

[Notice] The original paper, **Advanced Drone Swarm Security by Using Blockchain Governance Game**, has been published in the *Mathematics* (scan the QR code) and use the following citation of the original paper if you want to reference this paper:

Song-Kyoo Kim, "Advanced Drone Swarm Security by Using Blockchain Governance Game", *Mathematics* **10**:18 (2022), 3338.

The official URL: <https://www.mdpi.com/2227-7390/10/18/3338>
DOI: 10.3390/math10183338



Advanced Drone Swarm Security by Using Blockchain Governance Game

SONG-KYOO (AMANG) KIM

ABSTRACT

This research contributes to the security design of an advanced smart drone swarm network based on a variant of the *Blockchain Governance Game* (BGG), which is the theoretical game model to predict the moments of security actions before attacks, and the *Strategic Alliance for Blockchain Governance Game* (SABGG), which is one of the BGG variants which has been adapted to construct the best strategies to take preliminary actions based on strategic alliance for protecting smart drones in a blockchain-based swarm network. Smart drones are artificial intelligence (AI)-enabled drones which are capable of being operated autonomously without having any command center. Analytically tractable solutions from the SABGG allow us to estimate the moments of taking preliminary actions by delivering the optimal accountability of drones for preventing attacks. This advanced secured swarm network within AI-enabled drones is designed by adapting the SABGG model. This research helps users to develop a new network-architecture-level security of a smart drone swarm which is based on a decentralized network.

Keywords: Drone, swarm, Blockchain Governance Game; artificial intelligence, mixed game; stochastic model; fluctuation theory; 51 percent attack

I. INTRODUCTION

Drones occupy an essential place in both military and civilian applications for various roles including criminal investigations, public safety organizations, transportation management facilities, and surveillance forces [1]. Because of dynamic mobility, quick reaction and easy deployment, drones offer new possibilities for different applications with affordable expense [2]. A drone swarm is multiple drones being used at once and drones in a swarm communicate and collaborate, making collective decisions of collective actions. In a militarized drone swarm, instead of 10 or 100

distinct drones, the swarm forms a single, integrated weapon system guided by some form of artificial intelligence [3]. The Blockchain Governance Game (BGG) has been designed as a stochastic game model with the fluctuation and the mixed strategy game for analyzing the network to provide the decision making moment for taking preliminary security actions before attacks. The model is targeted to prevent blockchain based attacks (i.e., the 51 percent attack) and keeps the network decentralized. Atypical case which an attacker tries to build an alternative blockchain (blockchain forks) faster than regular miners [18].

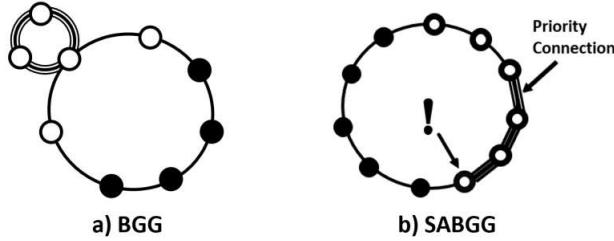


Fig 2. BGG vs. SABGG [18, 21]

II. STOCHASTIC GAME FOR ASDS SECURITY FRAMEWORK

The proposed ASDS network structure is considered and the drones in a swarm are connected each other and a swarm is hooked up as single Blockchain network (see Fig. 2). Drones in a swarm are fully connected but these may not connected with a command center (or a control center). This drone swarm could execute thier command artificially and independently even with disconection with a command center. Each drone randomly generates unique data (e.g., GPS cordinates, motor RPM values) and broadcast these data to other drones (which is equavalent with transaction in a blockchain network). Each drone generates the value based on its mechanical action and the generated values are sharing with all other drones in a swarm.

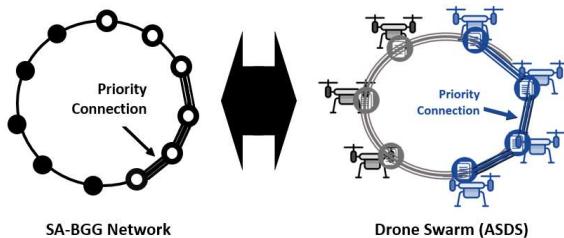


Fig 2. Adapting SA-BGG for the ASDS network architecture

To apply the SABGG into the ASDS network structure, the antagonistic game of two players (called "A" and "H") are introduced to describe the Blockchain network in a drone swarm as a defender and an attacker. The joint functional of the Blockchain network model with the strategic alliance is as follows:

$$\Phi_{\lceil \frac{M}{2} \rceil}(\xi, g_0, g_1, b, z_0, z_1) \quad (2.16)$$

$$= \mathbb{E} \left[\xi^\nu \cdot g_0^{A_{\nu-1}} \cdot g_1^{A_\nu} \cdot b^{A_\nu - B} \cdot z_0^{H_{\mu-1}} \cdot z_1^{H_\mu} \mathbf{1}_{\{\nu < \nu_2 < \mu\}} \right],$$

$$\|\xi\| \leq 1, \|g_0\| \leq 1, \|g_1\| \leq 1, \|b\| \leq 1, \|z_0\| \leq 1, \|z_1\| \leq 1. \quad (2.17)$$

where M indicates the total number of nodes (or ledgers) in the swarm network for each drone (see Fig. 2). The Theorem of SABGG establishes an explicit formula $\Phi_{[\frac{M}{2}]}$ from (2.7)-(2.10). Based on the theorem [25], the functional $\Phi_{[\frac{M}{2}]}$ of the process of (2.16) satisfies following expression:

$$\Phi_{[\frac{M}{2}]}(\xi, g_0, g_1, z_0, z_1) = \mathcal{D}_{(q,r,s)}^{([\frac{M}{2}], [\frac{M}{2}], [\frac{M}{2}])} \Lambda, \quad (2.18)$$

where

$$\Lambda = \sigma \cdot \Gamma \left(\frac{1 - \Gamma^1}{1 - \Gamma} \right) \left(\gamma_0^1 - \gamma_0 + \frac{\zeta \Theta_0}{1 - \zeta \Theta} (\gamma^1 - \gamma) \right), \quad (2.19)$$

and

$$\Theta := \gamma(g_0 g_1 bqr, z_0 z_1 s), \quad (2.20)$$

$$\Theta_0 := \gamma_0(g_0 g_1 bqr, z_0 z_1 s), \quad (2.21)$$

$$\gamma := \gamma(g_1 bq, z_1), \quad (2.22)$$

$$\gamma_0 := \gamma_0(g_1 bq, z_1), \quad (2.23)$$

$$\gamma^1 := \gamma(g_1 b, z_1), \quad (2.24)$$

$$\gamma_0^1 := \gamma_0(g_1 b, z_1), \quad (2.25)$$

$$\Gamma := \gamma(br, s), \quad (2.26)$$

$$\Gamma^1 := \gamma(r, 1), \quad (2.27)$$

$$\sigma := \mathbb{E}[b^{-B}]. \quad (2.28)$$

From (2.13)-(2.14), we can find the PGFs (probability generating functions) of the *exit index* ν :

$$\mathbb{E}[\xi^\nu] = \Phi_{[\frac{M}{2}]}(\xi, 1, 1, 1, 1) \quad (2.32)$$

Let us consider a two-person mixed strategy game, and player H (i.e., a drone swarm) is the person who has two strategies at the observation moment, one step before attackers complete to generate alternative chains with dishonest transactions. In this case, the cost will be not only all drones in a swarm but also the alliance costs. The normal form of games is as follows:

$$\text{. Players: } \mathbf{N} = \{A, H\}, \quad (2.37)$$

$$\text{. Strategy sets: }$$

$$\begin{aligned} \mathbf{s}_a &= \{"NotBurst", "Burst"\}, \\ \mathbf{s}_h &= \{"Regular", "Safety"\}. \end{aligned}$$

Based on the above conditions, the general cost matrix at the prior time to be burst $\tau_{\nu-1}$ could be composed as follows:

Table 1. Cost matrix

	$NotBurst (1 - q(s_h))$	$Burst (q(s_h))$
<i>Regular</i>	0	V
<i>Safety</i>	c_b	$c_b + V$

where $q(s_h)$ is the probability of bursting blockchain network (i.e., an attacker wins the game) and it depends on the strategic decision of player H:

$$q(s_h) = \begin{cases} \mathbb{E}\left[\mathbf{1}_{\{A_\nu \geq \frac{M}{2}\}}\right], & s_h = \{\text{Regular}\}, \\ \mathbb{E}\left[\mathbf{1}_{\{A_\nu - B \geq \frac{M}{2}\}}\right], & s_h = \{\text{Safety}\}, \end{cases} \quad (2.38)$$

and the alliance (i.e., "Safety" strategy of player H) cost should be less than the cost of other strategies. Otherwise, player H does not have to spend the cost of the strategic alliance with genuine drones. Recalling from (2.38), the probability of bursting a Blockchain network (i.e., an attacker wins the game) under the memoryless properties becomes the Poisson compound process:

$$q(s_h) = \begin{cases} \sum_{k>\frac{N}{2}} \mathbb{E}\left[\mathbf{1}_{\{A_\nu=k\}}\right], & s_h = \{\text{Regular}\}, \\ \mathbb{E}\left[\mathbb{E}\left[\sum_{k>\frac{N}{2}+B} \mathbb{E}\left[\mathbf{1}_{\{A_\nu=k\}}\right] \middle| B\right]\right], & s_h = \{\text{Safety}\}, \end{cases} \quad (2.39)$$

where

$$\mathbb{E}\left[\mathbf{1}_{\{A_\nu=k\}}\right] = \mathbb{E}\left[\mathbb{E}\left[\frac{\lambda_a \tau_\nu}{k!} \cdot e^{-\lambda_a \tau_\nu} \middle| \tau_\nu\right]\right]. \quad (2.40)$$

III. THE ASDS OPTIMIZATION PRACTICE

A network security in an ASDS network is considered in this subsection. The strategy for protecting the ASDS is for priority connection with neighbor drones to give the less chance that an attacker catches blocks with false control requests. The example in this paper is targeting 20 drones in single swarm and each estimated drone value is around 1,500 USD in the swarm (see Table II).

Name	Value	Description
M	20 [Drones]	Total number of the nodes in a drone swarm
V	$1,500 \text{ [USD/Drone]} \cdot M \text{ [Drone]}$	Total value of a Blockchain enabled swarm
$c(\varrho)$	$= 3\left(\frac{M}{2} - 1\right) \cdot \varrho \text{ [USD]}$	Cost for reserving nodes to avoid attacks per each car
$\mathbb{E}[\nu]$	3 [Trial]	Total number of blocks that changed by an attacker at $\tau_0 (= 0)$
B	—	Number of accepted allies at τ_ν

Table II. Initial conditions for the cost function

Based on the above conditions, the LP (Linear Programming) model could be described as follows from (2.43)-(2.46):

Objective
minimizing $G = \mathfrak{G}(\varrho)_{\text{Total}}$ (3.30)

Subject to

$$n \geq \frac{c(\varrho)}{V \cdot q^0 - c(\varrho)}; \quad (3.31)$$

From (2.46), the total cost $\mathfrak{S}(\varrho)_{\text{Total}}$ is as follows:

$$\mathfrak{S}(\varrho)_{\text{Total}} = (c(\varrho)(1 - q_\eta^1) + (c(\varrho) + V)q^1(\varrho))p_{A_{-1}} \quad (3.32)$$

$$+ V \cdot q^0(1 - p_{A_{-1}})$$

where

$$\begin{aligned} p_{A_{-1}} &= \mathbf{P}\left\{A_{\nu-1} < \frac{M}{2}\right\} \\ &\simeq \mathbf{P}\left\{A_\nu < \frac{M}{2} - \lambda_a \tilde{\delta}\right\} \\ &= \sum_{k=0}^{\left\{\frac{M}{2} - \lambda_a \tilde{\delta}\right\}} \left(\frac{\left\{\lambda_a (\tilde{\delta}_0 + \mathbb{E}[\nu-1]\tilde{\delta})\right\}^k}{k!} \cdot e^{-\lambda_a (\tilde{\delta}_0 + \mathbb{E}[\nu-1]\tilde{\delta})} \right), \end{aligned} \quad (3.33)$$

$$q^0 \simeq 1 - \sum_{k=0}^{\frac{M}{2}} \left(\frac{\left\{\lambda_a (\tilde{\delta}_0 + \mathbb{E}[\nu-1]\tilde{\delta})\right\}^k}{k!} \cdot e^{-\lambda_a (\tilde{\delta}_0 + \mathbb{E}[\nu-1]\tilde{\delta})} \right) \quad (3.34)$$

$$q^1(\varrho) = \sum_{j=0}^{\frac{M}{2}-1} \sum_{\{k \geq \frac{M}{2}+j\}} \left(\frac{\lambda_a (\tilde{\delta}_0 + \mathbb{E}[\nu-1]\tilde{\delta})}{k!} \cdot e^{-\lambda_a (\tilde{\delta}_0 + \mathbb{E}[\nu-1]\tilde{\delta})} \right) P_j, \quad (3.35)$$

$$P_j = \binom{\frac{M}{2}-1}{j} \varrho^j (1-\varrho)^{\frac{M}{2}-1-j}. \quad (3.36)$$

The total cost $\mathfrak{S}(\varrho)_{\text{Total}}$ could be minimized by given ϱ is the optimal value of the reserved nodes. The below illustration in Fig. 3 is atypical graph of an optimal result by using the SABGG based ASDS network based on the given conditions in Table II.

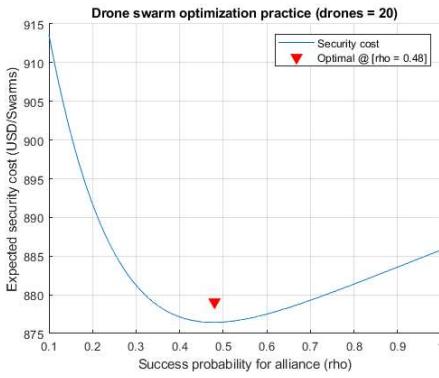


Fig. 3. Optimization Example for the ASDS

IV. CONCLUSION

An advanced secure drone swarm network architecture protects a drone swarm from an attacker by adapting a blockchain governance game variant. The~Strategic Alliance for Blockchain Governance Game (SABGG) which is an analytically proven game model has been applied as a blockchain governance game variant. The SABGG has

been adapted for a decentralized network to improve drone swarm security. The~special SABGG case demonstrates how the theoretical model is actually implemented for smart drone security. Although~this research is still theoretical and there are several steps remaining for actual implementation into real drones, the practical case demonstrates how an SABGG network could be implemented for smart drone securities and its feasibility. This paper is the first piece of research that applies an SABGG model into a swarm network architecture security. The~advanced smart drone swarm network is the successor of blockchain-governance-game-based IoT security applications, particularly in the intelligent military domain. The managerial aspects and actual implementations of smart drone operations could be the next step. Additionally, expending the domains for applying the BGG and its variants could definitely be another direction of future research.

REREFENCES

- [1] Vergouw, B.; Nagel, H.; Bondt, G.; Custers, B. Drone technology: Types, payloads, applications, frequency spectrum issues and future developments. In *The Future of Drone Use*; TMC Asser Press: The Hague, The Netherlands, 2016; pp. 21-45.
- [2] Y. Ko, J. Kim and et al. (2021), Drone Secure Communication Protocol for Future Sensitive Applications in Military Zone, *Sensors* 21:6, 2057.
- [3] Z. Kallenborn (2021), Israel's Drone Swarm Over Gaza Should Worry Everyone, [Online] <https://www.defenseone.com/ideas/2021/07/israels-drone-swarm-over-gaza-should-worry-everyone/183156/>
- [4] US Army (2021), Army advances learning capabilities of drone swarms, U.S. Army CCDC Army Research Laboratory Public Affairs, August 10, 2020, [Online] https://www.army.mil/article/237978/army_advances_learning_capabilities_of_drone_swarms
- [5] D. Hambling (2021), What Are Drone Swarms And Why Does Every Military Suddenly Want One?, *Forbes*, March 1, 2021, [Online] <https://www.forbes.com/sites/davidhambling/2021/03/01/what-are-drone-swarms-and-why-does-everyone-suddenly-want-one/>
- [6] Z. Kallenborn (2021), Meet the future weapon of mass destruction, the drone swarm, *Bulletin of the Atomic Scientists*, April 5, 2021, [Online] <https://thebulletin.org/2021/04/meet-the-future-weapon-of-mass-destruction-the-drone-swarm/>
- [7] DOD (2017), Department of Defense Announces Successful Micro-Drone Demonstration, US Dep. of Defense, January 9, 2017, [Online] <https://www.defense.gov/>
- [8] Naqvi, S.A.; Hassan, S.A.; Pervaiz, H.; Ni, Q. Drone-aided communication as a key enabler for 5G and resilient public safety networks. *IEEE Commun. Mag.* 2018, 56, 36-42.
- [9] Choudhary, G.; Sharma, V.; You, I. Sustainable and secure trajectories for the military Internet of Drones (IoD) through an efficient Medium Access Control (MAC) protocol. *Comput. Electr. Eng.* 2019, 74, 59-73.
- [10] He, D.; Chan, S.; Guizani, M. Communication security of unmanned aerial vehicles. *IEEE Wirel. Commun.* 2016, 24, 134-139.
- [11] V. Strobel, E. C. Ferrer and M. Dorigo (2018), Managing Byzantine Robots via Blockchain Technology in a Swarm Robotics Collective Decision Making Scenario. In Proceedings of the 17th International Conference on Autonomous Agents and MultiAgent Systems (AAMAS 18). International Foundation for Autonomous Agents and Multiagent Systems, Richland, SC, 541-549.
- [12] V. Strobel, E. C. Ferrer and M. Dorigo (2020), Blockchain Technology Secures Robot Swarms: A Comparison of Consensus Protocols and Their Resilience to Byzantine Robots, 7, pp. 1-22.
- [13] A. G. Millard, J. Timmis and A. F. T. Winfield (2014), Towards Exogenous Fault Detection in Swarm Robotic Systems, 14th Annual Conference, TAROS 2013, Oxford, UK, August 28--30, 2013, pp. 429-430.
- [14] Restuccia, F. Blockchain for the Internet of Things: Present and Future. Available online: <https://arxiv.org/abs/1903.07448> (accessed on 1 May 2019).
- [15] Jesus, E.F.; Chicarino, V.R.L.; de Albuquerque, C.V.N.; Rocha, A.A.D.A. Survey of How to Use Blockchain to Secure Internet of Things and the Stalker Attack. *Secur. Commun. Netw.* 2018, 2018, 9675050.
- [16] S. Nakamoto. 2008. Bitcoin: A peer-to-peer electronic cash system. (2008). <https://bitcoin.org/bitcoin.pdf>

- [17] G. Wood. 2014. Ethereum: A secure decentralised generalised transaction ledger. Ethereum project yellow paper. (2014). <http://gavwood.com/paper.pdf>
- [18] S.-K. Kim, Blockchain Governance Game. Comput. Ind. Eng. 2019, 136, 373-380.
- [19] V. Buterin. 2014. A next-generation smart contract and decentralized application platform. Ethereum project white paper. (2014). <https://github.com/ethereum/wiki/wiki/White-Paper>
- [20] C. Pincioli, V. Trianni and et al. (2012), ARGoS: a modular, parallel, multi-engine simulator for multi-robot systems, Swarm Intelligence, 6, pp. 271--295.
- [21] S.-K. Kim, Strategic Alliance for Blockchain Governance Game. Probab. Eng. Inf. Sci. 2020, pp. 1-17.
- [22] S. Micali, M. O. Rabin, Vadhan, S. P., Verifiable random functions, Proceedings of the 40th IEEE Symposium on Foundations of Computer Science, pp. 120-130, 1999.
- [23] S. Goldberg, L. Reyzin and et al., Verifiable Random Functions, IETF, [online] <https://datatracker.ietf.org/doc/draft-irtf-cfrgvr/09/>, 2021.
- [24] L. Guerrero-Bonilla, A. Prorok and V. Kumar (2017). Formations for resilient robot teams. IEEE Robot. Autom. Lett. 2, 841?848.
- [25] D. Saldana, A. Prorok and et al. (2017). Resilient consensus for time-varying networks of dynamic agents, in Proceedings of the American Control Conference (ACC) (Piscataway, NJ: IEEE Press), 252-258.
- [26] H. J. LeBlanc, H. Zhang, H. and et al. (2013), Resilient asymptotic consensus in robust networks. IEEE J. Select. Areas Commun. 31, pp. 766-781.
- [27] K. Saulnier, D. Saldana and et al. (2017), Resilient flocking for mobile robot teams. IEEE Robot. Autom. Lett. 2, pp. 1039-1046.
- [25] J. H. Dshalalow, First excess level process, Advances in Queueing, CRC Press, Boca Raton, FL, pp 244-261, 1995.