63rd FITCE International Congress
26 - 28 September 2024, Kraków, Poland

Hiding Radio Communication at Battlefields Using Unmanned Vehicles

Karol Zientarski, Mykyta Muravytskyi, Krzysztof Skoś, Kamil Chełminiak, and Pawel Kulakowski

AGH University of Krakow, Poland

Abstract

Mobile Ad-hoc Networks (MANETs) are commonly used in military scenarios as they provide the flexibility required to accommodate dense, chaotic, and heterogeneous topology, operating in areas without infrastructure. In this paper, we take a closer look at a MANET tactical network, i.e., a network that consists of military units connected through a radio channel. The ad-hoc approach brings many complications, including complex routing, neighbor detection, and mobility issues. However, our work focuses on providing a disguise for communication, lowering the probability of detection (LPD) [1] of the network. Many aspects affect adversary's capabilities to detect transmission; irrespective of these aspects reducing the received power at the adversary will make the detection task more difficult. This might even result in bringing received power below the detection threshold of the adversary's receiver, thus making it practically impossible to detect the transmission. Reducing the transmission power minimizes the probability of transmission being detected. However, the network must remain connected so that all units can still communicate with one another.

From another perspective, the performance of almost any ad-hoc network can be enhanced using unmanned vehicles [2]-[4] (UxV, where "x" stands for one of the four types of vehicles – air [5], ground, surface or undersea), especially in warfare conditions where their pros are undeniable. Our goal is to design an algorithm that deploys UxVs in such a way, that the connectivity in the network is increased [6] and what is more crucial, it allows to hide the transmission from a potential adversary. We created a Python program that generates ally and enemy units on the battlefield. We assume that we know the position of all the units (both allies and enemies), the detection power threshold is -110 dBm, and we limit maximum transmission power due to battery limitations on mobile units. We use the Friis loss model to calculate the power at the receiver of each unit.

Additionally, we distinguish four types of units. Three types of allied units (i.e., the infantry, the vehicles and the UxVs) and the enemy units. All units have radio stations with a receiver sensitivity level of -110 dBm, working at the 1.5 GHz frequency [7]. The Tx powers were adapted to match the desired range in the medium with the Friis loss model.

Ally and enemy units' horizontal positions are generated using a log-normal distribution on the square field to imitate concentration on the imaginary front line, and vertical positions are generated from uniform distribution. The ally units are placed on the left 90% of the field and the enemy units are placed on the right 30% of the field, therefore there is 20% of the area, where all units can be positioned. Additionally, the ratio of generated ally vehicles to generated ally infantry units is 1:4. When units are generated, a Prim's algorithm is used [8] to build the spanning tree for the existing ally nodes and to establish connectivity in the whole network. As an edge weight in Prim's algorithm, we use the respective distance between two nodes. In the next step, we add UxVs on the radio links, where there is no connectivity between units.

Initial units’ positions are far from ideal, thus gradient minimization is performed to refine the position. For optimization, our algorithm uses a classical gradient descent. The loss function takes the UxV’s position in the topology (x, y) as an input and returns the highest power at the adversary position. It was assumed that only one node can transmit at once and two overlapping signals from different nodes do not add up at the adversary node. For each step of gradient descent, the UxV position is changed, and the loss function is calculated again. For every single iteration of the algorithm, these steps are repeated 1000 times or up to the point when the loss function decreases the power lower than the desired threshold of -110 dBm. In the next part, we add a UxV to the spanning tree by executing the following algorithm: for every enemy unit, the power received from every allied unit is calculated and the maximal one is kept. These power levels are compared among the enemy units and the maximum one is kept. The UxV is placed on the edge with the biggest power level. The algorithm ends after 6 iterations of the UxV addition and the network fine-tuning or when every enemy unit's received power signal is lower than -110 dBm. To evaluate our model, the following five metrics are used: Avg/Sum of transmitting power, network footprint, i.e., the percentage of the area coverage, number of detected units, probability of communication detection, and number of used UxVs.

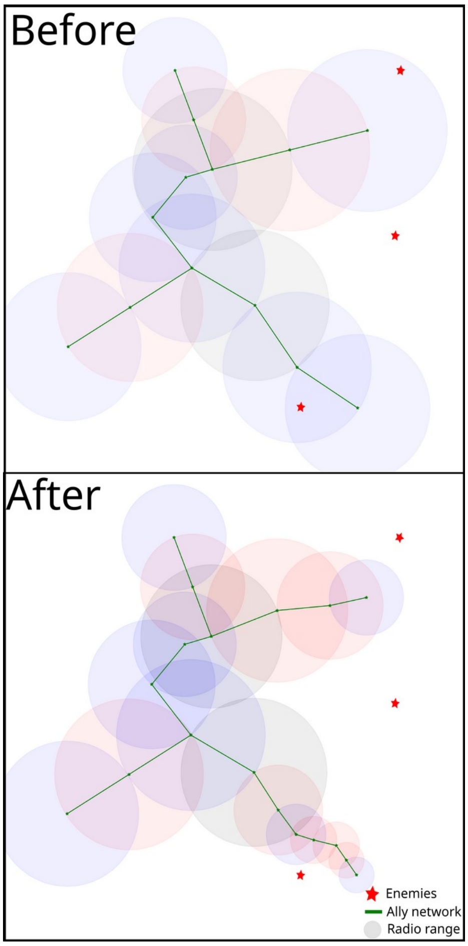

Fig. 1: Network example before and after optimization

We explored two scenarios. The first one is vital for understanding how the proposed algorithm performs in the single adversary case, where the dimensionality of the LPD problem is reduced to a single enemy unit. The adversary is very close to our units and has an extremely high probability of transmission detection. Most of the power at the enemy’s receiver comes from the two closest nodes. Our algorithm has successfully identified the problematic links where UxVs should be deployed to minimize the communication detection problem. The remaining parts of the network are intact. The deployed UxVs have created an arch further creating relay-based transmission away from the enemy. This scenario has shown that our algorithm can successfully and dynamically locate problematic areas of the topology, deploy UxVs to such areas, and calibrate their positions to minimize the probability of transmission detection. We have run 10 simulations assuming the same initial parameters except for units' positions. There are a few things to notice: the first few deployments have the most significant impact on the receiving power, thus making the following ones less meaningful. On average three UxVs are enough to bring the power below the detectability level and secure ally transmissions. In the subsequent scenario, there are multiple enemy units possible in the topology. Three enemy units are present in the topology, but only two of them are within the detectability range. As we have noticed in the single-enemy scenario, deployed UxVs form an arch around an enemy to bring the communication links as far from the enemy as possible. Another observation from the results can be made: the decreased transmitted power makes the Tx ranges smaller, thus decreasing the probability of detection by hidden enemies with unknown positions in real-life scenario. As a result of the optimization, the power for all three units drops below the threshold. In the multi-enemy scenario, an average of one UxV is needed for every enemy unit to achieve the detectability goal.

REFERENCES

[1] Brendan Sims, Mohammad Zamani, and Robert Hunjet. Distributed connectivity control in low probability of detection operations. In 2019 12th Asian Control Conference (ASCC), pages 1155–1160.

[2] Ming Zhu, Fei Liu, Zhiping Cai, and Ming Xu. Maintaining connectivity of manets through multiple unmanned aerial vehicles. Mathematical Problems in Engineering, 2015:952069, Nov 2015.

[3] Zhu Han, A. Swindlehurst, and K. Liu. Optimization of manet connectivity via smart deployment/movement of unmanned air vehicles. Vehicular Technology, IEEE Transactions on, 58:3533 – 3546, 10 2009.

[4] Andrew Coyle. Using directional antenna in uavs to enhance tactical communications. In 2018 Military Communications and Information Systems Conference (MilCIS), pages 1–6, 2018.

[5] Cory Dixon and Eric W. Frew. Optimizing cascaded chains of unmanned aircraft acting as communication relays. IEEE Journal on Selected Areas in Communications, 30(5):883–898, 2012.

[6] Jiazu Xie, Baoju Zhang, and Cuiping Zhang. A novel relay node placement and energy efficient routing method for heterogeneous wireless sensor networks. IEEE Access, 8:202439–202444, 2020.

[7] Radio specification: https://www.domotactical.com/products/sol8sdr-h2-special-role-radio-manet.

[8] R. C. Prim. Shortest connection networks and some generalizations. The Bell System Technical Journal, 36(6):1389–1401, 1957.