Connectivity and Intelligent Security for Digital Aviation

Huw Whitworth

Airport 4.0 is the air transport hub of the future. Advancements in wired and wireless connectivity, automation, artificial intelligence (AI), are key to improving the overall situational awareness, reduce costs and increase security. The introduction of these enablers will have repercussions both deep and wide, affecting every domain element of the aviation ecosystem from private networks to cargo management and surveillance. However, despite the impact these enablers would have on the aviation ecosystem it raises the poignant questions of:

- How would these systems integrate within our existing structures?
- What threat vectors do these introduce and how to combat to ensure a safe and efficient environment for all users?

The first point that must be conceded is that at its current state of maturity, novel communications mechanisms such as 5G cannot and should not be used to replace safety critical elements such as Air Traffic Control (ATC). However, they are more than capable of augmenting operationally critical infrastructure such as Airport Operations Control (AOC) and Airline Information Services Domain (AISD), providing high speeds and greater capacity while also enabling Internet of Things (IoT) and Critical Applications. This would be done by leveraging Network Slicing for to assure logical network isolation security in conjunction with the 5G use cases of Enhanced Mobile Broadband (eMBB), Ultra Reliable Low Latency Communication (uRLLC) and Massive Machine-Type Communications (mMTc) to ensure adherence to Quality of Service (QoS) and Service Level Agreements (SLA) requirements within a 5G heterogeneous environment. However, to assure both network isolation (Security) and SLA (Quality) adherence a method of resource allocation for network services is required. As such we consider using Markov Decision based Game Theory (Nash-Q) - Nash-Q is a reinforcement learning algorithm that improves decision-making in dynamic environments by learning from past experiences. It combines elements of game theory and Q-learning to find optimal strategies in complex, competitive scenarios - to model the strategic interaction between airport operators and their environment over time. The key feature is that the state of the system at any given time follows the Markov property, meaning that the future state depends only on the current state and not on the sequence of events leading to that state.

However, even the introduction of 5G technology for non-safety critical domains introduces a multitude of security concerns. These issues range from weak authentication, low processing power and the use of legacy assets to inconsistent security standards. In-fact the IoT HetNet principle enabled by 5G is both susceptible to and a key instrument in deploying cyber threats; as shown by the Mirai Botnet attacks. In this segment of the PhD we focus on the Availability section of the CIA triad; in particular countering Distributed Reflective Denial of Service D(r)(D)oS attacks.

The first stage was detecting and effectively classifying DDoS on networks. In other words, detecting the state change from “benign” to “attack”. For this we performed univariate time series classification that mixes convolutional and dense layers in a single neural network augmented with a gated recurrent unit. Instead of using standard , numeric representations of time series data as input to the network, the proposed method considered visual representations of it in the form of images generated via Gramian angular fields. This method allowed us to perform spacio-temporal analysis in both the long- and short-time domain. This methodology proved to be highly effective at both binary detection of network attacks but also more granular definitions of specific attack strategies being used in a computationally light manner. The advantage of this solution is that is its high adaptability and wide variety of use cases for detection a wide range of attacks with low computational power and minimal training.

Despite this success, detection of an attack is not enough. On the assumption that any cyber attacker will follow the process defined by the Lockheed Martin Cyber Kill Chain there are six stages where it is feasible to stop an attacker: Reconnaissance, Weaponization, Delivery, Exploitation, Installation or Command and Control; prior to the attacker reaching the final stage of Actions of Objectives and accomplishing their goals. Of all these stages the Reconnaissance stage was the most feasible to defend working on the principle that it is hard to exfiltrate an effective attack against an unknown entity.

To defeat and attacker at the Reconnaissance phase we proposed the use of Moving Target Defence (MTD) to deploy a Random Route Mutation (RRM) strategy deployed within the SDN controller to dynamically shift the packet routes and therefore the attack surface over time, breaking through the classic asymmetry that has previously defined the attacker defender relationship. However, to do MTD effectively, flow and network constraints had to be considered. We proposed a Model-Free (MF) Deep Reinforcement Learning (DRL) algorithm called Double Deep Q Learning with Prioritised Experienced Replay (DDQN-PER) which acted to maximise the number of shared paths for all active nodes minimising the total number of unique routes and thereby making the attack surfaces as small as possible. The method also considered the history of prior routes taken to minimise the number of repeated routes within a randomised timeframe.

At this point we must revisit the questions posed at the start of how these systems integrate and how to we combat the issues that this new topology brings to us. Within this case study we have hopefully shown that the proposed methodology is to augment, not replace. The logical isolation of secure communications on top of a public infrastructure enhances data rates and transfer reliability while minimising the OpEx for organisations. The expansion of the threat landscape has been considered and spacio-temporal machine learning analysis has been shown to be an effective and efficient solution. Finally, we have shown a scalable solution to sit within the SDN controller to mitigate the Reconnaissance phase of the cyber kill chain to protect heterogeneous networks while making sure

that user experience is not degraded, thereby ensuring the continuation of seamless aviation while ensuring security.

However, a key question remains which I would consider to be paramount to future deployment: How ensure trust and confidence in AI when deployed in a safety-critical environment when failure could be catastrophic.