2024 AIAA DATC/IEEE 43rd Digital Avionics Systems Conference (DASC), 29 September - 3 October 2024, San Diego, CA, USA
DOI:10.1109/DASC62030.2024.10748746

Moving Target Defence in 6G UAV Networks

Ahmed Alismail
Cranfield University, United Kingdom
A.alismail4@cranfield.ac.uk

Huw Whitworth
Cranfield University, United Kingdom
h.t.whitworth@cranfield.ac.uk

Saba Al-Rubaye
Cranfield University, United Kingdom
s.alrubaye@cranfield.ac.uk

Antonios Tsourdos
Cranfield University,United Kingdom
a.tsourdos@cranfield.ac.uk

Liz James
NCC Group, United Kingdom
liz.james@nccgroup.com

Lawrence Baker
NCC Group, United Kingdom
lawrence.baker@nccgroup.com

***Abstract*—This paper focuses on enhancing the resilience of Unmanned Aerial Vehicle (UAV) networks against reconnaissance cyber-attacks. We introduce a novel algorithmic framework for IP and Port hopping, specifically tailored for UAV networks, to implement Moving Target Defense (MTD). The algorithm dynamically changes IP addresses and communication ports, increasing network unpredictability and thwarting reconnaissance attempts. Furthermore, we combine Network-based Moving Target Defense with sixth generation (6G) Software-Defined Networking (SDN) to enable real-time reconfiguration of network policies, providing proactive defense capabilities. Additionally, we integrate honeypots as a cyber deception strategy to divert potential attackers and gather valuable insights into their tactics. Extensive simulations demonstrate the effectiveness of our approach in reducing reconnaissance success rates and enhancing UAV network security.**

***Index Terms*—Sixth Generation (6G), MTD, UAV, Honeypot**

I. Introduction

Unmanned aerial vehicles (UAVs) have been seeing a surge in popularity and experiencing a rapid adoption rate in various domains, the incipient surge of UAVs in recent years has largely been a result of an amalgamation of technology from the realms of microelectronics and aerospace engineering. Technological advancements in these domains have allowed UAVs to become smaller, cheaper, and more efficient, while simultaneously improving their reliability and versatility [1], [2]. In addition, it is anticipated that UAVs would have a substantial impact on future 6G networks through allowing flexible deployment and easing back-haul connection operations [3], [4]. Leveraging 6G networks for UAVs presents a promising prospect to establish reliable connectivity, simultaneously decreasing the expenses and requirements associated with scale, weight, and power consumption [5]. In the ever-evolving landscape of UAV system design, the field of cybersecurity has emerged as an essential component of ensuring the integrity, resilience, and reliability of UAV networks. These networks, often operating in complex and dynamic environments, are subject to a multitude of threats that could potentially disrupt operations and compromise mission objectives. Given the increasing reliance on UAVs in critical tasks such as Defense operations and emergency response, the imperative of securing UAV networks has never been more acute. Additionally, they find utility in applications for military use include a range of strategic uses, including monitoring, tracking of targets, and air-to-ground warfare, necessitating robust security measures for wireless communications between UAVs and ground stations [6] [7] [8] [9] [10].

The incorporation of UAVs into the national airspace has prompted substantial discussions among governmental and non-governmental entities in both public and private sectors concerning their security issues. Telecommunications providers are poised to play a crucial role in supporting eVTOL services as they offer a reliable network infrastructure, minimal delay in data transmission, and high-capacity services [11].

These attributes are essential for ensuring secure and efficient flight management, as well as establishing strong connectivity among various aircraft. The advanced communication system could be categorised into edge cloud, core network, Advanced Air Mobility (AAM/UTM) , and telemetry services , based on their functionalities and performance [12]. From a security standpoint, the prevalence of various cyber-attacks underscores the vulnerabilities of UAVs at different levels. Undoubtedly, malevolent entities capitalise on the extensive use of UAVs in civilian domains, capitalizing on the vulnerabilities inherent in commercial drones, thereby posing a significant threat to public safety [13]. However, the execution of complex AAM operations necessitates the utilisation of sophisticated communication, navigation, and surveillance (CNS) capabilities, as well as the deployment of resilient cybersecurity technologies, there is additionally a need to build more sophisticated collaborative decision-making frameworks [14].

The fundamental cause of the significant network security issue lies in the inherent asymmetry between offensive attacks and defensive measures. Initially, the attackers possess the temporal advantage, as they are able to engage in Conducting thorough assessment of vulnerabilities and testing for vulnerabilities on a specific target in a repetitive manner until their ultimate objective is attained. Furthermore, the attackers possess an asymmetric information advantage, as they are able to initiate and execute an attack whenever an exploitable vulnerability is present. In contrast, the defenders are burdened with the task of safeguarding all potential vulnerabilities and thwarting all possible attack vectors employed by the

attackers. System attackers have a cost advantage in terms of expanding their attack due to the uniformity in network configurations. This uniformity facilitates the execution of large-scale attacks with relative ease and minimal expenditure, particularly following the success of a small-scale attack. The network configurations commonly exhibit characteristics of determinism, static, and homogeneous. The deterministic and static characteristics provide attackers with the benefits of time and information, while the homogeneity characteristic grants them a cost advantage. In essence, these characteristics serve to mitigate the challenges encountered by malicious actors in conducting network scans, pinpointing specific targets, and acquiring critical intelligence. This provides the attackers the benefits of constructing, initiating, and disseminating attacks. While knowledge-temporal imbalances can be addressed by systems security engineering approaches such as having clearly defined interfaces, detection capabilities deployed on interfaces and a robust incident response plan in the situation where a cyber event occurs, there is a growing need more more active response mechanisms. The current solution to this is Moving Target Defence (MTD) MTD provides an active mechanism to make early phases in the Cyber Kill Chain such as Reconnaissance and Weaponization harder when attempting to use an initial foothold to pivot through a network architecture.

MTD presents a unique approach to address the inherent imbalance between offensive attacks and defensive measures wherein the protected system employs dynamic shifting in order to constantly move the attack surface, a process that can be effectively controlled and managed by the system administrator. Thus, the attack surface that is vulnerable to potential attackers exhibits a state of disorder and undergoes dynamic changes. Consequently, the exertion expended by potential attackers, encompassing both financial expenses and intrinsically, will be significantly amplified in order to execute a triumphant attack. Therefore, the likelihood of successful attacks will be diminished, effectively strengthening the resiliency and security of the protected system. It is imperative to acknowledge that MTD does not represent a distinct approach, but rather a principle of active defense.

Various system attributes, including IP address, service port number, protocol, and running platform, can be subject to variation, resulting in a diverse range of Moving Target Defense (MTD) mechanisms. For instance, the application of MTD to the IP address opens the door to a range of approaches for mutating the IP address. Similarly, when MTD is applied to the running platform, a variety of dynamic techniques for the platform emerge. Furthermore, this technique has the potential to enhance the efficacy of current security evaluation or defense methodologies.

The novel contribution of this work is the integration of Unmanned Aerial Vehicles (UAVs) in to the Software-Defined Networking (SDN) environment augmented with honeypots to produce a robust and cohesive defense strategy. This has been enabled via MATLAB algorithmic development for IP and Port hopping, tailored for UAV networks in the form of Network based Moving Target Defence (NMTD) instantiated within an SDN and honeypots to form a proactive and adaptive defense strategy for UAV networks in order to strengthen the protection of critical assets against evolving cyber threats.

II. Literature Review

Currently, system and network administrators find themselves in a reactive mode where they primarily focus on patching and upgrading vulnerable systems to ensure their security. The conventional defense mechanisms and approaches employed by administrators align with the policy, protection, detection, response, and recovery (PPDRR) model.

The PPDRR policy serves as the keystone for the implementation of protection, detection, response, and recovery processes. Protection is commonly attained by employing conventional static security technologies, such as firewalls, cryptography, and authentication mechanisms. The utilisation of detection mechanisms facilitates the identification of novel threats and vulnerabilities, thereby serving as the fundamental premise for initiating a response. The response phase holds significant importance within the security cycle as it serves as a crucial link and offers the most efficient means to address potential threats. The final stage in the security cycle is the process of recovery. After the recovery process, the system will be returned to either its original pristine state or an enhanced state with improved security measures compared to its previous state. The comprehensive and dynamic security cycle encompasses protection, detection, response, and recovery, all of which are guided by established policies.

A. Moving Target Defence

MTD is considered an active defence strategy due to its ability to automatically alter one or more attributes, thereby increasing the level of effort required for successful attacks. The active capability of a Mobile Threat Defense (MTD) system is not contingent upon the condition or circumstances of the environment in which it is deployed. In order to enhance its efficacy and applicability, it is recommended that an MTD (Moving Target Defence) system be endowed with reactive capabilities, enabling it to promptly respond to any observed or perceived anomalous event [15].

At present, certain mechanisms have been developed to possess both active and reactive capabilities concurrently. Examples of such mechanisms include ChameleonSoft [16] and moving attack surface (MAS) [17]. The operational mode of Moving Target Defences (MTDs) deviates from the conventional PPDRR security model. The integration of MTDs alters the standard defence processes employed by traditional defence mechanisms and approaches, resulting in the emergence of a novel security framework.

1) Types of Moving Target Defence: The study of Moving Target Defence can be split in to two distinct areas of research: Spatial based or Temporal based. **Spatial Based Moving Target Defence** Spatial MTD strategies exhibit practicality as defensive measures for diverse components within systems,

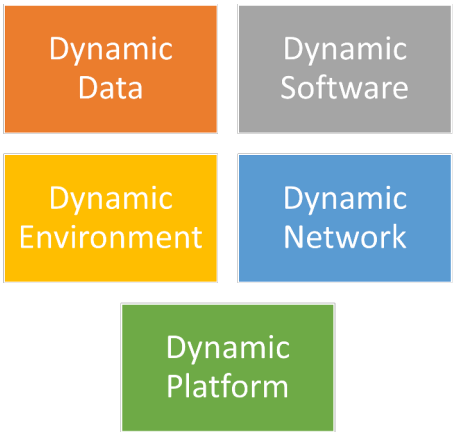

Fig. 1: Types of Spatial based MTD

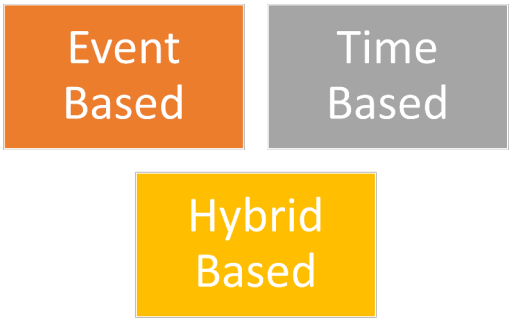

Fig. 2: Temporal MTD Strategies

various security threats, and the scope of possible utilisation situations. The objective is to enhance the intricacy of cyberattacks through the reduction of system homogeneity, stativity, or certainty. Based on the network stack protocol layers, various strategies are identified, namely the dynamic runtime environment layer MTD, dynamic software layer MTD, dynamic data layer MTD, dynamic platform layer MTD, and dynamic network layer MTD, as shown in Figure 1 **Temporal Based MTD** The classification of MTD techniques in timeliness-based MTD is determined by criteria that are used to ascertain the appropriate timing for executing a move. There are three distinct categories of temporal defence given in Figure 2:

Operation based MTD The classification of MTD techniques in operation-based MTD is determined by criteria that ascertain the optimal approach for movement. In their study, Hong and Kim [18] classified MTD techniques into three categories according to the characteristics of the operations involved: shuffling, diversity, and redundancy.

Shuffling The shuffling technique involves the reorganisation or randomization of system configurations. This could involve the alteration of IP or the dynamic modification of virtual machine (VM) migration timing. The primary objective of shuffling-based MTD methods is to enhance the level of disorientation and ambiguity for potential attackers. This is achieved by rendering the discovery of susceptible targets more challenging, either through making the information gathered by aggressors outdated or by depleting their resources through the acquisition of irrelevant data. In essence, the utilisation of shuffling-based MTD techniques can effectively impede or postpone unauthorised access by potential attackers to a given target system. Due to the increased duration available for monitoring attack behaviours, such as reconnaissance attacks, system defence mechanisms, such as Intrusion Detection Systems (IDS), are able to develop more sophisticated strategies for countering the identified attacks.

IP shuffling The application of IP shuffling, mutations, and host randomization has been observed in numerous network domains as part of shuffling-based Moving Target Defense (MTD) techniques. In their study, Sharma [19] designed an IP shuffling MTD technique that leverages the principle of IP multiplexing (or demultiplexing) within a Software-Defined Networking (SDN) framework. In their study, MacFarland and Shue [20] implemented a technique involving the mutation of host IP addresses in order to safeguard a network of significant scale. This was achieved through using an SDN controller, which effectively managed DNS (Domain Name System) interactions. The IP randomization technique proposed by Antonatos [21] serves the purpose of mitigating hitlist worm attacks. This technique aims to prevent malicious worms from acquiring intelligence concerning potential targets within the system, thus increasing the difficulty for attackers to recognise new and susceptible targets. The IP shuffling technique implemented by Jafarian [22] involved the unpredictable mutation of IP addresses in order to minimise the overhead associated with MTD operations. The researchers employed SDN based OpenFlow (OF) protocol, which is commonly employed to allocate Virtual IP addresses that are translated from or to the actual IP address of a host. In their research, Carroll [23] investigated the implementation of network address shuffling MTD strategy for safeguarding honeypots. They employed probability models to assess the likelihood of successful attacks, taking into account factors such as network size, the quantity of addresses targeted by attackers, the number of system vulnerabilities, and the frequency of shuffling-based MTD activation. In their study, Kampanakis [24] implemented host randomization and mutation techniques to assess the impact of employing the MTD approach on the attackers' overhead within an SDN.

Port hopping The approach of port hopping was investigated by Luo [25] as a means of countering reconnaissance attacks. This technique, which is based on the shuffling-based MTD notion, aims to conceal service identities and create confusion for potential attackers. This study aims to measure the efficacy of the suggested port hopping technique by evaluating the probability of successful attacks in relation to various key design parameters. The parameters include:

- The amount of probes
- The range
- The Port Pool
- The number of susceptible services
- The Rate of Port Hopping

Network Topology Shuffling The notion of Network Topology Shuffling involves the continuous alteration of routes within networks in order to disrupt an attacker's path information. Achleitner and colleagues [26], [27] introduced a framework for generating virtual topologies to mitigate network scanning attacks, utilising SDN technology. The authors Hong [28] introduced an optimal network reconfiguration technique in the context of SDN environments, employing the premise of shuffling-based MTD. The researchers successfully addressed a shuffling assignment problem and demonstrated the enhanced level of network security resulting from the diversification of network routing paths.

B. Attack Surfaces

The goal of the defenders is to reduce the vulnerable components within the system, thus reducing the attack surface [29]. This objective can be accomplished through the implementation of security patches, the closure of unused ports, and adherence to established security protocols.

In their publication, the authors of [27] provide a description of the attack surface, which is defined as a specific subset of resources within a given system that possess the potential to be exploited for the purpose of launching an attack. The authors additionally put forth a proposition for an attack surface metric as a means of evaluating the relative security of different systems. This metric aims to quantify the probability of a system being targeted for an attack.

The manipulation of the attacker's perspective of the system is addressed in papers [30], [31] where the authors utilise a graph based method to strategically manipulating the assailant's probes thereby maximising the distance between the external system view and the internal view. This is done while considering a predetermined upper cost for the defender.

III. Methodology

Within this section we promote a multi-agent UAV network including SDN and MTD. Examining the strategies and techniques utilised for securing UAVs against cyber threats, with particular emphasis on the preliminary stage of a cyberattack, namely reconnaissance. The importance of preventing reconnaissance activities is emphasised by the fact that a successful mapping of a network by an attacker can greatly enhance the probability of a subsequent attack, such as a Denial of Service (DoS), achieving its objectives. The focus of our methodology revolves on the investigation and advancement of dynamic defence strategies, specifically Network Moving Target Defence (NMTD), with the aim of protecting UAVs against reconnaissance efforts. The development of SDN-based mechanisms for IP and port hopping is a crucial element of this approach. The utilisation of this particular technique introduces an element of unpredictability within the network infrastructure, thereby rendering the task of mapping the network and acquiring vital information more difficult for potential attackers. Consequently, this disruption hampers their reconnaissance efforts. In addition, we incorporate deception technology, particularly honeypots, into the SDN system in order to enhance the confusion and diversion of potential attackers. Honeypots function as decoys that mimic the real network nodes, with the specific purpose of isolating and monitoring malicious activities conducted by adversaries. The provision of an early warning system for potential attacks and the acquisition of valuable insights into the methods employed by attackers serve to augment our defensive capabilities. The proposed algorithm is given below in Figure 1.

Algorithm 1 Algorithm for IP and Port Hopping

```
0: Initialize: network parameters
0: Generate IP and Port Pool
0: Assign real IP and Port to each UAV
0: for each UAV do
0:     Assign realIP and realPort
0: end for
0: Map real IP & Port with virtual IP & Port for the initial
   iteration
0: for each UAV do
0:     Generate and assign virtual IP and port
0: end for
0: Start hopping mechanism
0: while true do
0:     Display IP Address Table
0:     Wait for hopping time
0:     for each UAV do
0:         Update virtual IP and port
0:         if unique combination is found then
0:             Update table
0:         else
0:             Exit loop and proceed to Step 1
0:         end if
0:     end for
0: end while
0:  Send used virtual IP and Port to Honeypot
0: for each used IP and Port do
0:     Send to honeypot
0: end for
0: Loop back to Step 11 =0
```

Table **??** provides as summary of the individual steps within the algorithm. Our method comprises three core segements: the routing table, the UAV environment and the Honeypot environment.

A. Routing Table Construction

The first stage involves constructing the routing table for IP and Port hopping. In addition to facilitating network visualization, it will also function as a log table throughout the mission length, enabling retrospective analysis of network activities during the operation. The system is comprised of seven columns:

1) **Devices:** The devices encompassing the designation UAVs.
2) **Real IP:** The real IP refers to the initial assignment of an IP address to each UAV at the beginning of the

TABLE I: Steps and Descriptions

Step	Description
1	**Initialize Network Parameters:** Set up network parameters like subnet, IP address range, port range, and number of UAVs.
2	**Generate IP and Port Pool:** Create a pool of available IP addresses and ports.
3	**Assign Real IP and Port to Each UAV:** Assign unique real IP and port to each UAV, removing used values from the pool.
4	**Map Real IP & Port with Virtual IP & Port:** Assign each UAV a virtual IP and port for the initial iteration.
5	**Start Hopping Mechanism:** In a continuous loop, frequently change virtual IP addresses and ports. If a unique combination is found, update the table; otherwise, exit the loop.
6	**Send Used Virtual IP & Port to Honeypot:** Send old virtual IP and port combinations to a honeypot to detect unauthorized access.
7	**Terminate:** End the algorithm based on certain conditions or a set number of iterations.

flight, which remains constant throughout the whole of the mission.

3) **Real Port:** The real Port refers to the initial assignment of a port to each UAV at the beginning of the flight, which remains constant throughout the whole of the mission.
4) **Virtual IP:** Used to perform the hopping mechanism with each hopping time.
5) **Virtual Port:** Utilized to perform the mechanism of hopping throughout each hopping period.
6) **Time:** Records the precise timing of each instance of hopping, serving as a mission log.
7) **Hopping Time:** Refers to the specific moment at which the algorithm transitions to the subsequent set of Virtual IP addresses and Ports assigned to the devices inside the network.

$$\text{number of possible combinations} = \frac{aIPs \times aPorts}{nUAV} = \frac{77 \times 77}{7} = 847 \quad (3\text{-}1)$$

$$\text{Virtual IP} = aIP - nUAV = 77 - 7 = 70 \quad (1)$$

$$\text{Virtual Ports} = aPorts - nUAV = 77 - 7 = 70 \quad (2)$$

$$\text{number of usable combinations (C)} = \frac{vIPs \times vPorts}{nUAV} = \frac{70 \times 70}{7} = 700 \quad (3)$$

$$\text{Mission Duration} = \frac{\text{HT} \times \text{nC}}{60} = \frac{21 \times 700}{60} = 245 \text{ min} \quad (4)$$

$$\text{Mission Duration with random (HT)} = \frac{\max(\text{HT}) \times \text{nC}}{60} = \frac{\max(21\text{-}30) \times 700}{60} = 350 \text{ min} \quad (5)$$

An example is given in Table **??**.

B. UAV Network Environment

The dynamic environment was created as a model of a multi-agent UAV network, specifically designed to showcase the IP and Port hopping effects generated by the algorithm applied in the routing table. Figure 35 shown below illustrates a network of UAVs, whereby each node symbolises a UAV in flight, and the interconnecting links represent the communication channels between them within a dynamic setting.

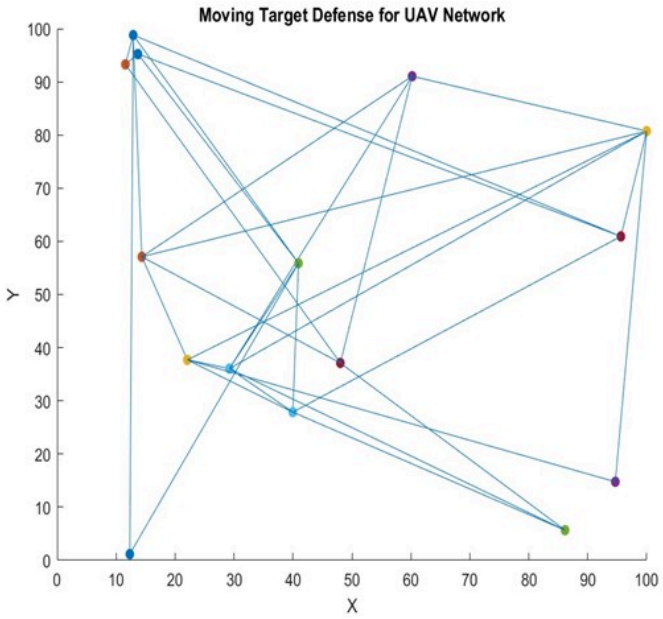

Fig. 3: Proposed UAV environment in MATLAB

The dynamic environments replicate a network of flying UAVs, whereby the quantity of nodes is directly correlated to the number of UAVs present in the routing table. Each node in the network will be assigned an IP address and port number. As the network operates, nodes will periodically update their IP addresses and port numbers based on the method specified in the routing table.

Figure 3 shows the conceptual simulation environment for the UAVs

C. Honeypot Networks

Honeypots isolate attacks in to operating within a virtual environment, enabling the network security team to closely monitor the activities the hacker attempts to execute within the actual network. Furthermore, this might potentially provide the defence team with the chance to ascertain the identity

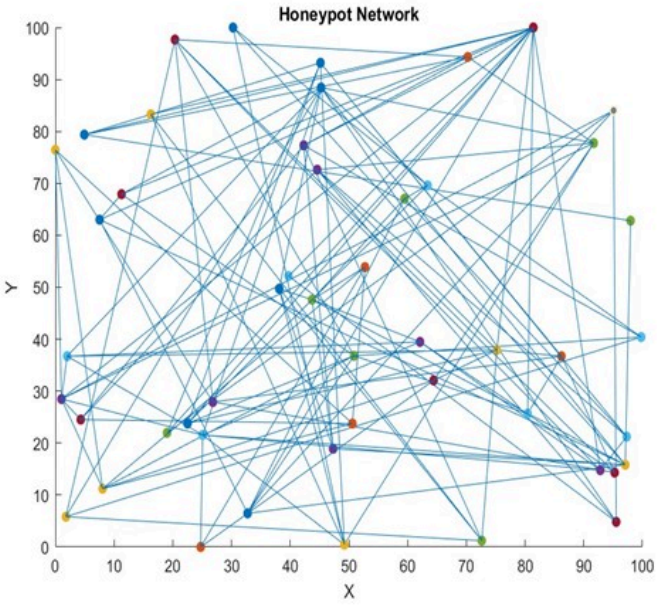

Fig. 4: Proposed Honeypot structure in MATLAB

of the attacker or even launch a retaliatory strike on the perpetrator's network, so impeding their capacity to carry out further attacks on the UAV network. As seen in Figure 4, each node inside the honeypot environment represents a historical combination of IP and Port that has previously been used within the routing table. Hence, it is essential for the honeypot to possess the ability to accommodate all potential combinations of IP addresses and ports. This stands in contrast to UAV systems, where the number of nodes is limited to the quantity of devices included in the routing table. From the standpoint of the defence team, the activation of any node inside the honeypot environment is seen as a potentially suspicious behaviour. Consequently, the honeypot serves as an alarm mechanism for the defence team, functioning as a decoy to the actual system, with the intention of luring the attacker into believing they have gained access to a genuine network.

However, in order to efficiently deploy a honeypot structure within the UAV domain the defenders must clearly define the operating parameters of the mission.

D. Mission Parameters

In order to accurately determine the duration of the operation, it is necessary to use the prescribed formulas provided below. Initially, it is necessary to determine the quantity of UAVs that will be used inside the network. Additionally, it is important to consider the range of IP & Port that are accessible. The hopping time refers to the duration between consecutive hops inside the network.

$$\text{number of possible combinations} = \frac{aIPs \times aPorts}{nUAV} \tag{6}$$

$$Virtual\ IP = aIP - nUAV \tag{7}$$

$$Virtual\ Ports = aPorts - nUAV \tag{8}$$

$$Mission\ Duration = HT \times nC \tag{9}$$

$$\text{number of usable combinations (C)} = \frac{vlPs \times vPorts}{nUAV} \tag{10}$$

$$Mission\ Duration\ with\ random(HT) = max(HT) \times nC \tag{11}$$

TABLE II: Mission Parameters

Notation	Description
$nUAV$	Number of UAV
$aIPs$	Available IP range
$aPorts$	Available Ports range
$vlPs$	Virtual IP
$vPorts$	Virtual Ports
HT	Hopping Time
C	Usable Combinations
nC	Number Usable Combinations

IV. Results and Analysis

A scenario was created for our mission, so we can perform the initial calculation which will give us the number of combination allowed for to be utilized and mission duration, using Equations 1 - 6. The table shows number UAVs, available IPs range, available Ports, hoping time and finally the subnet.

TABLE III: Scenario Parameters

Parameter	Value
Number of UAVs	7
Available IPs Range	1-77
Available Ports Range	7-83
Hopping Time	21-30 s
Subnet	192.168.1.0

Applying the equation that have been introduced earlier in the paper we find the mission parameters such as: possible combinations of available IPs & Ports and the estimated duration of the mission with the thesis's combination.

$$\begin{aligned}\text{number of possible combinations} &= \frac{aIPs \times aPorts}{nUAV} \\ &= \frac{77 \times 77}{7} = 847\end{aligned} \tag{12}$$

$$\text{Virtual IP} = aIP - nUAV = 77 - 7 = 70 \tag{13}$$

$$\text{Virtual Ports} = aPorts - nUAV = 77 - 7 = 70 \tag{14}$$

$$\begin{aligned}\text{number of usable combinations (C)} &= \frac{vIPs \times vPorts}{nUAV} \\ &= \frac{70 \times 70}{7} = 700\end{aligned} \tag{15}$$

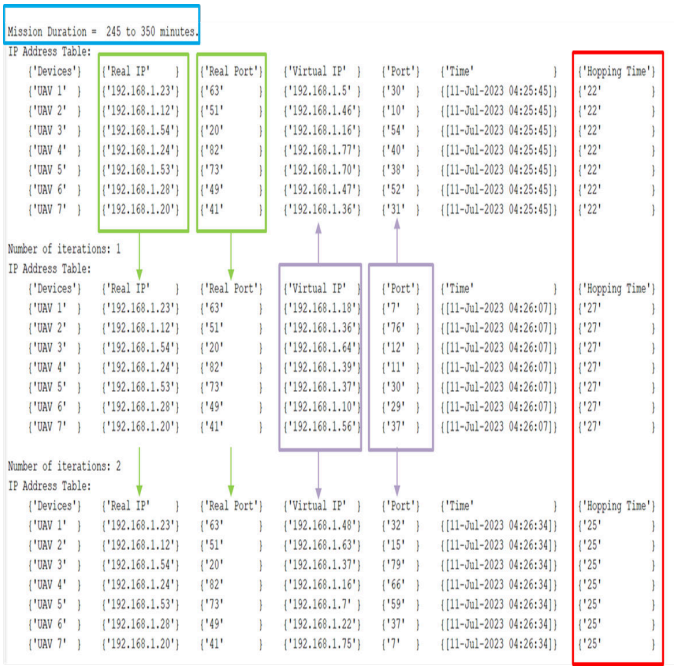

Fig. 5: UAV Routing Table

$$\text{Mission Duration} = \frac{\text{HT} \times \text{nC}}{60} = \frac{21 \times 700}{60} = 245 \text{ min} \tag{16}$$

$$\text{Mission Duration with random (HT)} = \frac{\max(\text{HT}) \times \text{nC}}{60} = \frac{\max(21\text{-}30) \times 700}{60} = 35 \tag{17}$$

Once the parameters have been defined, the mission duration is derived based on the given parameters. Subsequently, the algorithm for IP and Port hopping is initiated by generating a routing table that assigns real IP & Ports to each UAV in the network. Following this, each UAV in the network is allocated a virtual IP and virtual port for the initial iteration. In the second iteration the virtual IPs & Ports for the UAVs will change at the end of the hopping time. Figure 5 illustrates how the routing table behaves with each iteration. The virtual IP and & Ports hoping highlighted in purple and demonstrate how the virtual IPs & Ports hop with each iteration, while the real IPs & Ports are highlighted in green will have the same value until the end of the mission.

A. UAV Simulations

Multi agent UAV network flying in 3-D environments have been simulated in MATLAB. As the figure shows the UAVs flying in the environment and we set up a fix node in cyan to act as the SDN controller. As shown in Figure 6 UAVs are connected to the SDN as depict in the figure below to simulate the communication link. Virtual IPs & Ports

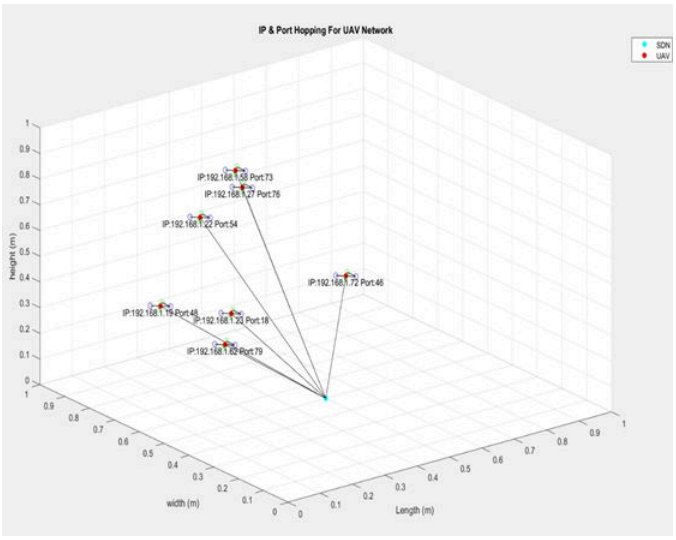

Fig. 6: UAV Network in MATLAB at time 'T'

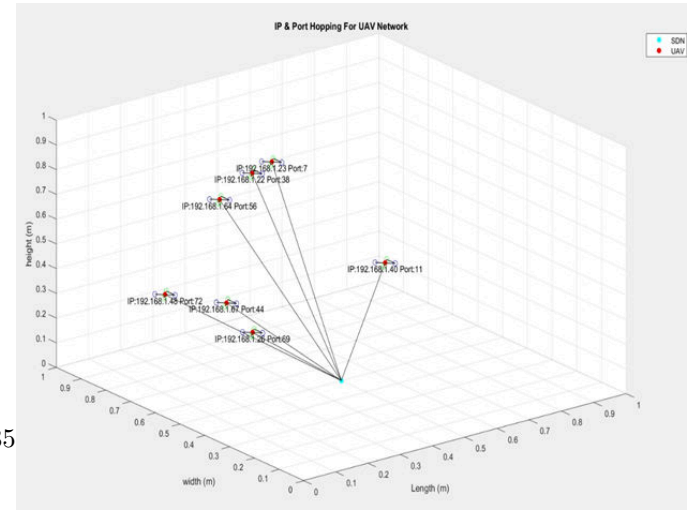

Fig. 7: UAV Network at 'T+1'

printed below each UAV to help with visualizing the live updating (hoping) value with each iteration. Figure 7 shows the following timestamp to show the updated virtual IPs and Ports for each operational UAV.

B. The Honeypot Network

The Figure 8 illustrates a network of nodes linked together in a 3-D environment. The nodes value are the first used virtual IPs & Ports in the UAV network environment, where we have seven UAVs in the UAV network and we have seven nodes in the Honeypot network at time 't'.

Figure 9 below shows the Honeypot network after the fourth time step. here we see the number of nodes has increased from seven at the first iteration to be twenty- eight.

C. UAV - Honeypot Interaction

When the hopping time finish the IPs and Ports in the UAV network transfer from the active environment to the honeypot

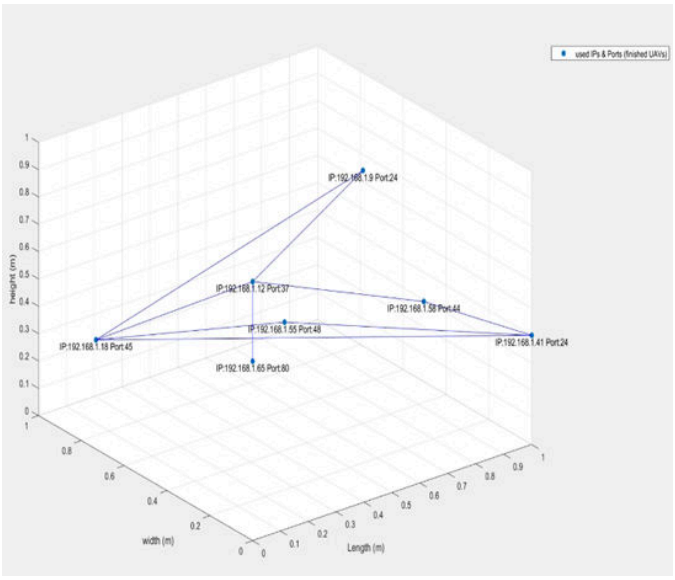

Fig. 8: Honeypot structure at time 't'

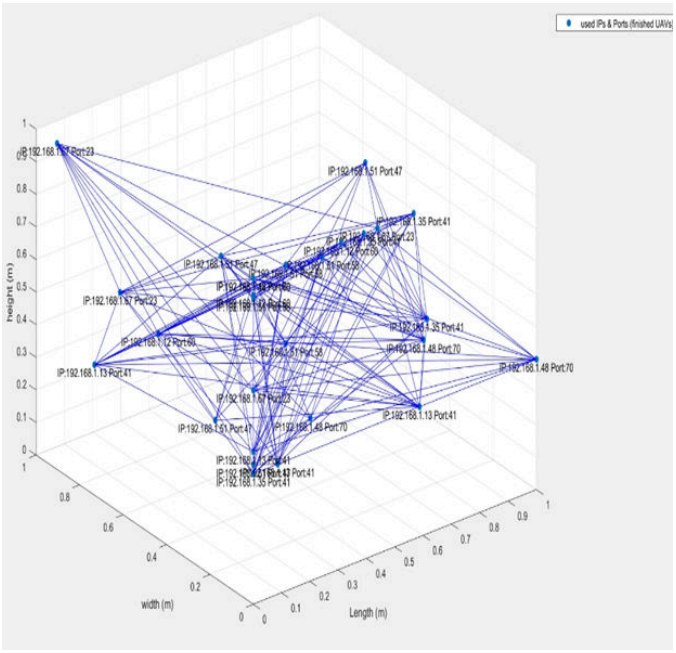

Fig. 9: Increased growth of 4 iterations

environment, UAV IPs & Ports are generated from the routing table replace the used IPs & Ports in the UAV network as shown in Figure 10. The subsequent network state at time T+1 is shown in Figure 11 Within the proposed system the routing table is responsible for transmitting the virtual IP & Ports associated with each UAV, as well as providing the hopping time for the first interval. The UAV network will receive IP & Port from the routing table. Following the predetermined hopping time has elapsed, the UAVs will transmit the used IP & Port to the honeypot network. Concurrently, the UAVs will acquire new IP & Port from the routing table. The Honeypot

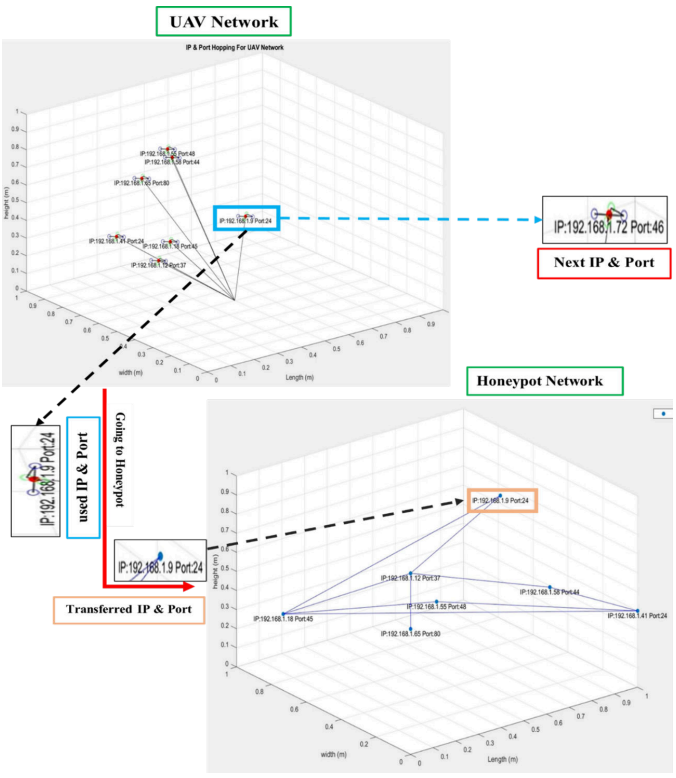

Fig. 10: Transition between UAV and Honeypot Networks at time T

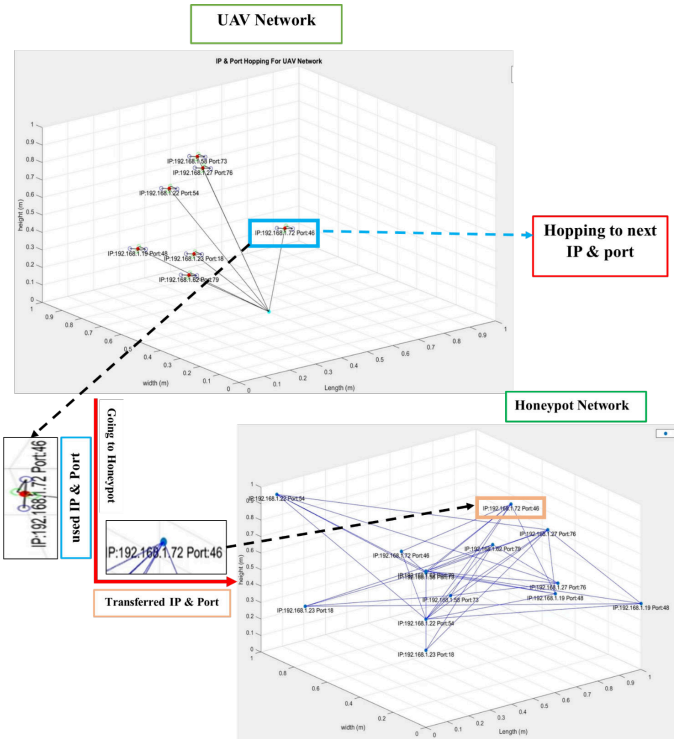

Fig. 11: Transition between UAV and Honeypot Networks at time T+1

receives the used IP & Ports from the UAV network and retains them for the purpose of monitoring any activity, with the intention of alerting the defending side.Once all possible combinations have been exhausted, the mission will conclude, resulting in the honeypot network containing the same number of nodes as the total number of combinations created by the algorithm. In our present case, this number is 700.

V. Conclusion

The use of Network-Based Moving Target Defense (NMTD) offers a compelling option for enhancing the security of Unmanned Aerial Vehicles (UAVs) due to its characteristics of being lightweight, scalable, adaptable in real-time, and cost-effective. The NMTD system enhances the defensive capabilities of UAVs by dynamically modifying network settings. This proactive approach effectively safeguards against reconnaissance and targeted cyber-attacks, hence maintaining the integrity, confidentiality, and availability of critical mission data and communications.

Acknowledgment

This work has been partially funded by the EPSRC CHEDDAR Project (Communications Hub for Empowering Distributed Cloud Computing Applications and Research) under grant numbers EP/X040518/1 and EP/Y037421/1. The authors would like to thank NCC Group for their support.

References

[1] Y. Liu, H.-N. Dai, Q. Wang, M. K. Shukla, and M. Imran, "Unmanned aerial vehicle for internet of everything: Opportunities and challenges," *Computer Communications*, vol. 155, p. 66–83, Apr. 2020. [Online]. Available: http://dx.doi.org/10.1016/j.comcom.2020.03.017

[2] S. Vashisht, S. Jain, and G. Aujla, "Mac protocols for unmanned aerial vehicle ecosystems: Review and challenges," *Computer Communications*, vol. 160, 06 2020.

[3] M. Gapeyenko, V. Petrov, D. Moltchanov, S. Andreev, N. Himayat, and Y. Koucheryavy, "Flexible and reliable uav-assisted backhaul operation in 5g mmwave cellular networks," *IEEE Journal on Selected Areas in Communications*, vol. 36, no. 11, pp. 2486–2496, 2018.

[4] B. Li, Z. Fei, and Y. Zhang, "Uav communications for 5g and beyond: Recent advances and future trends," *IEEE Internet of Things Journal* vol. 6, no. 2, pp. 2241–2263, 2019.

[5] A. Warrier, S. Al-Rubaye, D. Panagiotakopoulos, G. Inalhan, and A. Tsourdos, "Interference mitigation for 5g-connected uav using deep q-learning framework," in *2022 IEEE/AIAA 41st Digital Avionics Systems Conference (DASC)*, 2022, pp. 1–8.

[6] M. Wazid, A. K. Das, N. Kumar, A. V. Vasilakos, and J. J. P. C. Rodrigues, "Design and analysis of secure lightweight remote user authentication and key agreement scheme in internet of drones deployment," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 3572–3584, 2019.

[7] Z. Lv, S. Zhang, and W. Xiu, "Solving the security problem of intelligent transportation system with deep learning," *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, no. 7, pp. 4281–4290, 2021.

[8] T. Alladi, V. Chamola, N. Naren, and N. Kumar, "Parth: A two-stage lightweight mutual authentication protocol for uav surveillance networks," *Computer Communications*, vol. 160, 05 2020.

[9] Z. Ali, S. A. Chaudhry, M. S. Ramzan, and F. Al-Turjman, "Securing smart city surveillance: A lightweight authentication mechanism for unmanned vehicles," *IEEE Access*, vol. 8, pp. 43 711–43 724, 2020.

[10] S. Garg, G. S. Aujla, N. Kumar, and S. Batra, "Tree-based attack–defense model for risk assessment in multi-uav networks," *IEEE Consumer Electronics Magazine*, vol. 8, no. 6, pp. 35–41, 2019.

[11] V. Towhidlou, S. Al-Rubaye, and A. Tsourdos, "Lte handover design for cellular-connected aircraft," in *2022 IEEE/AIAA 41st Digital Avionics Systems Conference (DASC)*, 2022, pp. 1–5.

[12] S. Al-Rubaye, A. Tsourdos, and K. Namuduri, "Advanced air mobility operation and infrastructure for sustainable connected evtol vehicle," *Drones*, vol. 7, no. 5, 2023. [Online]. Available: https://www.mdpi.com/2504-446X/7/5/319

[13] R. Guo, B. Wang, and J. Weng, "Vulnerabilities and attacks of uav cyber physical systems," p. 8–12, 2020. [Online]. Available: https://doi.org/10.1145/3398329.3398331

[14] C. Conrad, S. Al-Rubaye, and A. Tsourdos, "Intelligent embedded systems platform for vehicular cyber-physical systems," *Electronics*, vol. 12, no. 13, 2023. [Online]. Available: https://www.mdpi.com/2079-9292/12/13/2908

[15] M. Carvalho, J. M. Bradshaw, L. Bunch, T. Eskridge, P. J. Feltovich, R. R. Hoffman, and D. Kidwell, "Command and control requirements for moving-target defense," *IEEE Intelligent Systems*, vol. 27, no. 3, pp. 79–85, 2012.

[16] M. Azab, R. Hassan, and M. Eltoweissy, "Chameleonsoft: A moving target defense system," in *7th International Conference on Collaborative Computing: Networking, Applications and Worksharing (CollaborateCom)*, 2011, pp. 241–250.

[17] Y. Huang and A. K. Ghosh, *Introducing Diversity and Uncertainty to Create Moving Attack Surfaces for Web Services*. New York, NY: Springer New York, 2011, pp. 131–151. [Online]. Available: https://doi.org/10.1007/978-1-4614-0977-9$_8$

[18] J. B. Hong and D. S. Kim, "Assessing the effectiveness of moving target defenses using security models," *IEEE Transactions on Dependable and Secure Computing*, vol. 13, no. 2, pp. 163–177, 2016.

[19] D. P. Sharma, D. S. Kim, S. Yoon, H. Lim, J.-H. Cho, and T. J. Moore, "Frvm: Flexible random virtual ip multiplexing in software-defined networks," in *2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)*, 2018, pp. 579–587.

[20] D. C. MacFarland and C. A. Shue, "The sdn shuffle: Creating a moving-target defense using host-based software-defined networking," in *Proceedings of the Second ACM Workshop on Moving Target Defense*, ser. MTD '15. New York, NY, USA: Association for Computing Machinery, 2015, p. 37–41. [Online]. Available: https://doi.org/10.1145/2808475.2808485

[21] S. Antonatos, P. Akritidis, E. P. Markatos, and K. G. Anagnostakis, "Defending against hitlist worms using network address space randomization," in *Proceedings of the 2005 ACM Workshop on Rapid Malcode*, ser. WORM '05. New York, NY, USA: Association for Computing Machinery, 2005, p. 30–40. [Online]. Available: https://doi.org/10.1145/1103626.1103633

[22] J. Jafarian, E. Al-Shaer, and Q. Duan, "Openflow random host mutation: Transparent moving target defense using software defined networking," *HotSDN'12 - Proceedings of the 1st ACM International Workshop on Hot Topics in Software Defined Networks*, 08 2012.

[23] T. E. Carroll, M. Crouse, E. W. Fulp, and K. S. Berenhaut, "Analysis of network address shuffling as a moving target defense," in *2014 IEEE International Conference on Communications (ICC)*, 2014, pp. 701–706.

[24] P. Kampanakis, H. Perros, and T. Beyene, "Sdn-based solutions for moving target defense network protection," in *Proceeding of IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks 2014*, 2014, pp. 1–6.

[25] Y.-B. Luo, B.-S. Wang, and G.-L. Cai, "Effectiveness of port hopping as a moving target defense," in *2014 7th International Conference on Security Technology*, 2014, pp. 7–10.

[26] S. Achleitner, T. F. La Porta, P. McDaniel, S. Sugrim, S. V. Krishnamurthy, and R. Chadha, "Deceiving network reconnaissance using sdn-based virtual topologies," *IEEE Transactions on Network and Service Management*, vol. 14, no. 4, pp. 1098–1112, 2017.

[27] S. Achleitner, T. La Porta, P. McDaniel, S. Sugrim, S. V. Krishnamurthy, and R. Chadha, "Cyber deception: Virtual networks to defend insider reconnaissance," in *Proceedings of the 8th ACM CCS International Workshop on Managing Insider Security Threats*, ser. MIST '16. New York, NY, USA: Association for Computing Machinery, 2016, p. 57–68. [Online]. Available: https://doi.org/10.1145/2995959.2995962

[28] J. B. Hong, S. Yoon, H. Lim, and D. S. Kim, "Optimal network reconfiguration for software defined networks using shuffle-based online mtd," in *2017 IEEE 36th Symposium on Reliable Distributed Systems (SRDS)*, 2017, pp. 234–243.

[29] Jalowski, M. Zmuda, and M. Rawski, "A survey on moving target defense for networks: A practical view," *Electronics*, vol. 11, no. 18, 2022. [Online]. Available: https://www.mdpi.com/2079-9292/11/18/2886

[30] S. T. Trassare, R. Beverly, and D. Alderson, "A technique for network topology deception," in *MILCOM 2013 - 2013 IEEE Military Communications Conference*, 2013, pp. 1795–1800.

[31] J. Hong, S. Enoch, D. Kim, A. Nhlabatsi, N. Fetais, and K. Khan, "Dynamic security metrics for measuring the effectiveness of moving target defense techniques," *Computers Security*, vol. 79, 08 2018.

.

Moving target defence in 6G UAV networks

Alismail, Ahmed

2024-09-29

Alismail A, Whitworth H, Al-Rubaye S, et al., (2024) Moving target defence in 6G UAV networks. 2024 AIAA DATC/IEEE 43rd Digital Avionics Systems Conference (DASC), 29 September 2024 - 3 October 2024, San Diego, CA, USA

https://doi.org/10.1109/dasc62030.2024.10748746