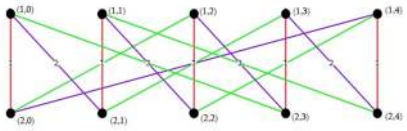

Figure 1. A Knödel graph with $n \geq 2$ vertices.

Definition 1. Two weighted graphs, G and H, are called isomorphic, if there exist a one-to-one correspondent mapping between the set of their nodes, $f: V(G) \to V(H)$, such that any two vertices u and v are adjacent in the graph G if and only if the vertices $f(u)$ and $f(v)$ are adjacent in H and $t_G(u,v) = t_H(f(u), f(v))$.

Local Interchange Operation.
Let $E_v(G)$ denotes the set of edges incident to the given vertex v, and an edge e is given with one of its two incident vertices, v. The following subsets of the set $E_v(G)$ are considered as a result of application of the "local interchange" method: "permutation of greater valued nodes" or "permutation of lesser valued nodes".

Wheel gossip graphs [6]

Definition 2. The operation of "permutation of greater valued nodes", $P^+(e)$, on the edge connecting the vertices u and v, is called the modification of G resulting in permutation of edges incident to e, as follows [6]:
$E_u(P^+(e)G) = \rho_u^-(e,G) \cup \rho_v^+(e,G)$,
$E_v(P^+(e)G) = \rho_v^-(e,G) \cup \rho_u^+(e,G)$.

Applications.

NOHO gossip graphs.
Let $A_l^- = \{ P-(e) \mid tG(e) < l \}$.

By applying the A_2^- operation on the Knödel graph, we obtain NOHO gossip graphs with minimum time $\lfloor \log n \rfloor$ (open problem by A. Liestman) [11].

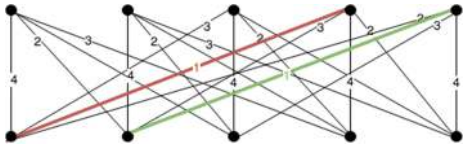

Figure 2. NOHO gossip graph.

Minimal Gossip Graphs.
New method for construction of minimal gossip graphs ($f(n) = 2n-4$, $T = 2\lfloor \log n \rfloor - 3$) for a fixed quantity of vertices belonging to certain limited interval.

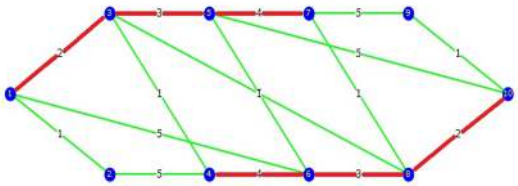

Figure 3. Gossip graph with minimal calls.

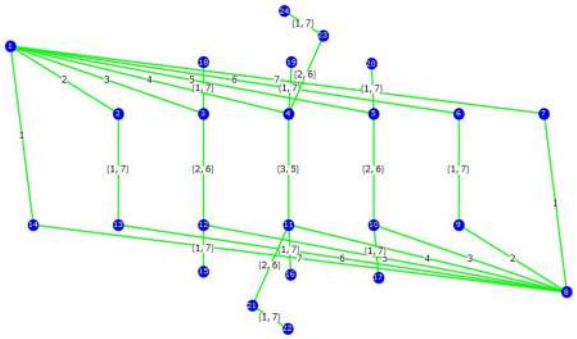

Figure 4. Gossip graph with minimal time and minimal calls.

$n \leq 2^{\frac{k}{2}+1}$, if k is even,
$n \leq 3 \times 2^{\frac{k-1}{2}}$, if k is odd,

$T' = 2\lfloor \log n \rfloor - 2$, if k is even,
$T' = 2\lfloor \log(n/3) \rfloor + 1$, if k is odd.
In case of odd base measure [10], the minimal gossip is obtained for the following intervals: {{5-6}, {9-12}, {17-24}, {33-48}, {65-96}, {129-192}, {257-384}, {513-768} ...}

Fault-tolerant Gossip Graphs.
A new method for constructing fault-tolerant gossip graphs based on Wheel graphs is introduced. The method optimizes the upper bound $\tau(n,k)$ for certain less values of k, $\tau(n,k) \leq 2nk/3 + O(n)$.

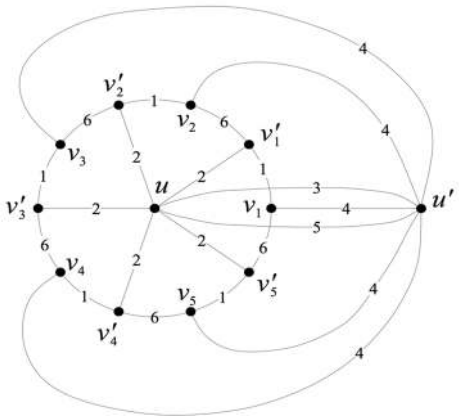

Figure 5. A wheel graph with an even number of vertices ($n = 12$).

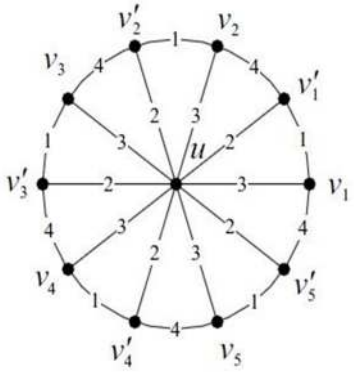

Figure 6. A wheel graph with an odd number of vertices ($n = 11$).

In order to mitigate risks of node or channel loss during the gossip process (see [14] for the complete list of possible failures bounded with a certain crash types in non-adaptive channels), a research was conducted to find a sequence of calls with a minimal length that will guarantee the information full exchange between the system nodes, even if at most k calls (arbitrarily) fail in that process.

The sequence of calls with minimal length denoted by $\tau(n,k)$ and satisfying the above conditions depends on the number of the system nodes and the required level of fault-tolerance. Up to date, this is an open problem, and there exist only lower and upper bounds for $\tau(n,k)$. The latest results are the following: $\tau(n,k) \leq \frac{n}{2} log_2 n + nk/2$, for n being a power 2 number, and $\tau(n,k) \leq 2n\lfloor log_2 n \rfloor + n\lceil \frac{k-1}{2} \rceil$, otherwise.

Hypothesis: In the fault-tolerant gossip graphs, the upper bound on the minimum required number of calls and minimum number of ticks are:

$$\tau(n,k) \leq n[log\, n]/2 + nk/2, \text{ and}$$
$$T(n,k) = [log\, n] + k, \text{ respectively.}$$

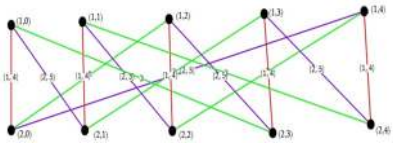

Figure 7. k-fault-tolerant gossip graph with minimal time.

Construction of 1-fault-tolernat gossip graph ($k = 1$) over a Knödel graph. Given a Knödel graph, a gossip graph ($k = 0$) and a 1-fault-tolenant graph ($k = 1$) is constructed according to the Figure8 given below.

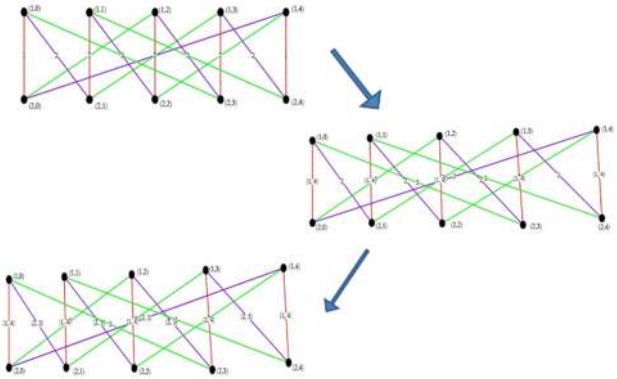

Figure 8. Iterative construction of the k-fault-tolerant graph.

Definition 3. An edge-permuted Knödel graph with $n \geq 2$ vertices (n is even) and $1 \leq \Delta \leq \lfloor \log n \rfloor$degrees is denoted by $M_{\Delta,n}(p)$, where vertices present a set of pairs (i,j); $i = 1,2$ and $0 \leq j \leq \frac{n}{2} - 1$. For each of the j and $l = 1,\ldots,\Delta$, there exist an 1-weighted edge between $(1,j)$ and $(2,(\, j + 2\text{^}\{p + l - 1\} - 1)\ mod\ n/2)$ vertices, where $p = 0,\ldots,\Delta - 1$ is an integer selected for the given graph.

Edge-permuted Knödel graphs.

Theorem. The graph

$$G = M_{\lfloor log n \rfloor, n(p)} + M_{1,n(p)}$$

is a complete gossip graph for any $n \neq 2^k$ and $p = 0,\ldots,\Delta - 1$. [6].

$G = M_{\lfloor log\, n \rfloor, n(p)} + M_{1,n(p)}$ is not isomorphic to the $W_{\lfloor log\, n \rfloor, n} + W_{1,n}$ graph (excepted for $n = 2^k - 2$) even though both are gossip graphs.

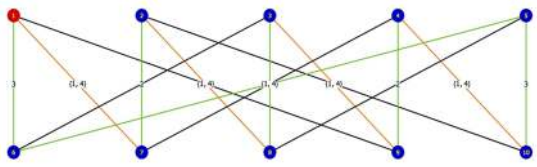

Figure 9. Edge-permuted Knödel graph.

Within the scope of this research, our developed methods and relevant algorithms have been involved aimed at construction of information dissemination and full exchange schemes. Selected schemes are of a required fault-tolerance [5].

Below is the set of methods and logical schemes contributing to information full exchange between the logically linked swarm UAVs.

- For the gossip process, a method has been introduced enabling the construction of new topologies equivalent in terms of the two main characteristics of gossip schemes

(number of calls and ticks). These topologies are not isomorphic to known models [12-13].

- Distinct and non-isomorphic modifications of known communication models have been obtained preserving the original values of the main characteristics typical to gossip schemes. These models have been verified to be appropriate for relevant swarm architectures [1-2].
- Gossip schemes of the required level of fault-tolerance have been developed enabling the information full exchange between the swarm UAVs provided the minimum number of calls and ticks [1].
- Algorithms for bypassing static barriers have been introduced based on our theoretical results obtained in this direction [3]. The motion of UAVs is carried out along quasi-random trajectories within allocated subspaces according to the Euler walk rotor-router model [4].
- Fault-tolerance schemes (algorithms) have been developed to neutralize probable disturbances of communication during the exchange of information (captured images being "successful" steps of displacement in a rotor-router model). Our results obtained in this area have been already summarized in [5]. In the event of separate UAV crash, the swarm will be dynamically reconfigured/reshaped to another group with an equivalent structure that meets the optimal requirements thus ensuring the continuity of the mission.
- Methods and algorithms enabling replenishment of UAVs are introduced to improve the quality of the overall image of the area under investigation [6].
- Image processing algorithms, such as: decoding, collective image recognition, synthesis, 2D (3D later on) image reproduction with the ability to visualize, have been developed accordingly.
- Multispectral gossip/broadcast schemes with required optimal characteristics implementing information full exchange between UAVs have been developed using Knodel, circulant and wheel graph topologies. Data warehouse has been constructed accordingly.
- Algorithms of k-fault-tolerance have been developed using our <interchange operation [12-13] aimed at generation of ad-hoc structures with equivalent characteristics, also to neutralize probable disturbances of communication during the exchange of information.
- Algorithms for the UAV swarm replenishment in the event of individual UAV crash, also methods for redistribution of logical links between the nodes of dynamically reconfigured/reshaped swarm, have been introduced and approved accordingly.
- The motion of UAVs within the swarm, as well as the information full exchange between the swarm UAVs are implemented in the universal rotor-router model and can stand for its novel interpretation. The proposed solution promotes certain premises for the design of the swarm hardware and software by embedding our solution with unified low-cost components with very basic tasks to be performed [4].
- During the research and aimed the verification of the results obtained, our "Graph Plotter" package was used [7]. Besides, newly parallel algorithms have been introduced accordingly during the overall software system development [8-9].

The entire system software has been implemented with the help of the following computing infrastructures which are at the disposal of the Group: ArmGrid Computing Complex (368 core Intel Quad Core Xeon E5420 2.5 Ghz, RAM 8 GB); Cloud Environment IaaS (Infrastructure as a Service) (about 400 core) and access to virtual cards (Nvidia V100).

III. Data and Transfer Security Solutions

The wireless nature of UAV swarms implies factors and issues such as: battery power, bandwidth, constraints, mobility, security, etc., which heavily affect the selection of cryptographic algorithms and key management schemes. Taking into account the amount of data to be transmitted and the reality that devices involved in communication cannot perform computationally-intense operations, use of symmetric key cryptography has been suggested. Besides, the following approaches have been selected aimed at provision of data and transfer security.

- Encryption/decryption of captured images are performed using AES-256.
- UAV's within ad-hoc networks are authenticated by sending/receiving secret tokens hashed with individual portions of secret keys distributed according to the specified secret sharing scheme.
- For every UAV in the swarm, a point on an elliptic curve is selected and secured accordingly. An elliptic curve E over the real numbers R is defined by a Weierstrass equation, $E: y^2 + a_1xy + a_3xy + a_3y = x^3 + a_2x^2 + a_4x + a_5$ with coefficients $a_1, a_2, a_3, a_4, a_5 \in N, \Delta \neq 0$. The set of points on the curve is: $E(L) = \{(x, y) \in R \times R: y^2 + a_1xy + a_3xy + a_3y - x^3 - a_2x^2 - a_4x - a_5 = 0)\} \cup \{0\}$ with point of infinity or 0 point.
- Authentication of UAVs aimed at assertion of their membership to the relevant configuration is performed via efficient computation of the certain simplification of a non-singular curve equation according to well-known principles of threshold cryptography. Using AES-256 implies embedding ECC-521 for equivalent secrecy.
- A Cryptographic Key Management scheme operates and distributes keys in order to ensure only legitimate UAVs in the swarm hold valid keys and can access the swarm data during gossiping sessions.
- Group Key Secrecy scheme is suggested to guarantee that it is computationally infeasible for an adversary to discover the swarm cryptographic keys and deduce secret tokens.
- Group Access Control designed properly manages permission or denial of membership into swarms.
- In order to preserve the secrecy of the swarm data, Group keys are updated upon certain events such as a certain UAV joining or leaving the swarm.

Acknowledgment

This work was supported by the RA Science Committee, in the frames of the research project 20TTAT-RBe016.

REFERENCES

[1] V. Hovnanyan, S. Poghosyan and V. Poghosyan, "Method of local interchange to investigate Gossip problems," *Transactions of IIAP of NAS RA, Mathematical Problems of Computer Science*, vol. 40, pp. 5-12, 2013.

[2] V. Hovnanyan, S. Poghosyan and V. Poghosyan, "Method of local interchange to investigate Gossip problem: part 2," *Transactions of IIAP of NAS RA, Mathematical Problems of Computer Science*, vol. 41, pp. 15-22, 2014.

[3] V. Hovnanyan, S. Poghosyan and V. Poghosyan, "Gossiping Properties of the Edge Permuted Knodel Graphs," C*SIT, IEEE conference proceedings*, pp. 17-20, 2017.

[4] V.S. Poghosyan and V.B. Priezzhev, "Euler tours and unicycles in the rotor-router model", *J. Stat. Mech.* P06003, 2014.

[5] V. Hovnanyan, S. Poghosyan and V. Poghosyan, "New Methods of Construction of Fault-Tolerant Gossip Graphs," CSIT, pp. 75-78, 2013.

[6] V. Hovnanyan, S. Poghosyan and V. Poghosyan, "Fault-tolerant gossip graphs based on Wheel graphs," *Transactions of IIAP of NAS RA, Mathematical Problems of Computer Science*, vol. 42, pp. 43-53, 2014.

[7] V. Hovnanyan, V. Poghosyan and S. Poghosyan, "Graph Plotter: a Software Tool for the Investigation of Fault-tolerant Gossip Graphs," CSIT, pp. 20-22, 2013.

[8] V.S. Poghosyan, S.S. Poghosyan and H.E. Nahapetyan, The Investigation of Models of Self-Organized Systems by Parallel Programming Methods Based on the Example of an Abelian Sandpile Model, *Proc. CSIT Conference 2013*, Yerevan Armenia, Sept. 23-27, pp. 260-262, 2013.

[9] Hayk E. Nahapetyan, Suren S. Poghosyan, Vahagn S. Poghosyan and Yuri H. Shoukourian, "The Parallel Simulation Method for d-dimensional Abelian Sandpile Automata", *Mathematical Problems of Computer Science* 46, pp. 117-125, 2016.

[10] V. Hovnanyan, S. Poghosyan and V. Poghosyan, "Fault-tolerant Gossip Graphs Based on Wheel Graphs", T*ransactions of IIAP of NAS RA, Mathematical Problems of Computer Science*, vol. 42, pp. 43-53, 2014.

[11] V. Hovnanyan, S. Poghosyan and V. Poghosyan, "Open problems in gossip/broadcast schemes and the possible application of the method of local interchange", *IEEE conference proceedings*, CSIT, pp. 73-78, 2015.

[12] V. Hovnanyan, "Gossiping Properties of the Modified Knodel Graphs", Transactions of IIAP of NAS RA, *Mathematical Problems of Computer Science*, vol. 46, 126-131, 2016.

[13] V. Hovnanyan, S. Poghosyan and V. Poghosyan, "Gossiping Properties of the Edge-Permuted Knodel Graphs", *CSIT*, pp. 17-20, 2017, IEEE conference proceedings

[14] A. Pelc, "Fault-tolerant broadcasting and gossiping in communication networks", Networks vol. 28, 1996.

[15] Y. Zhou, B. Rao and W. Wang, "UAV Swarm Intelligence: Recent Advances and Future Trends," in IEEE Access, vol. 8, pp. 183856-183878, 2020.