EUROPEAN COOPERATION
IN SCIENCE
AND TECHNOLOGY

EURO-COST

CA20120 TD(22)03019
Valencia, Spain
September 20-22, 2022

SOURCE: AGH University of Science and Technology, Poland

Minimising Network Detection Probability in MANETs Using Unmanned Vehicles

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

Corresponding author:
Pawel Kulakowski
Institute of Telecommunications
AGH University of Science and Technology
Krakow, Poland
Phone: +48 12 617 3967
Email: kulakowski@agh.edu.pl

Minimising Network Detection Probability in MANETs Using Unmanned Vehicles

Karol Zientarski, Mykyta Muravytskyi, Krzysztof Skoś, Kamil Chełminiak, and Pawel Kulakowski
AGH University of Science and Technology, Krakow, Poland

***Abstract*—History shows that information is one of the key factors in military conflicts. Therefore there is a need to maintain communication channels on the battlefield. In this document, a simulator that allows to optimise the network to minimise the risk of detection by enemies was created. The simulator, using the Prim's algorithm and the fine-tuning shows how a mobile ad-hoc network between soldiers aided with unmanned vehicles can become undetectable for enemy units.**

I. Introduction

Mobile Ad-hoc Networks (MANETs) are commonly used in military scenarios as they provide flexibility required to accommodate dense, chaotic, and heterogeneous topology, operating in areas without infrastructure.

In this paper, we take a closer look at the MANET tactical network - a network that consists of military units connected through a radio channel. The ad-hoc approach brings lots of complications, including, but not limited to, complex routing, neighbour detection and mobility issues. However, our work focuses on providing a disguise for the communication, lowering the probability of detection (LPD) of the network [1]. Many considerations affect an adversary's capabilities to detect transmission; irrespective of these considerations 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. Whilst reducing the transmission power reduces the probability of transmission being detected, 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.

In Section II we explain the scenario and methodology of our research. In Section III we describe our LPD optimisation algorithm. In Sections IV and V, we discuss the results of the research and their influence on the topic respectively.

TABLE I
Tx powers and radio ranges for different type of units

Unit type	Tx power [mW]	Radio range [km]
Infantry	25	25
Vehicle	63	40
UxV	143	60

II. Research methodology and scenario

We created a Python program that generates the ally and enemy units on the battlefield. The goal of our study was to create a network between ally units that was hard or even impossible to detect by enemy units.

A. Scenario assumptions

1) We know the exact position of all the units (ally and enemy ones) e.g. from the GPS, satellite images or another military tracking technology.
2) We use the Friis loss model and calculate power at the receiver of each unit.
3) We select a threshold power value for detection according to the exemplary radio communicator [7] used in the military communication equal to -110 dBm.
4) Radio units are portable and have a finite battery life, hence the requirement of limitation of maximum transmission power.

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 the receiver sensitivity level of -110 dBm, working on the 1.5 GHz frequency [7]. The Tx powers were adapted to match the desired range in the medium with the Friis loss model. The Tx specification is shown in Table I.

III. Algorithm

A. Generating units

Ally and enemy units are generated using a log-normal distribution on the square field. 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

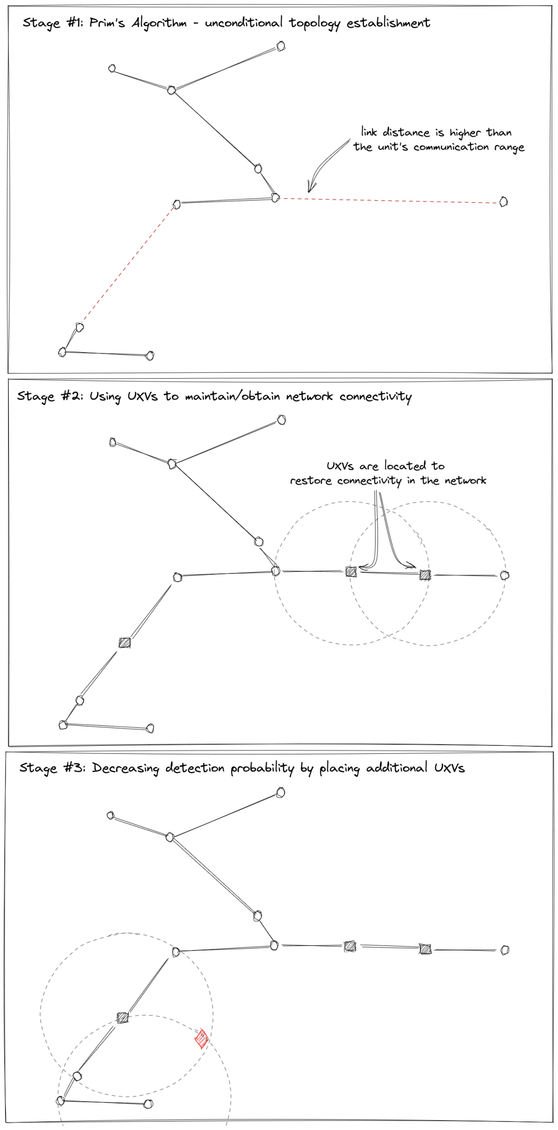

Fig. 1. Three stages of the network creation process. #1: ally unit generation and building the spanning tree, #2: obtaining connectivity and, #3: optimising the network. Legend: black circle - ally unit, black square - UxV, red rectangle - enemy unit, black line – the connection between allies, red dotted line – the connection between allies that is longer than the allies' ranges

is 20% of the area, where all units have a chance to be positioned. For example, for a field, which is 100 km long, the allies may be generated from 0 to 90 km and the enemies might be generated from 70 to 100 km. Additionally, the ratio of generated ally vehicles to generated ally infantry units is 1:4.

B. Building the spanning tree between the stations

After the generation of the units, 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.

Prim's algorithm is a greedy algorithm that finds a minimum spanning tree for a weighted undirected graph. Given a matrix of points, the algorithm starts with a designated point and an empty visited node list. In the next steps, starting from the designated point, the algorithm picks an edge with the smallest weight connected to an unvisited node. Then the newly connected node becomes designated. The algorithm ends when all nodes are visited and a connected graph with no cycles is created.

As an edge weight in Prim's algorithm, we use the respective distance between two nodes, thus in general, we decrease the probability of choosing longer edges and minimise Tx power levels. The example network topology is shown in Fig. 1, Stage #1.

In the next step, we add UxVs on the radio links, where there is no connectivity between units.

We distinguish three distinct cases of UxV deployment:

1) If the sum of the unit's radio ranges is larger than the distance between them, we add only one UxV in the middle, in between the stations.
2) If the sum of the unit's radio ranges is smaller than the distance between them, we add two UxVs on the ends of the unit's radio ranges.
3) In case when the sum of the unit's radio ranges is smaller than the distance between them and the sum of the two UxV's radio ranges is smaller than the distance between units decreased by the sum of the unit's radio ranges, two UxVs are added on the ends of the unit's radio ranges and additional (necessary) UxVs are distributed evenly on the link.

These cases are depicted in Fig. 2 and the effect of this algorithm part is shown in Fig. 1, Stage #2.

C. Optimisation

A simplified approach from the locality algorithm sets up the positions that are far from ideal, therefore there is a need to find a better position for the deployed node. This problem becomes highly complex when trying to solve it globally, however, we can consider only the nearest surroundings looking for better positioning. The optimisation problem example is shown in Fig. 1, Stage #3. Next, gradient minimisation is performed to refine the position.

For optimisation, our algorithm uses a classical gradient descent. A loss function was defined:

$$Fc(r) = \sum_{n=1}^{N} P(r_n) \tag{1}$$

where r_n is the enemy unit, N is the number of enemy units in the scenario and $P(r_n)$ is the power of the strongest signal received by the n-th enemy.

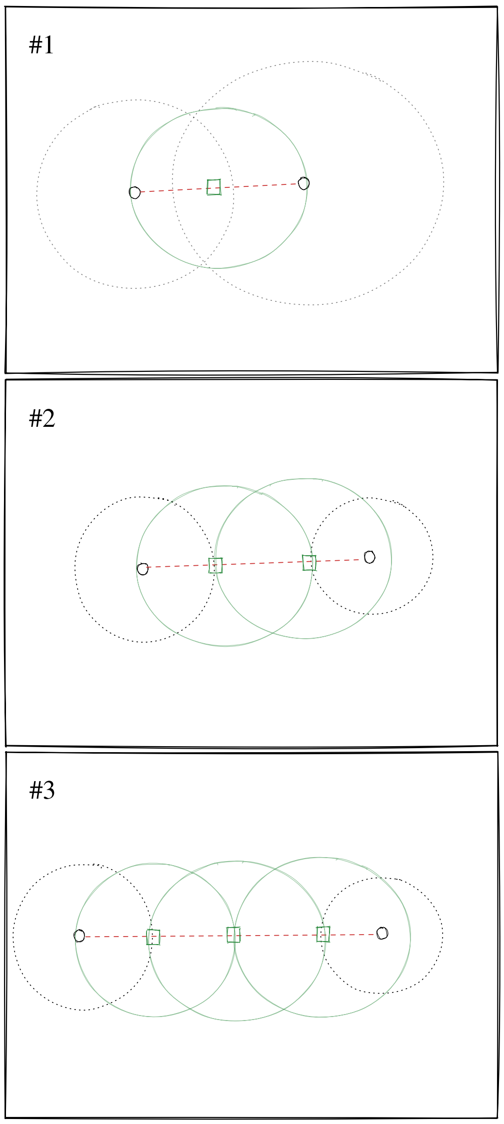

Fig. 2. Three possible scenarios during the network creation. Legend: black circle - ally unit, grey circle - ally radio range, green square - UxV, green circle - UxV radio range, red dotted line – the connection between allies that is longer than the ally's ranges

The loss function takes 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, as TDMA is commonly used in ad-hoc networks. Additionally, two overlapping signals from different nodes do not add up at the adversary node.

For each step, the UxV position is changed and the loss function is calculated again.

For every single iteration of the algorithm, the above 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.

D. *UxV addition*

In this part, we want to add UxV to the topology. To choose the best spanning tree we execute the following algorithm:

1) For every enemy unit the power received from every allied unit is calculated and the maximal one is saved.
2) These power levels are compared among the enemy units and the maximal one is saved
3) Let E be the chosen enemy and A be the ally, from which E received the signal with the largest power. The UxV is placed on the E's longest egde.

E. *Algorithm end*

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.

F. *Metrics*

To evaluate our model, the folowing five metrics are used.

1) Avg/Sum of transmitting power, related to battery consumption
2) Network footprint – the percentage of the area coverage calculated as the quotient of the area covered by the signal and the total area (to simplify calculations the coverage is checked in the lattice points 500m apart)
3) Number of detected units
4) Probability of communication detection
5) Number of used UxVs

IV. Results

The proposed algorithm has been tested through numerous simulation runs. Some of the results are presented and discussed below.

A. *Single enemy unit*

The first scenario 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. This results allow us to compare our model to the one presented in [9].

It is shown in Fig. 3 that 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 is coming from the two closest nodes. It's obvious that the link between them is the key point of optimisation.

Our algorithm has successfully identified the problematic links where UxVs should be deployed to minimise the communication detection problem. The results are shown in Fig. 4. It's worth noticing that the remaining

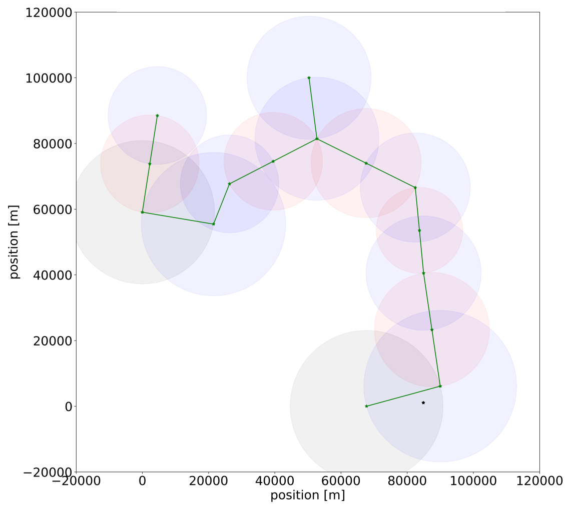

Fig. 3. Topology without optimisation with one enemy. Black star - enemy unit, a green star with grey circle – a vehicle with its radio range marked, a green star with blue circle - infantry with its radio range marked, a green star with red circle - UxV with its radio range marked, green line – the connection between ally units

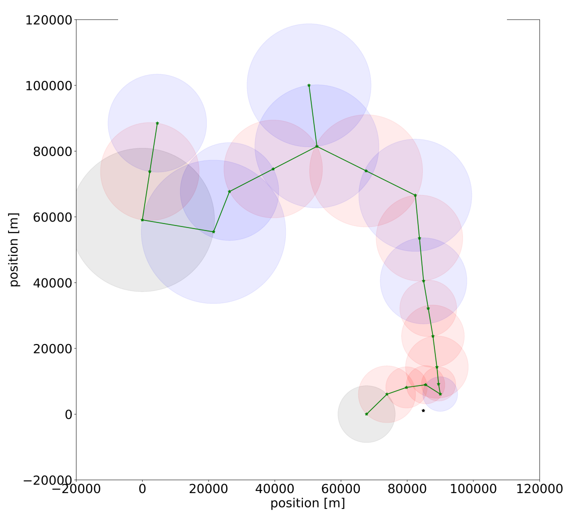

Fig. 4. Topology with optimisation with a single enemy. Black star - enemy unit, a green star with grey circle – a vehicle with its radio range marked, a green star with blue circle - infantry with its radio range marked, a green star with red circle - UxV with its radio range marked, green line – the connection between ally units

parts of the network are intact, meaning no UxVs are deployed there, as such deployment would not have any impact on the power at the enemy's position. Deployed UxVs have created an arch further creating relay-based transmission away from the enemy.

Fig. 5 depicts the received power as a function of number of deployed UxVs for the topology shown in Fig. 3. The most significant drop is attained after the introduction of the second UxV. This can be easily

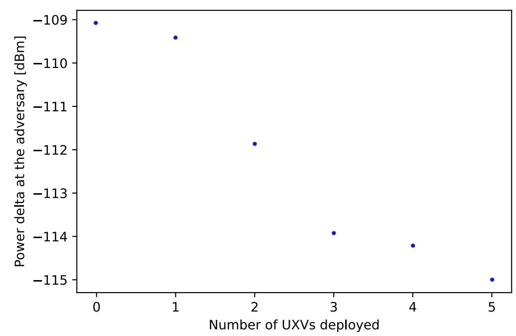

Fig. 5. Received power as a function of several deployed UxV for the topology shown in Fig. 3-4

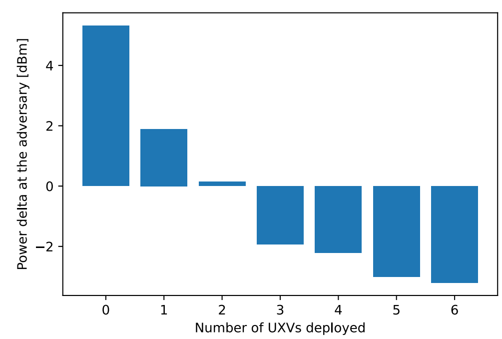

Fig. 6. Mean difference between the power received at the adversary and the detection threshold as a function of the number of the UxVs deployed for the one enemy unit scenario

explained by the closest ally unit having two neighbour connections that require optimisation. By putting UxVs on those links we can bring the receiving power down below the detectability threshold.

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 achieve the defined goal, which is minimising the probability of transmission detection.

We have run 10 simulations assuming the same initial parameters except for units' positions. The averaged results are presented in Fig. 6. To highlight the receiving power changes, a difference of power and the detection threshold is used as a metric. In this metric the positive value means that the signal level is above the detectability threshold and the negative means being below the threshold. 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.

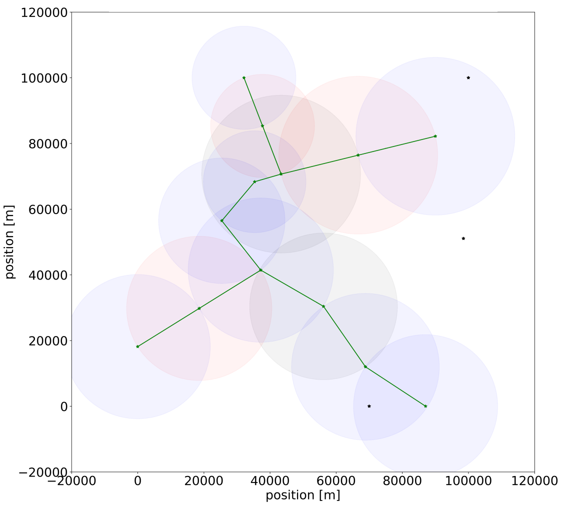

Fig. 7. Topology without optimisation with multiple enemies. Black star - enemy unit, a green star with grey circle – a vehicle with its radio range marked, a green star with blue circle - infantry with its radio range marked, a green star with red circle - UxV with its radio range marked, green line – the connection between ally units

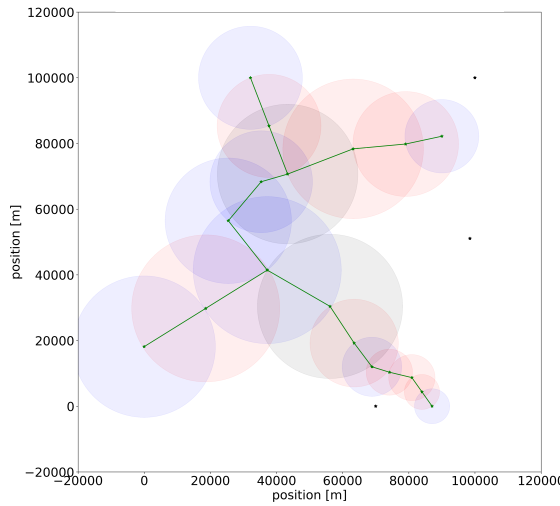

Fig. 8. Topology with optimisation with multiple enemies. Black star - enemy unit, a green star with grey circle – a vehicle with its radio range marked, a green star with blue circle - infantry with its radio range marked, a green star with red circle - UxV with its radio range marked, green line – the connection between ally units

Very similar results were attained in publication [9]. The following conclusion matches the results of our simulations: 'A single UxV will significantly reduce the large peaks in the power seen at the adversary, the extra UxVs still reduce the received power but not as significantly'. However it's worth mentioning that initial assumptions for the simulations are different, yet final results are comparable.

B. Multiple enemy units

Our algorithm has made a step further assuming that there are multiple enemy units possible in the topology. As there is very little research on optimising topology in such scenarios, the results are discussed but not compared.

As previously, the selected topology (shown in Fig. 7) is used to present the performance of the algorithm.

Three enemy units are present in the topology, but only two of them are within the detectability range. Compared to the single enemy scenario, the complexity increases: there are two problematic areas to consider and to deploy UxV units.

As it is shown in Fig. 8, the algorithm has decided to put a single UxV to reduce power at the top adversary and the rest at the bottom, which reflects the complexity differences of the problematic areas. As we've 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 when reaching the potential enemy location. It makes sense as there might

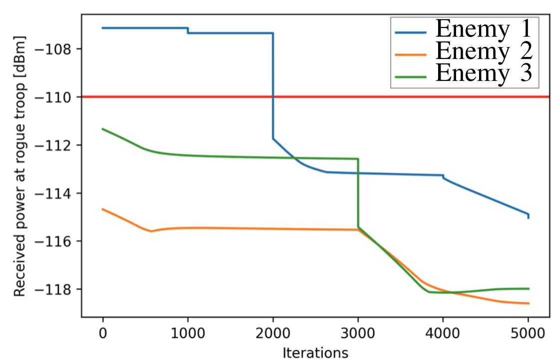

Fig. 9. Changes in power levels received by enemy units change over several optimisation algorithm iterations. Every 1000 iterations a new UxV is added to the network. The Red line marks the detection threshold

be enemy units we are unaware of and the closer to the enemy positions we get, the less of a communication footprint we want to leave.

Fig. 9 shows how power levels at enemy positions change over several algorithm iterations. In the beginning, we can see that only one adversary receives power above the threshold. The other one that was in the range has suffered from fading effect. As a result of the optimisation, the power for all three units drops below the threshold. As already mentioned, the bottom area had a double link problem therefore two UxVs were required.

Same as in the previous scenario, we have run several simulations and averaged the results, which are presented in Fig. 10. In the multi-enemy scenario, an average of one UxV is needed for every enemy unit to achieve the

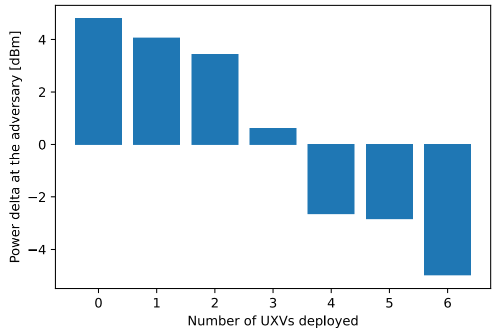

Fig. 10. Mean difference between the power received at the adversary and the detection threshold as a function of the number of the UxVs deployed for the multiple enemy units scenario

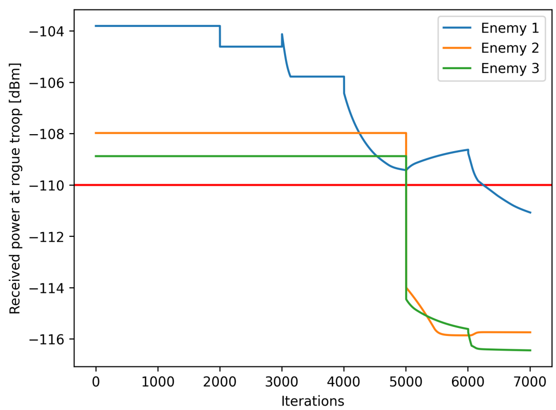

Fig. 11. Changes in power levels received by enemy units change over several optimisation algorithm iterations. Every 1000 iterations a new UxV is added to the network. The Red line marks the detection threshold

detectability goal.

Finally in Fig. 11, another example is shown how the power levels are minimised at enemy positions. However, in this situation, all three enemies were generated in positions where they receive power above the threshold. In the end, our algorithm was able to decrease the received power at all adversaries below the threshold, thus completely hiding the communication.

V. Conclusions

In this paper, we have described the algorithm that uses unmanned vehicles to minimise communication detection probability also known as the LPD problem. Several simulations have been performed and results have been investigated. It has been shown that the prudent placement of UxV relays can have a significant impact on signal power level at the adversary's position, thus lowering the probability of transmission getting detected. We have used a complex multi-dimensional optimisation technique, that has proved to be effective when dealing with several adversary units within a single topology. However, as some of the assumptions and simulation parameters are far from being realistic, further research would be needed and enhancement of the algorithm required.

VI. Future work and discussion

As our goal was limited to show how UxVs can be used to grapple with LPD problem, we made some assumptions to simplify other less related factors. For instance, we assumed that MANET had a kind of distributed intelligence: all of the positions were precisely known in every node, which allowed us to easily build a spanning tree of communication links. A more realistic approach as suggested in [10] would be to accept limited available information in each node and a dynamic topology where nodes could move around.

Another simplification included trivialising the propagation models. In this work we decided to stick to the simplest radio environment possible, as simulating close-to-realistic environments was not the goal of this paper.

Further work could focus on these aspects, develop more realistic UxV behaviour, and dynamic complex environment, introduce incomplete information or suggest a different approach and compare the results.

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.

[9] Andrew Coyle, Benjamin Campbell, and Robert Hunjet. Minimising the network detection probability using autonomous vehicles. In *2020 Military Communications and Information Systems Conference (MilCIS)*, pages 1–6, 2020.

[10] Ning Li, J.C. Hou, and L. Sha. Design and analysis of an mst-based topology control algorithm. *IEEE Transactions on Wireless Communications*, 4(3):1195–1206, 2005.