Staying Hidden at Battlefields While Communicating via Unmanned Vehicles

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

AGH University of Krakow, Kraków, Poland

https://doi.org/10.26636/jtit.2025.FITCE2024.2086

Abstract — History shows that information is one of the key factors in military conflicts. During military conflicts, there is a need to maintain a communication channel on the battlefield while staying hidden from the enemy. In this paper, we present a simulator that allows to use a communication network and minimize the risk of being detected by the enemy. The simulator, using the Prim algorithm and fine-tuning, shows how a mobile ad-hoc network established between soldiers with the aid of unmanned vehicles, i.e. drones, may become undetectable for the enemy by properly optimizing drone positions.

Keywords — low probability detection, MANET, Prim algorithm, RSSI, UxV

1. Introduction

Mobile ad-hoc networks (MANETs) are commonly used in military scenarios, as they provide the flexibility required to accommodate a dense, chaotic and heterogeneous topology and are capable of operating in areas without any infrastructure.

In this paper, we take a closer look at a tactical MANET network composed of military units connected through a radio channel. The ad-hoc approach brings lots of complications including, but not limited to, complex routing, neighbor detection, and mobility issues. However, our work focuses on providing a disguise for communication, thus lowering the probability of detection (LPD) of the network [1].

Many factors affect the ability of an adversary to detect a radio transmission. Regardless of these, reducing the power received by the foe will make the detection task more difficult. This could even result in bringing the received power below the detection threshold of the adversary's receiver, thus making it impossible to detect the transmission. Although reducing transmission power limits the probability of it being detected, the network must remain operational, so that all units can still communicate with one another.

Despite that, 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 underwater), especially in warfare conditions where their advantages are undeniable. Our goal is to design an algorithm that deploys UxVs in such a way that connectivity within the network is increased [6] and, more crucially, it allows the transmission from a potential adversary.

This paper is based on the presentation made at the 63rd FITCE 2024 international congress and titled "Hiding Radio Communication at Battlefields Using Unmanned Vehicles". However, the scope of our work is more extensive, as it includes algorithm details, additional scenarios, and comprehensive analysis of results, along with an in-depth discussion. The rest of this paper is organized as follows. In Section 2, we discuss previous works related to our topic. In Section 3, we explain the scenario and methodology of our investigation. In Section 4, we describe the LPD optimization algorithm. In Sections 5 and 6, we discuss the results of the research and their impact on the topic, respectively.

2. Related Work

There are several approaches to reducing the probability of detection of a network (LPD). For example, [7] presents an LPD algorithm for mobile networks, including field tests, based on the received signal strength indicator (RSSI) with a combination of the minimum spanning tree (MST) topology, referred to as RSSI distributed MST (RDMST). In [8], the authors explore possibilities of minimizing area coverage with enemy unit avoidance. Furthermore, in [9], a novel device capable of emulating networks for LPD problems is shown.

Furthermore, in [10], an idea of an LPD mobile network using UAV swarms was proposed based on numerous aerial devices that create, from scratch, and entire network that is hidden from enemy ground units. However, it is assumed that the distance from adversaries is known and calculated from RSSI measurement at the enemy receivers.

The topic of MANET networks covers a broad range of issues, and some authors conducted valuable research in the form of surveys. In [11], the authors discussed recent advances in protocol development and MANET applications. Next, it is known that the development of machine learning and artificial intelligence creates new possibilities for network optimization. In [12], AI-based MANET routing protocols, including both machine learning and biologically inspired approaches, are discussed.

On the other hand, the review featured in [13] presents a different approach to MANET cybersecurity, discussing a galore

Tab. 1. Simulation parameters.

Parameter	Value
Infantry Tx power	25 mW
Infantry radio range	25 km
Vehicle Tx power	63 mW
Vehicle radio range	40 km
UxV Tx power	143 mW
UxV radio range	60 km
Number of ally units	10
Number of ally infantry units	8
Number of ally vehicle units	2
Number of enemy units	3
Number of UxV adding cycles	6
Gradient descent iterations	1000
Map size	100 ×100 km
Map fraction occupied by allies	90%
Map fraction occupied by enemies	30%
Precision for map coverage calculations	0.2 km
Gradient learning rate	6

of security issues and cyberattacks aimed at MANET susceptibilities. The problem of hiding a whole network is only one of the vulnerabilities addressed in this paper. However, it is important to consider other cybersecurity challenges when designing a MANET.

In this work, we use the Prim algorithm to create minimum spanning trees (MSTs) [14]. Despite being an old approach, it is still used for present applications [15]. It is known that there are numerous other algorithms suitable for MST creation, e.g. Kruskal or Boruvka [16]. However, when comparing time complexities, Prim's is:

$$\mathrm{O}\big((V-1)\log(V)+E\log(V)\big)$$

and Kruskal's is:

$$\mathrm{O}\big(E\log(E)+V\log(V)\big)\,,$$

where E is the number of edges and V is the number of vertices. Furthermore, in practice, the complexities can be simplified to $\mathrm{O}(E\log(V))$ and $\mathrm{O}(E\log(E))$, respectively [17].

When the initial number of edges is much greater than the number of initial vertices, the Prim algorithm is more efficient [18]. Boruvka's algorithm has a time complexity of $\mathrm{O}(E\log(V))$, making it only as fast as Prim's algorithm [19].

3. Research Methodology and Scenario

We created a Python simulator that generates the required ally and enemy units on the battlefield. The goal of our study was to create a network between allies that was hard to detect by their enemies. The simulation parameters are presented in Tab. 1.

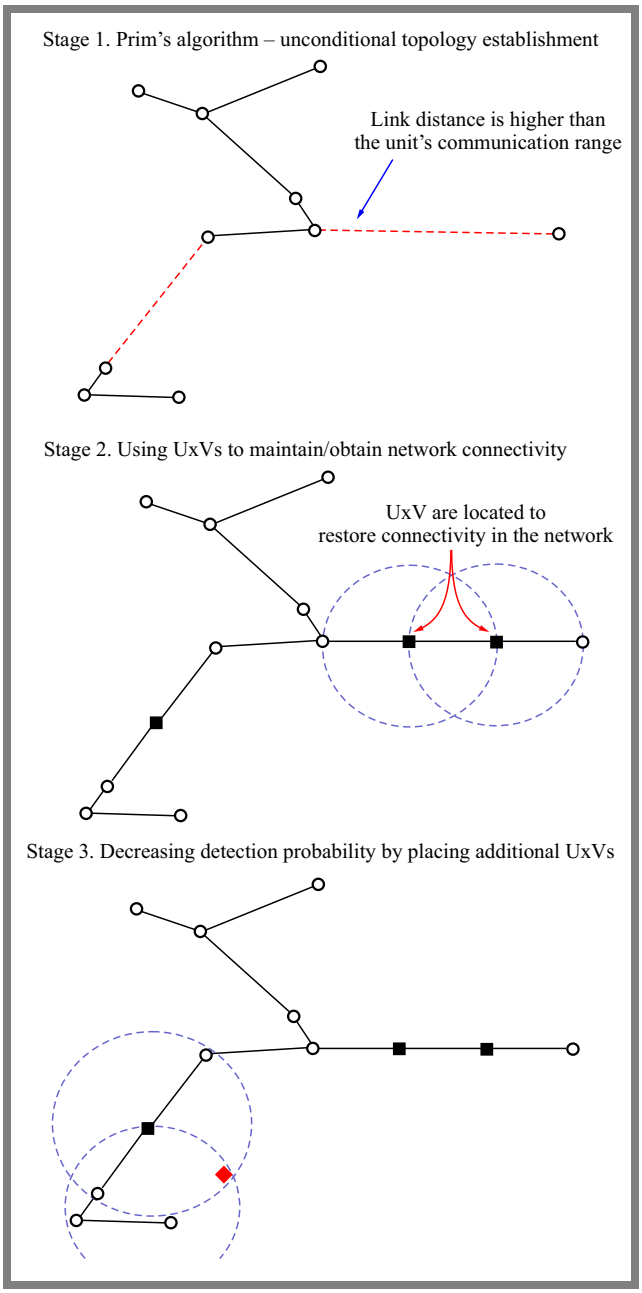

Fig. 1. Three stages of the network optimization process: 1) generating allied units generating allied units and building the spanning tree, 2) obtaining connectivity, and 3) optimizing the network. Legend: a black circle means an allied unit, a black square is UxV, a red rectangle stands for an enemy unit, a black line illustrates a connection between allies, a red dotted line identifies a connection between the allies that is longer than the allies' range.

Scenario assumptions:

1) The exact position of all the units (allied and enemy) is known, e.g. from GPS, satellite images, or other military tracking technologies.
2) We use the Friis loss model and calculate the power at the receiver of each unit.

3) We select a threshold detection power value according to an exemplary radio communicator used in military communication, equaling –110 dBm.
4) Radio units are portable and have a finite battery life, hence the requirement to limit the maximum transmission power.

In addition, we distinguish four types of units. Three types of allied units (i.e. the infantry, vehicles, and UxVs) and enemy units. All of them have radio stations with a receiver sensitivity of –110 dBm, operating at the 1.5 GHz frequency. The transmitter (Tx) powers were adapted to match the desired range in the medium with the Friis loss model. The detailed Tx specification is shown in Tab. 1.

4. Algorithm

4.1. Generating Units

Allied and enemy units are generated on a square field using log-normal distribution. Allies are placed on the left 90% of the field, and enemy units are placed on the right. Therefore, there exists a 20% of the area where all units have a chance of being positioned.

For example, for a field that is 100 km long, the allies may be generated within 0 to 90 km, and the enemies might be generated from 70 to 100 km. Furthermore, the ratio between allied vehicles and infantry units is 1:4.

4.2. Building the Spanning Tree Between the Stations

After unit generation, the Prim algorithm [14] is used to build the spanning tree for existing ally nodes and establish connectivity throughout the entire network. It 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 list of visited nodes.

In the subsequent 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 the Prim algorithm, we use the respective distance between two nodes. Thus, in general, we decrease the probability of choosing longer edges and minimize the power levels of Tx. The topology of the network is shown in Fig. 1, stage 1.

In the next step, we add UxVs to 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 at the ends of the unit's radio ranges.

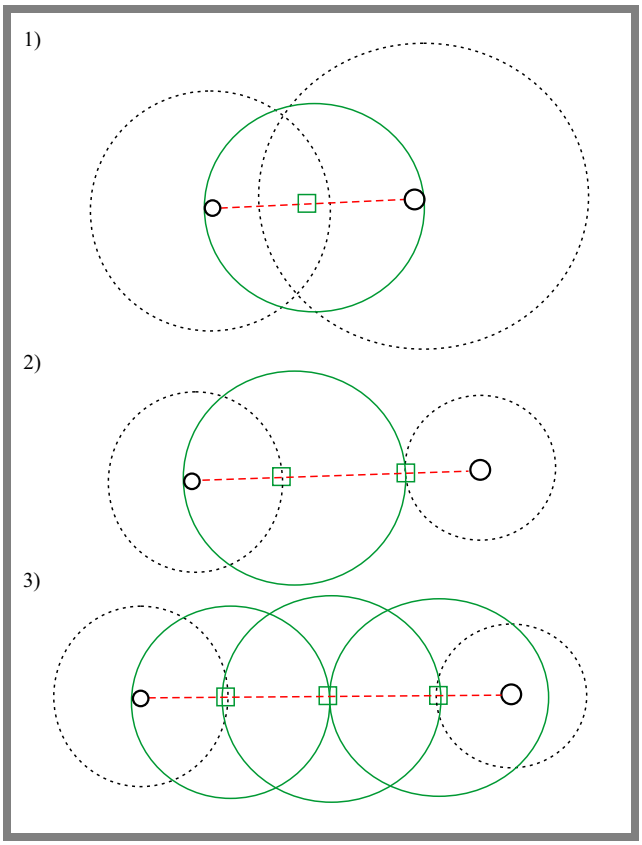

Fig. 2. Three possible scenarios taken into consideration during the network design phase. Legend: a black circle shows an allied unit, a dashed circle stands for allied radio range, a green square is an UxV, a green circle covers the UxV radio range, a red dotted line identifies the connection between allies that is longer than the range of the ally.

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 part of the algorithm is shown in Fig. 1, stage 2.

4.3. Optimization

A simplified approach from the locality algorithm sets up positions that are far from ideal. Therefore, a better position for the deployed node is needed. This problem becomes highly complex when trying to solve it globally; however, we can consider only the nearest surroundings, looking for a better positioning. The example of the optimization problem is shown in Fig. 1, stage 3. Next, gradient minimization is performed to refine the position.

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

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

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.

The loss function takes the position of UxV in the topology (x, y) as input and returns the highest power in the adversary position. It was assumed that only one node can transmit simultaneously, as TDMA is commonly used in ad-hoc networks.

Additionally, two overlapping signals from different nodes do not show 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 where the loss function decreases to a power lower than the desired threshold of –110 dBm.

4.4. UxV Addition

In this part, the UxV is added 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 edge.

4.5. Algorithm End

The algorithm ends after 6 iterations of adding the UxV and fine-tuning the network, or when the received power signal is less than –110 dBm.

4.6. Metrics

To evaluate the model, the following 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 500 m apart.
3) Number of detected units.
4) Probability of communication detection.
5) Number of used UxVs.

5. Results

The proposed algorithm has been evaluated in numerous simulations runs. Some of the results are presented and discussed in this Section.

5.1. 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. These results allow us to compare the presented model with the one from [20].

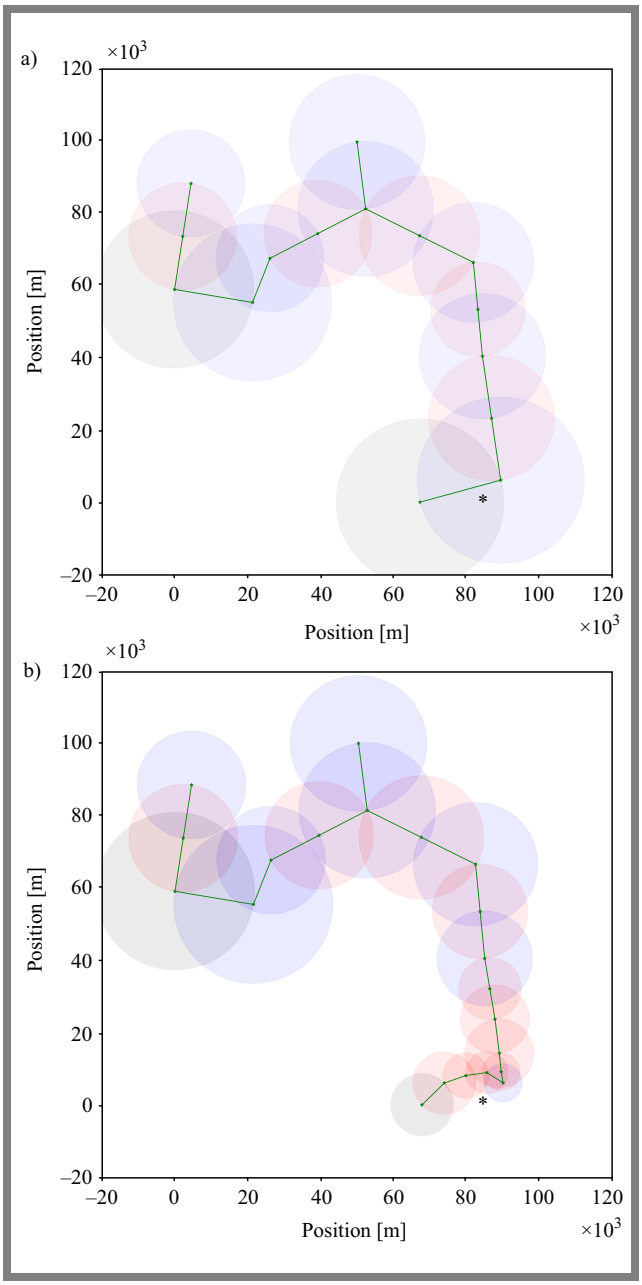

Fig. 3. Topology without optimization with a single enemy a) and with optimization b). A black star stands for an enemy unit, a green star with a gray circle means a vehicle with its radio range marked, a green star with a blue circle is an infantry unit with its radio range marked, a green star with a red circle denotes an UxV with its radio range marked, and a green line shows a connection between allies.

It is shown in Fig. 3a that the adversary is very close to our units and has an extremely high probability of transmission detection. Most of the power in the enemy's receiver is coming from the two closest nodes. It is obvious that the link between them is the key point for optimization.

Our algorithm has successfully identified the problematic links where UxVs should be deployed to minimize the probability of communication being detected. The results are shown

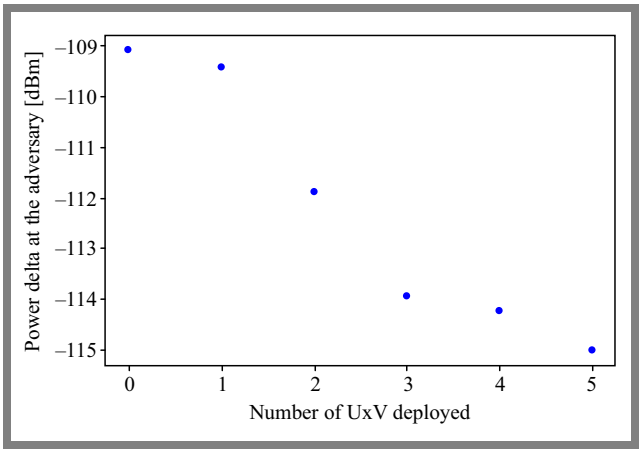

Fig. 4. Received power as a function of several deployed UxV for the topologies shown in Fig. 3.

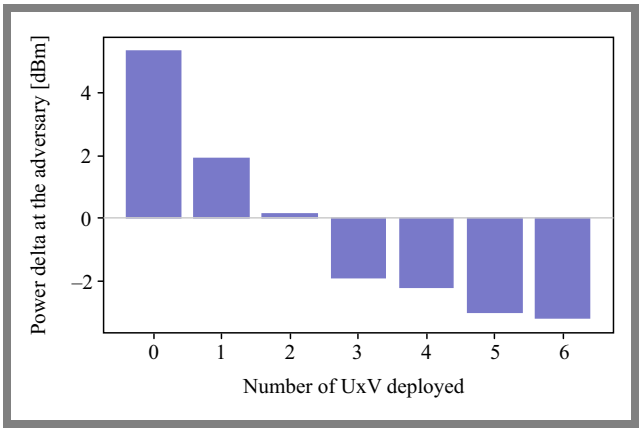

Fig. 5. Mean difference between the power received by the adversary and the detection threshold as a function of the number of UxVs deployed for one enemy unit.

in Fig. 3b. It should be noted that the remaining parts of the network are intact, which means that no UxVs are deployed there, as such a deployment would not exert any impact on the power at the enemy's position. The deployed UxVs have formed an arch, moving the relay-based transmission further away from the enemy.

Figure 4 shows the received power as a function of the number of UxV deployed for the topology shown in Fig. 3b. The most significant drop is achieved after the introduction of the second UxV. This can be easily explained by the closest ally unit having two neighboring connections that require optimization. By putting UxVs on those links, we can bring the receiving power down, below the detectability threshold.

This scenario has shown that the investigated algorithm is capable of successfully and dynamically locating problematic areas of the topology, deploying UxVs to such areas, and calibrating their positions to achieve the defined goal, namely, minimizing the probability of transmission detection.

We have run 10 simulations based on the same initial parameters, except for the positions of the units. The averaged results are presented in Fig. 5. To highlight changes in receiving power, the difference in power and detection threshold is used as a metric. In this metric, a positive value means

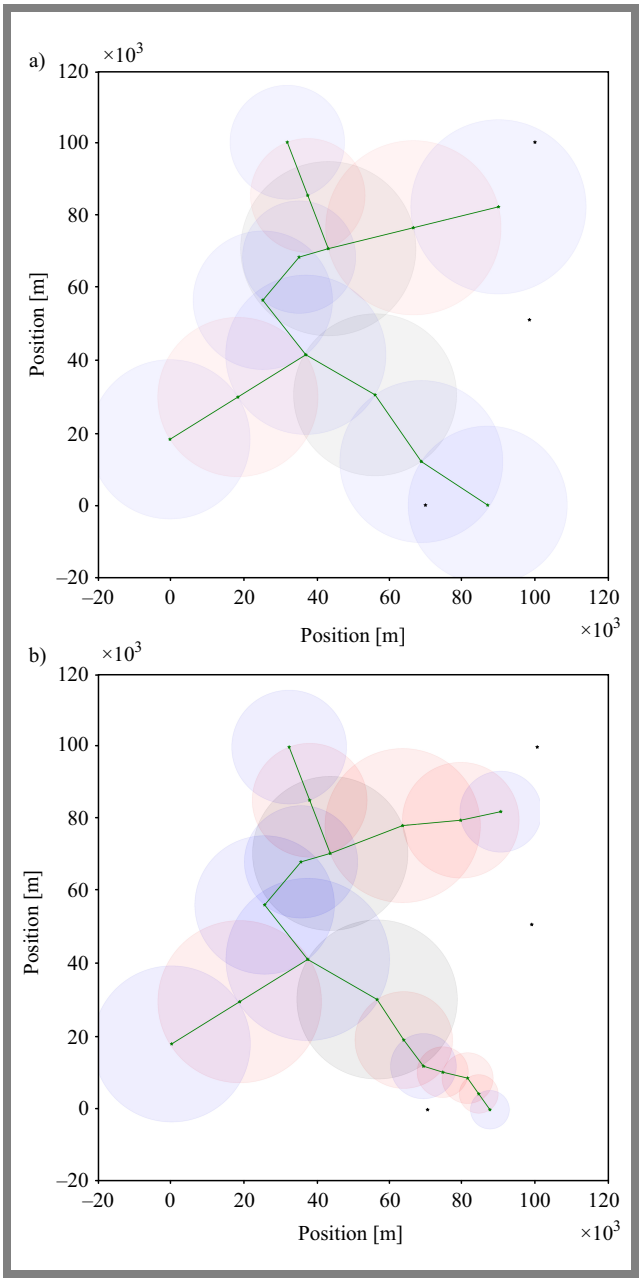

Fig. 6. Topology without optimization with multiple enemies a) and with optimization b). A black star identifies an enemy unit, a green star with a gray circle shows a vehicle with its radio range marked, a green star with a blue circle stands for an infantry unit with its radio range marked, a green star with a red circle is an UxV with marked radio range, and a green line identifies a connection between allied units.

that the signal level is above the detectability threshold, and a negative value means that the signal level is below the said threshold.

There are a few things to note. The first few deployments have the most significant impact on the receiving power, making the following ones less meaningful. On average, three UxVs are enough to bring the power below the detectability level and secure allied transmissions.

Very similar results were obtained in publication [20]. Both scenarios are based on similar assumptions, where only one

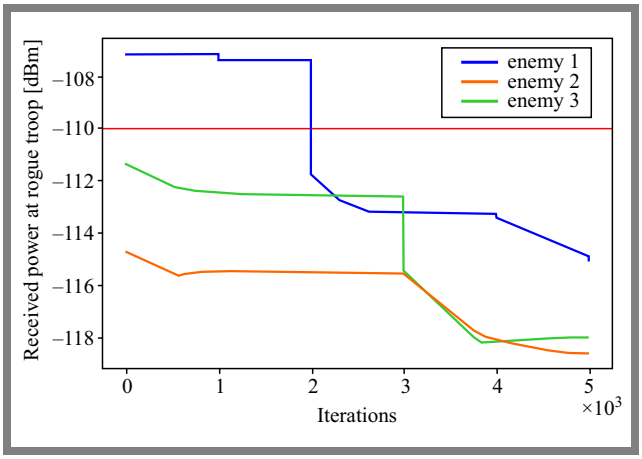

Fig. 7. Changes in power levels received by enemy units vary over several iterations of the optimization algorithm. Every 1000 iterations, a new UxV is added to the network. The red line marks the detection threshold.

enemy and UxVs are added to the network. In [20], initially, the units are not energetically constrained, i.e., the network will always be connected without any initial placement of the UxV, which may result in a larger coverage of the network area and a higher probability of detection.

However, both results show that the final results are comparable. The most significant UxVs are placed in the first iteration, because they cause the most prominent reduction in signal strength received by adversaries. Subsequent UxV addition cycles also cause a decrease in the received signal strength, but the change is more subtle. At the same time, this change may be critical for the detection of the network.

5.2. Multiple Enemy Unit

Our algorithm has taken a step further, assuming that multiple enemy units may be present within the topology. As there is very little research on optimizing topology in such scenarios, the results are discussed, but not compared.

As it was the case previously, the selected topology (shown in Fig. 6a) is used to test the performance of the algorithm.

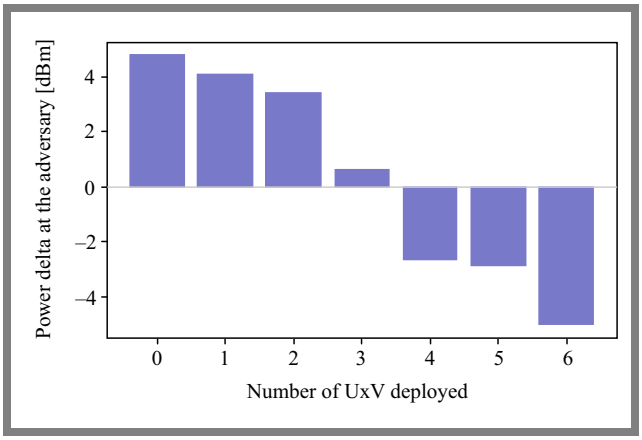

Fig. 8. Mean difference between the power received at the adversary and the detection threshold as a function of the number of UxVs deployed in the scenario with multiple enemy units.

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

As shown in Fig. 6b, the algorithm has decided to reduce power by adding a single UxV above the adversary, and the rest at the bottom, reflecting the differences in the complexity of the problematic areas. As we have noticed in the single-enemy scenario, the deployed UxVs form an arch around an enemy to bring the communication links as far away from the enemy as possible.

Another observation can be made from the results. The decreased transmitted power makes the Tx ranges smaller when reaching the potential enemy location. This makes sense, as there might be enemy units we are unaware of, and the closer to the enemy positions we get, the less of a communication footprint we are willing to leave.

Figure 7 shows how the power levels at the enemy positions change over several iterations of the algorithm. Initially, we can see that only one adversary receives power above the threshold. The other in range suffered from a fading effect. As a result of the optimization process, 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.

Similarly, as in the previous scenario, we have run several simulations and averaged the results, which are presented in Fig. 8. In the multi enemy scenario, an average of one UxV is needed for every enemy unit to achieve the detectability goal.

Finally, another example shown in Fig. 9 illustrates how the power levels are minimized at enemy positions. However, in this case, all three enemies were generated at positions where they received power above the threshold. In the end, our algorithm was able to decrease the power received by all adversaries below the threshold, thus completely hiding the communication.

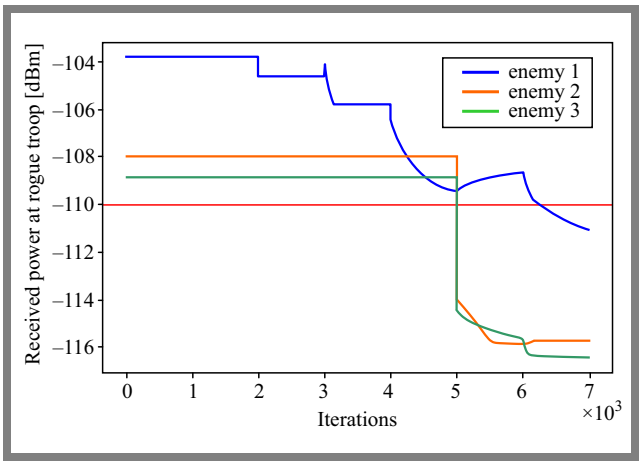

Fig. 9. Changes in power levels received by enemy units vary over several iterations of the optimization algorithm. Every 1000 iterations, a new UxV is added to the network. The red line marks the detection threshold.

6. Conclusions

In this paper, we have described an algorithm that uses unmanned vehicles to minimize the probability of communication detection, also known as the LPD problem. Several simulations have been performed, and the results have been investigated. The prudent placement of UxV relays has been shown to have a significant impact on the signal power level at the adversary position, thus reducing the probability of the transmission being detected.

We have used a complex multidimensional optimization technique that has proved to be effective when dealing with several adversary units within a single topology. However, since some of the assumptions and simulation parameters are far from realistic, more research would be needed to improve the algorithm.

7. Future Prospects and Discussion

As our goal was limited to showing how UxVs can be used to deal with the LPD problem. Therefore, we made some assumptions to simplify other less related factors. For example, we assumed that MANET featured some kind of distributed intelligence: all 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 [21], would consists in accepting the limited amount of information available in each node and a dynamic topology in which the nodes could move.

Another simplification included trivializing 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 the following aspects: developing more realistic UxV behavior and dynamic complex environments, introducing incomplete information, suggesting a different approach, and comparing the results.

References

[1] B. Sims, M. Zamani, and R. Hunjet, "Distributed Connectivity Control in Low Probability of Detection Operations", *2019 12th Asian Control Conference (ASCC)*, Kitakyushu, Japan, 2019.

[2] M. Zhu, F. Liu, Z. Cai, and M. Xu, "Maintaining Connectivity of MANETs Through Multiple Unmanned Aerial Vehicles", *Mathematical Problems in Engineering*, art. no. 952069, 2015 (https://doi.org/10.1155/2015/952069).

[3] Z. Han, A.L. Swindlehurst, and K.J.R. Liu, "Optimization of MANET Connectivity via Smart Deployment/movement of Unmanned Air Vehicles", *IEEE Transactions on Vehicular Technology*, vol. 58, pp. 3533–3546, 2009 (https://doi.org/10.1109/TVT.2009.2015953).

[4] A. Coyle, "Using Directional Antenna in UAVs to Enhance Tactical Communications", *2018 Military Communications and Information Systems Conference (MilCIS)*, Canberra, Australia, 2018 (https://doi.org/10.1109/MilCIS.2018.8574110).

[5] C. Dixon and E.W. Frew, "Optimizing Cascaded Chains of Unmanned Aircraft Acting as Communication Relays", *IEEE Journal on Selected Areas in Communications*, vol. 30, no. 5, pp. 883–898, 2012 (https://doi.org/10.1109/JSAC.2012.120605).

[6] J. Xie, B. Zhang, and C. Zhan, "A Novel Relay Node Placement and Energy Efficient Routing Method for Heterogeneous Wireless Sensor Networks", *IEEE Access*, vol. 8, pp. 202439–202444, 2020 (https://doi.org/10.1109/ACCESS.2020.2984495).

[7] A. Coyle, A. Gupta, and B. Campbell, "RDMST- A Novel Distributed Topology Control Algorithm for Low Probability of Detection Mobile Communication Networks", *Procedia Computer Science*, vol. 205, pp. 68–77, 2022 (https://doi.org/10.1016/j.procs.2022.09.008).

[8] A. Neumann *et al.*, "Diversity Optimization for the Detection and Concealment of Spatially Defined Communication Networks", *Proc. of the Genetic and Evolutionary Computation Conference*, pp. 1436–1444, 2023 (https://doi.org/10.1145/3583131.3590405).

[9] J. Yockey, B. Campbell, A. Coyle, and R. Hunjet, "Emulating Low Probability of Detection Algorithms", *2020 30th International Telecommunication Networks and Applications Conference (ITNAC)*, Melbourne, Australia, 2020 (https://doi.org/10.1109/ITNAC50341.2020.9315105).

[10] J. Fan *et al.*, "Area Surveillance with Low Detection Probability Using UAV Swarms", *IEEE Transactions on Vehicular Technology*, vol. 73, pp. 1736–1752, 2024 (https://doi.org/10.1109/TVT.2023.3318641).

[11] D. Ramphull, A. Mungur, S. Armoogum, and S. Pudaruth, "A Review of Mobile Ad Hoc Network (MANET) Protocols and Their Applications", *2021 5th International Conference on Intelligent Computing and Control Systems (ICICCS)*, Madurai, India, 2021 (https://doi.org/10.1109/ICICCS51141.2021.9432258).

[12] F. Safari *et al.*, "A Review of AI-based MANET Routing Protocols", *2023 19th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*, Montreal, Canada, 2023 (https://doi.org/10.1109/WiMob58348.2023.10187830).

[13] A. Nadeem and M.P. Howarth, "A Survey of MANET Intrusion Detection & Prevention Approaches for Network Layer Attacks", *IEEE Communications Surveys & Tutorials*, vol. 15, pp. 2027–2045, 2013 (https://doi.org/10.1109/SURV.2013.030713.00201)

[14] R.C. Prim, "Shortest Connection Networks and Some Generalizations", *The Bell System Technical Journal*, vol. 36, pp. 1389–1401, 1957 (https://doi.org/10.1002/j.1538-7305.1957.tb01515.x).

[15] H. Doppalapudi, C.K. Reddy N, V. Dagumati, and Vidhyasagar BS, "Modeling Prim's Algorithm for Tourism Sites in India", *2022 IEEE International Symposium on Smart Electronic Systems (iSES)*, Warangal, India, 2022 (https://doi.org/10.1109/iSES54909.2022.00140).

[16] F. Huang, P. Gao, and Y. Wang, "Comparison of Prim and Kruskal on Shanghai and Shenzhen 300 Index Hierarchical Structure Tree", *2009 International Conference on Web Information Systems and Mining*, Shanghai, China, 2009 (https://doi.org/10.1109/WISM.2009.56).

[17] Aishwarya, R. Maurya, and R. Sharma, "Comparison of Prim and Kruskal's Algorithm", *International Research Journal of Modernization in Engineering Technology and Science*, vol. 5, 2023.

[18] A. Mohan, W.X. Leow, and A. Hobor, "Functional Correctness of C Implementations of Dijkstra's, Kruskal's, and Prim's Algorithms", *Proc. of Computer Aided Verification CAV 2021*, virtual event, 2021 (https://doi.org/10.1007/978-3-030-81688-9_37).

[19] J. Chen, "The Analysis and Application of Prim Algorithm, Kruskal Algorithm, Boruvka Algorithm", *Applied and Computational Engineering*, vol. 19, pp. 84–89, 2023 (https://doi.org/10.54254/2755-2721/19/20231012).

[20] A. Coyle, B. Campbell, and R. Hunjet, "Minimizing the Network Detection Probability Using Autonomous Vehicles", *2020 Military Communications and Information Systems Conference (MilCIS)*, Canberra, Australia, 2020 (https://doi.org/10.1109/MilCIS49828.2020.9282373).

[21] N. Li, J.C. Hou, and L. Sha, "Design and Analysis of an MST-based Topology Control Algorithm", *IEEE Transactions on Wireless Communications*, vol. 4, pp. 1195–1206, 2005 (https://doi.org/10.1109/TWC.2005.846971).

Karol Zientarski, M.Sc.
E-mail: k.zientarski98@gmail.com
AGH University of Krakow, Kraków, Poland
https://www.agh.edu.pl/en

Mykyta Muravytskyi, M.Sc.
E-mail: nick.muravytskyi@gmail.com
AGH University of Krakow, Kraków, Poland
https://www.agh.edu.pl/en

Krzysztof Skos, M.Sc.
Institute of Telecommunications
https://orcid.org/0009-0006-8354-7184
E-mail: kskos@agh.edu.pl
AGH University of Krakow, Kraków, Poland
https://www.agh.edu.pl/en

Kamil Chełminiak, M.Sc.
E-mail: kamil-chelminiak@wp.pl
AGH University of Krakow, Kraków, Poland
https://www.agh.edu.pl/en

Pawel Kulakowski, Ph.D.
Institute of Telecommunications
https://orcid.org/0000-0003-0362-3396
E-mail: pawel.kulakowski@agh.edu.pl
AGH University of Krakow, Kraków, Poland
https://www.agh.edu.pl/en
https://tele.agh.edu.pl/~kulakowski