# Coagulation attacks over networked UAVs: concept, challenges, and research aspects

Vishal Sharma*, Ravinder Kumar†, Kathiravan Srinivasan‡, Dushantha Nalin K. Jayakody§
*Department of Information Security Engineering, Soonchunhyang University, Asan-si 31538, Republic of Korea
Email: vishal_sharma2012@hotmail.com
†Computer Science and Engineering Department, Thapar University, Patiala, Punjab, India
Email: ravinder@thapar.edu
‡Department of Computer Science and Information Engineering, National Ilan University, Yilan County, Taiwan (R.O.C)
Email: kathiravan@niu.edu.tw
§Department of Software Engineering, Institute of Cybernetics, National Research Tomsk Polytechnic University, Russia
Email: nalin.jayakody@ieee.org

***Abstract*—Unmanned Aerial Vehicles (UAVs) have grasped an important role in the modern day networking. A lot of applications are being developed using aerial vehicles as a pivot. These vehicles provide a vast range of support to modern day networks. Modern computing applications such as Urban Computing, Internet of Things, Ubiquitous Computing, and the Internet for All have sought applications of UAVs to attain complex tasks. However, securing aerial vehicles in a network is not an easy task because of the difference in communication standards and range of applicability. Aerial nodes are prone to various types of attack in a network such as Sybil attack, wormhole attack, sinkhole attack, or impersonation attack. These attacks lead to a large number of vulnerabilities causing fatal incidents. A new attack is introduced in this paper termed as "Coagulation Attack". This term is derived from the clotting properties of fluids. This paper introduces the concept, issues, challenges, and research aspects of coagulation attack. A simulation study is also presented that shows the impact of such attacks over networked UAVs.**

***Index Terms*—Coagulation Attack, UAVs, Ad Hoc network.**

## I. Introduction

Communication networks have been the backbone for data sharing. These networks have seen tremendous advancement over the last decade. Modern day networks have extended their limits and started using varied nodes for data transmissions. One of such examples is the use of Unmanned Aerial Vehicles (UAVs) as network nodes for enhanced connectivity [1]. UAVs have gained a lot of attention over the years. These vehicles are gaining popularity in their use as network nodes. Extending the applications of existing network is their primary goal. Use of multiple UAVs in cooperative mode have further introduced a new network formation that behaves as traditional networks, but, with a capability of operating autonomously as well as manually.

Modern computing applications such as Urban Computing, Internet of Things, Ubiquitous Computing, and the Internet for All have sought applications of UAVs to attain complex tasks [2] [3] [4]. However, with their rapid use, certain issues are yet to be handled for robust and fault-tolerant networking. A lot of network attacks have been discussed over the years, and several security measures have been taken against them. Vulnerability assessment can help in identification of all possible threats to an aerial network [5] [6] [7]. Security has always been a concern for UAVs. Trustworthy and secure communication system is the major demand of UAV systems [8] [9] [10].

Over the years, the concept of attacks in UAVs has been studied as cyber-physical systems and various case studies have been presented to it. Such scenarios treat UAVs equivalent to cyber systems and analyze them for various possible attacks and countermeasures [11] [12]. Cyber attacks can heavily impact the operations of a regular aerial vehicle by affecting its autopilot systems. Vulnerability in autopilot systems can cause devastating effects, which may result in fatal incidents [13]. False data injections are the other major aspects of cyber attacks [14]. One of the crucial issues with cyber attacks can be the impact on drone delivery system. Such attacks can damage the entire business model as well as transform aerial vehicles into potential attackers [15].

This paper introduces a new attack which can prove fatal for the whole network, and is termed as "Coagulation Attack". The attack derives its name from coagulation property of fluids. Coagulation refers to solidification or clotting of substances. With an ease of reconfigurability and availability, this type of attack has full possibilities to affect the whole network operating with UAVs. In this paper, the concept of coagulation attacks, issues in handling them, various research aspects and simulative case study have been discussed which are to be focused in future for robust and fault-free connectivity over networked UAVs.

## II. Coagulation Attack: Concept

Coagulation attack refers to a change in the state of UAVs operations primarily affecting the physical configurations and maneuvers. Coagulation attacks unlike other are not easy to detect, and countermeasures involve proper capturing of

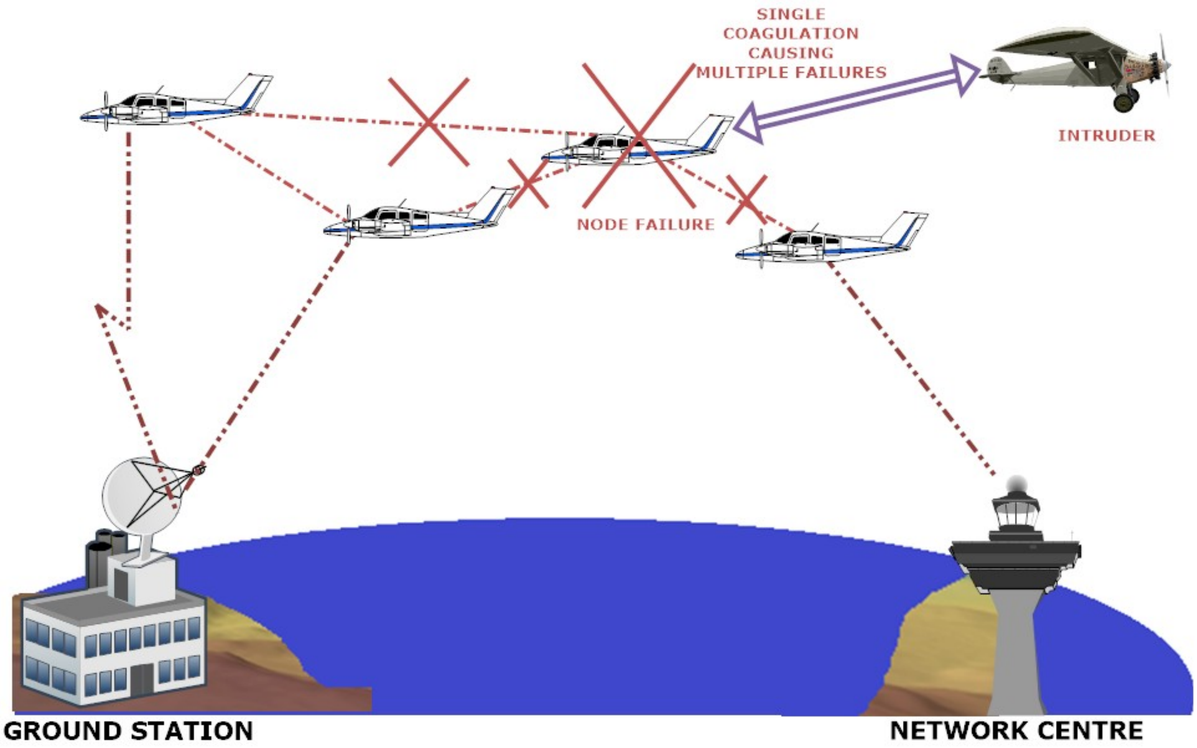

Fig. 1. A sample scenario for coagulation attack.

vulnerabilities. Based on the factors causing the attack, coagulation attack is categorized into four major parts, namely, UAV freezing, waypoint alterations, enforced collision, and UAV hijacking. All these are the major adversaries caused due to coagulation attack. A simple scenario showing coagulation attack on a single node is presented in Fig. 1. The details of these are given below.

- **UAV Freezing**: It refers to the node failure caused due to alterations in physical configurations of the UAVs directly affecting its maneuvers. UAV freezing causes mobility loss leading to network failures. These attacks are caused by the intrusion, signal jamming, and session hijacking.
- **Waypoint Alterations**: During operations, it might appear that UAVs are fully-functional. But, these vehicles might be under the threat of waypoint modifications. Waypoint modifications cause overlapping of mobility patterns leading to a collision. These attacks are fatal, and it is difficult to identify and trace their effect.
- **Enforced Clustering**: Unlike waypoint alterations, enforced clustering causes UAVs to form sub-clusters and create their own sub-network that operates in contrast to existing network. Vulnerability to this attack provides most of the information regarding patterns and configurations of the UAVs. If these are not detected in time, these may cause devastating effects.
- **UAV Hijacking**: It refers to capturing UAVs from a remote location by controlling its communication channels. UAVs operate using the instruction given to them manually or autonomously in a code format. However, these instructions can be easily cracked by reverse engineering, which allows a third party to override the movement of UAVs and control them remotely. Such attack already exists in the literature and is one of the important classifications of coagulation attack [16].

All of these are types of coagulation attack that can prove fatal for both networks as well as ground units.

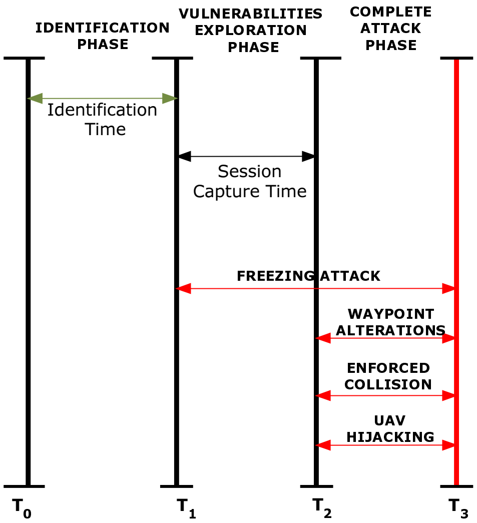

Fig. 2. Phases and slots for various coagulation attacks.

## III. Coagulation Attack: Phases

These attacks have been identified as a new set of vulnerabilities that a UAV network faces while operating in cooperative mode. These attacks can either affect a single link between two nodes or can affect the whole network. For a better understanding, the attack procedure is divided into three phases, namely, identification phase, session break/creating vulnerabilities, and attack phase.

The description of each of the phase is given below:

- **Identification Phase**: It is the initial phase which starts with the network observation. An attacker looks for possible entries into the network and fetches the network data by using existing compromising approaches such as session hijacking, and then, identifies the possible vulnerabilities that can cause any one of the above-given attacks.
- **Session Break and Creating Vulnerabilities**: Most of the networks in the initial phase are prone to these attacks. If a possible vulnerability is found, attackers exploit them to acquire a session to launch any one of the above-listed attacks. During this phase, a new set of codes can be used to launch a particular coagulation attack. This is the crucial phase from both attackers as well as defense point of view.
- **Attack Phase**: Once an attack is launched, the coagulation compromises the network with attackers. It is the final phase and is very difficult to revoke once the network is under the control of an attacker. This state is referred to as "State of Coagulation".

Diagrammatic description and slot for a particular coagulation attack are shown in Fig. 2. Coagulation attack is caused mostly by mapping the self-programmed data/code into the existing network and then generating adversaries to affect it. Once under attack, the possibilities of a network to recover from coagulation state are minimum. Coagulation attacks can be checked and monitored by deploying a network monitor. The main objective of a network controller is to prevent a network from undergoing the state of coagulation at any point of time during the whole mission.

## IV. Challenges

UAVs are very expensive network units that cannot afford loss or threat, as such incidents can cause a lot of damage in terms of cost, nation sovereignty, and life. The aim of this paper is to introduce the concept of coagulation attacks and inspire researchers to follow counter-measures while developing and deploying UAV networks. Following is the list of challenges faced by a network prone to coagulation attacks.

- Network performance should not be affected while taking countermeasures against such attacks.
- System should be capable of identifying nodes and errors in the case of a compromised network.
- Network restoration should be fast and safe during the recovery phase.
- Dynamic topology changes offer large benefits to these networks, but during recovery, this can cause hindrance as identification of fault becomes difficult with rapid topology change.
- Selection of appropriate bands for data sharing is one of the key issues with these networks.
- Over battery consumption for attack-reducing computations is one of the major challenges.
- Coagulation attack affects UAV proximity and decreases the level of coordination.
- Over computational burden increases the complexity, and thus, leads to network failures.
- These attacks decreases the adaptability of the network.
- Network might become unresponsive. This makes it next to impossible for a network to recover from coagulation attack.
- Coagulation attack also increases the counterfeit possibilities which can cause an attack on a ground station that controls and manages the coordination between aerial vehicles.

## V. Simulation Case Study

In order to clearly understand the effect of various types of coagulation attack, a simulative analysis is carried. The simulative case study suggests the most affecting coagulation attack, possibilities of a particular attack under complete vulnerable conditions, possibilities of recovery after an attack, chances of loss of UAVs, and time taken by an attacker to compromise the network. A vulnerable environment is considered to study the effect of coagulation attacks. A general UAV network is created in $Matlab^{TM}$ with UAVs ranging between 1 to 10 operating for data transmission, command, and control. A simple task of maneuvering an area is programmed to understand the level of vulnerabilities caused due to these attacks. The standard network configurations used for analysis of such attacks are presented in Table I. The network is realized for a number of slots (Time in seconds) taken by the particular attack to reach from identification to attack phase. This analysis is carried in two parts. First is carried by fixing the topology during the whole network, and second is done by varying the topology. Simulations suggest that network with varying topology take more time to undergo an attack in comparison with the network with fixed topology. Also, network hijacking is the adverse coagulation attack that a network can face during operations. Thus, a varying topology can aloof a network from coagulation attack for some time. The plots for comparison between different coagulation attacks based on the requirement of time slots with fixed, and varying topologies are presented in Fig. 3, and Fig. 4, respectively.

TABLE I
PARAMETER CONFIGURATIONS

| **Parameters** | **Value** |
|---|---|
| UAVs | 1-10 |
| Traffic Type | CBR |
| Antenna Type | Omni-Directional |
| Transmission Mode | Broadcast |
| Maximum Buffer Size | 20000 bytes |
| Aerial Speed | 10-15 m/s |
| Aerial Transmission Range | 1 km |
| Initial Network Bandwidth | 10 MHz |
| Maximum Iterations | 1000 |

TABLE II
COMPARISON BETWEEN VARIOUS COAGULATION ATTACKS.

| Attack | Affect | Probability of attack | Possibility of recovery | Loss of UAVs | Time to attack | Network Type | |
|---|---|---|---|---|---|---|---|
| | | | | | | Single UAV | Multi-UAVs |
| UAV Freezing | Moderate | High | High | May be | Low | ✓ | ✓ |
| Waypoint Alterations | High | High | High | May be | Moderate | ✓ | ✓ |
| Enforced Clustering | High | High | Low | Yes | Moderate | × | ✓ |
| UAV Hijacking | Extreme | Moderate | Very Low | Yes | High | ✓ | ✓ |

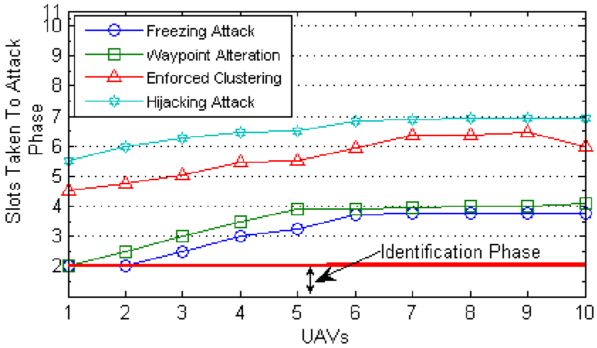

Fig. 3. Slot requirement for coagulation attack with fixed topology.

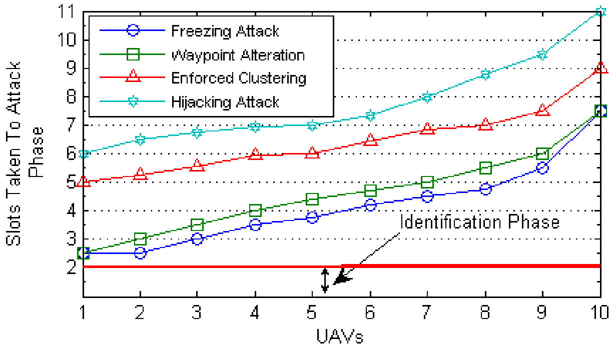

Fig. 4. Slot requirement for coagulation attack with varying topology.

Table II presents a comparison between the various coagulation attacks on the basis of parameters listed above. Further, the network is analyzed for its performance during normal operations, and during coagulation attack phase. UAV freezing is selected for analysis with a network size of 10 UAVs. The attack is launched at 400 seconds after the start of simulations and is carried continuously until the end of simulations. The analysis shows that Packet Delivery Ratio (PDR) decreases abruptly and almost reaches the threshold value; below which the network is unsustainable. The thresholds are assumed and can be varied depending on the scenario and configurations. The plot for comparison of PDR during normal network operations and attack phase is shown in Fig. 5. The analysis is also traced for network latency. The attack causes many overheads, and thus, increases the network latency beyond the threshold value. Threshold value defines the limit up to which the network can sustain without any loss. The comparative plot for network latency is presented in Fig. 6. The number of failures causes high delays and higher loss of packets. Thus, more re-transmissions are required to cope up with the network conditions. But, coagulation attack causes the number of re-transmissions to increase abruptly which causes a total shutdown of the network. The plot for the requirement of a number of re-transmissions during normal operations,

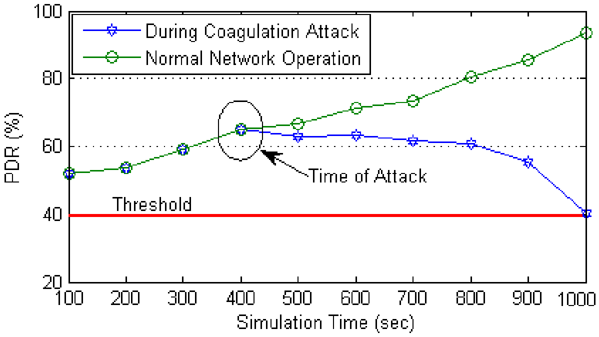

Fig. 5. Packet delivery ratio vs. simulation time.

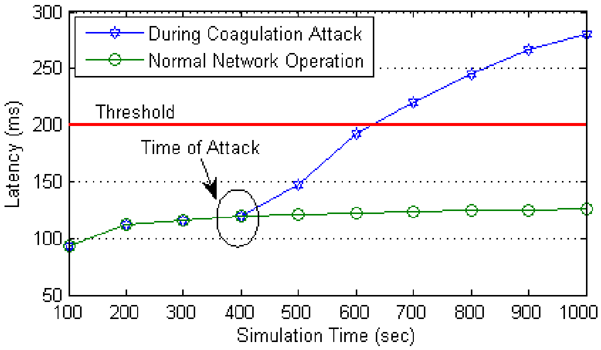

Fig. 6. Latency vs. simulation time.

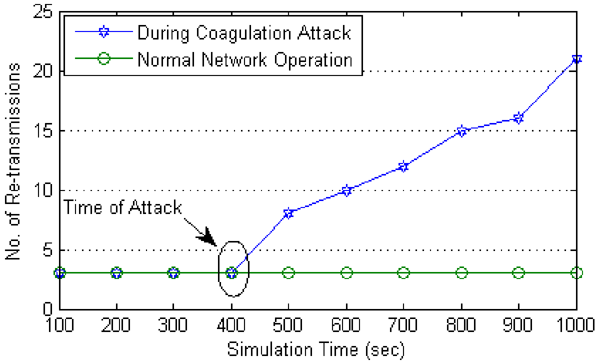

Fig. 7. No. of re-transmissions vs. simulation time.

and during attack phase is presented in Fig. 7. Simulation analysis shows that the coagulation attack can prove fatal for the network especially involving aerial nodes. It can cause devastating effect and can lead to multiple failures that may affect the overall mission for which UAVs are configured. Hence, the focus needs to be given to such network problem, and a proper solution is required to prevent a network from these attacks.

## VI. Discussions and Open Issues

Attacks on UAVs have already been studied by many researchers. Most of them have focused on the cyber attacks which directly affect the performance of the network formed between the UAVs. Coagulation attack is itself a type of cyber attack, which is presented with sub-classification of the type and impact of the vulnerability. The simulation study presents the impact of such attacks and tries to bring this into focus for possible elimination over UAVs. Apart from the study and analyses presented in this paper, there are several open issues which are to be taken care of while understanding the detailed impact of coagulation attacks. These include,

- The impact of communication standard used for transmission between the UAVs and ground systems needs to be considered for further understanding the level of vulnerabilities of coagulation attack.
- The coagulation attacks need to be evaluated in the presence of other cyber and network threats such as Sybil attack, impersonation attack, wormhole attack, node capturing, eavesdropping, sinkhole attack, etc.
- Apart from studying the impact of coagulation attacks, approaches need to be developed to counterfeit the vulnerabilities and security concerns raised by these attacks over network UAVs.
- More emphasized security analyses and formal evaluations are to be conducted over networked UAVs, and the effect of such attacks should be studied over other performance metrics.
- Layer-wise structuring and evaluation of existing security approaches for prevention against coagulation attacks need to be examined and evaluated for further improvements.

## VII. Conclusion

In this paper, a new coagulation attack is introduced which particularly affects the high mobility networks such as UAV networks. Coagulation attack causes mobility alterations of the nodes. Multiple variants of coagulation attack lead to the devastating effect on the network operations. Such attacks raise serious issues in development and deployment of aerial nodes for flying network formations. The simulation study demonstrates the level of threat these attacks can cause to normal operations of a network. Efficient solutions are required to keep networks aloof from such attacks. Protocols and architectures are required that have embedded properties to counter affect the coagulation attacks. Security of physical layer using improved encoding scheme can be a possible solution against such attacks.

Further investigations and studies are required to analyze all the factors that cause vulnerabilities leading to coagulation attack. Implementation analysis and possible remedies will be presented in future reports.

## References

[1] V. Sharma and R. Kumar, "A cooperative network framework for multi-uav guided ground ad hoc networks," *Journal of Intelligent & Robotic Systems*, vol. 77, no. 3-4, pp. 629–652, 2015.

[2] E. AbdAllah, H. Hassanein, and M. Zulkernine, "A survey of security attacks in information-centric networking," *Comm. Surv. Tutorials, IEEE*, vol. 17, pp. 1441–1454, thirdquarter 2015.

[3] L. Zhang, G. Ding, Q. Wu, Y. Zou, Z. Han, and J. Wang, "Byzantine attack and defense in cognitive radio networks: A survey," *Comm. Surv. Tutorials, IEEE*, vol. 17, pp. 1342–1363, thirdquarter 2015.

[4] S. Riazul Islam, D. Kwak, M. Humaun Kabir, M. Hossain, and K.-S. Kwak, "The internet of things for health care: A comprehensive survey," *Access, IEEE*, vol. 3, pp. 678–708, 2015.

[5] A. Banerjee, K. K. Venkatasubramanian, T. Mukherjee, and S. K. S. Gupta, "Ensuring safety, security, and sustainability of mission-critical cyber–physical systems," *Proceedings of the IEEE*, vol. 100, no. 1, pp. 283–299, 2012.

[6] K. Hartmann and C. Steup, "The vulnerability of uavs to cyber attacks-an approach to the risk assessment," in *Cyber Conflict (CyCon), 2013 5th International Conference on*, pp. 1–23, IEEE, 2013.

[7] M. Barrere, R. Badonnel, and O. Festor, "Vulnerability assessment in autonomic networks and services: A survey," *Commun. Sur. Tutorials, IEEE*, vol. 16, pp. 988–1004, Second 2014.

[8] O. Zouhri, S. Benhadou, and H. Medromi, "A new adaptative security protocol for uav network," in *Advances in Ubiquitous Networking 2*, pp. 649–657, Springer, 2017.

[9] V. Sharma and R. Kumar, "G-fanet: an ambient network formation between ground and flying ad hoc networks," *Telecommunication Systems*, pp. 1–24, 10.1007/s11235-016-0210-2, 2016.

[10] V. Sharma and R. Kumar, "Teredo tunneling-based secure transmission between uavs and ground ad hoc networks," *International Journal of Communication Systems*, 10.1002/dac.3144, 2016.

[11] L. Negash, S.-H. Kim, and H.-L. Choi, "Distributed unknown-input-observers for cyber attack detection and isolation in formation flying uavs," *arXiv preprint arXiv:1701.06325*, 2017.

[12] H. Sedjelmaci, S. M. Senouci, and M.-A. Messous, "How to detect cyber-attacks in unmanned aerial vehicles network?," in *Global Communications Conference (GLOBECOM), 2016 IEEE*, pp. 1–6, IEEE, 2016.

[13] A. Kim, B. Wampler, J. Goppert, I. Hwang, and H. Aldridge, "Cyber attack vulnerabilities analysis for unmanned aerial vehicles," in *Infotech@ Aerospace 2012*, p. 2438, 2012.

[14] A. Abbaspour, K. K. Yen, S. Noei, and A. Sargolzaei, "Detection of fault data injection attack on uav using adaptive neural network," *Procedia Computer Science*, vol. 95, pp. 193–200, 2016.

[15] A. Sanjab, W. Saad, and T. Başar, "Prospect theory for enhanced cyber-physical security of drone delivery systems: A network interdiction game," *arXiv preprint arXiv:1702.04240*, 2017.

[16] K. Hartmann and K. Giles, "Uav exploitation: A new domain for cyber power," in *Cyber Conflict (CyCon), 2016 8th International Conference on*, pp. 205–221, IEEE, 2016.