Connectivity Augmentation in Tactical Mobile Ad hoc Networks

Steffen Reidt\(^1\) and Stephen D. Wolthusen\(^1,2\)

1. Royal Holloway, University of London, Egham, Surrey TW20 0EX, UK
2. Norwegian Information Security Laboratory, Gjøvik University College, N-2818 Gjøvik, Norway
Email: \{s.reidt,stephen.wolthusen\}@rhul.ac.uk

Abstract—Tactical networks in urban environments are constrained by limited line-of-sight communication and frequent network partitioning. Moreover, energy efficiency for both communication and computation is a major concern as such networks are typically limited to battery-powered devices.

Additional resources such as autonomous unmanned vehicles (UVs) or unmanned aerial vehicles (UAVs) are available in today missions. In this paper we investigate the connectivity augmentation of platoon size networks by said network resources, especially UAVs.

We propose an authentication and negotiation protocol to securely request information and services from said resources. Services potentially provided in considered scenarios can incorporate the forwarding of data with a certain bandwidth, information about the UV’s primary mission or missions, or a communication back-link to an infrastructure network. We therefore also investigate the adjustment of UAV flight patterns and a movement protocol that enables UAVs to hover above a group of nodes on the ground.

The algorithm for motional adjustment and their impact on the connectivity of the network are evaluated in section IV. Section V concludes the paper.

The remainder of this paper is structured as follows: Section II provides an overview of service protocols in the literature. Section III. Algorithms for motional control and adjustment and their positive impact on the connectivity of the network are evaluated in section IV. Section V concludes the paper.

II. RELATED WORK

Service discovery protocols as proposed in [2] and [3] focus on enabling the network components to find each other and their provided services. Unlike these protocols, we consider scenarios were the service providing UAVs do not propagate their existence and willingness to provide a service. Instead, the requesting nodes ask for the service of a UAV that is in communication range. The services in these scenarios might be the forwarding of data with a certain bandwidth, information about the UAVs mission, or a communication back-link to an infrastructure network. The protocols that are required to realize such service requests are authentication and negotiation protocols. In the following we will give an overview of the respective protocols in the literature.
Authentication: Stajano and Anderson consider in their Resurrecting Duckling paper [4] a thermometer, which allows authorized devices to display, monitor and reuse its measured data. The thermometer represents more general scenarios in a mobile ad hoc network, and is used to motivate their thoughts about authorization, authentication and integrity. Since pre-shared keys shall not be assumed, and public key cryptography (PKC) is considered to be too expensive, the initial key exchange is performed by physical contact. To this end an electric contact is used to transmit the key material in plaintext. Balfanz et al. [5] follow this approach, and propose an authentication scheme, which requires an initial pre-authentication. The pre-authentication is performed via a side-channel, which could be the electric contact from Stajano’s and Anderson’s scheme. Due to the assumption of a secure side-channel, public key operations are not required.

In the application we are focusing it, a secure side-channel cannot be assumed. We however can avoid a PKC and especially prevent a man in the middle attacks by the assumption of pre-shared symmetric keys as discussed in section III-B.

Since compromised nodes might use stolen identities and credentials for authentication, additional authentication methods are of interest. Glynos et al. [6] investigate in an authentication method, which combines well known cryptographic mechanisms, with different sources of identification information. Such sources incorporate device specific characteristics as radio frequency fingerprint and radio frequency watermark.

Negotiation: Wang and Wang [7] propose a negotiation protocol for real-time multimedia applications over wireless networks. Their focus is on a combined structure of application-oriented and network-oriented negotiation protocols. Application-oriented protocols establish the agreement for an end-to-end service, while network-oriented protocols negotiate for network resources, i.e. the assigned data bandwidth. A pure application based negotiation protocol for capability allocation for MPEG-21 peer-to-peer communication is explored by Rosenberg et al. [8]. Pure network-oriented protocols are proposed in [9], [10] and [11]. Cheng et al. [9] develop the Dynamic Service Negotiation Protocol (DSNP), which is designed to negotiate the Service Level Specification (SLS) in the IP layer, either from host to network, or from network to another network. Durham and Boyle specify the Common Open Policy Service (COPS) [11], which is extended to the service negotiation protocol COPS-SLS by Nguyen et al. [10].

Upper protocols provide a variety of techniques to develop an authentication and negotiation protocol for service requests to an UAV. In case of a successful authentication, a UAV will provide the requested services according to its policies. In order to realize an implementation of the protocol and the resulting services, a clear definition of the executable layer of the policy as described by Schloegel et al. [12] will be required. Upper layers of the policy, which contain formal definition of policy specifications and decision structures, are out of the scope of this paper. As stated above, we consider an UAV to provide the following services: Forwarding of data with a certain bandwidth, information about the UAVs mission (e.g. rough movement of the UAV in the next 10 minutes), or a communication back-link to a infrastructure network.

In addition to these services, an UAV can also support the ad hoc networks by altering its position and movement patterns in such a way as to benefit the networking requirement of the ad hoc network nodes soliciting its support. Again it is the issue of the higher level policies to decide about a possible motional adjustment, which are not discussed here. The concrete methods to adjust movements however, provide the interface to the executable layer of the policy and will be investigated in section IV.

Approaches in the literature to autonomously navigate single UAVs are [13], [14], [15] In these proposals, the UAVs can perform quite simplistic movements by solving optimization problems. Our approach to control UAVs’ movements differs from existing ones, since we either define the route of the UAV allowing slight deviations, or we enable single UAVs to freely choose their route by a swarm-intelligence like protocol.

III. AUTHENTICATION AND NEGOTIATION PROTOCOL

Authentication protocols for MANETs vary in their design depending on the capability of the mobile devices and their application dependent pre-configuration. Unlike in the Resurrecting Duckling approach [4], we cannot assume a physical connection between an UAV for example and a node on the ground. A quite strong assumption however, that is indeed reasonable for the considered scenario is the existence of a shared key between each two nodes. In this section we first recall the scenarios we are aiming at, before presenting our authentication and negotiation protocol thereupon.

A. The Scenario

The scenarios we are focusing on in this paper comprise platoon size missions, in which the connectivity between the nodes is likely to be interrupted by buildings or huge distances between the soldiers. We assume the platoon and respective supporting nodes (SN) (especially given by UAVs) to start their mission equipped with a security architecture, including symmetric keys between each pair of nodes. Handy-size UAVs such as the Bird Eye 500 [16] or the Orbiter Mini UAV [17] have a flight time of maximal 1 and 3 hours, respectively. Intensive communication with the UAV will even decrease this time period. If a new group of soldiers joins the mission, then a UAV can either get the additional key material by an intermediate landing, or if the current UAVs has a short remaining flight time it is replaced by a new one. Micro-size UAVs [18] with a weight of only 250 grams and a flight time of 60 minutes can even be carried by soldiers them self. In this paper we however
consider the case, where the UAVs are started from the mission’s base station.

B. Protocol

Security and Design: Both, the platoon and the SN need to avoid giving any sensitive information to strangers or the enemy. Our proposed protocol therefore incorporates mutual authentication and the optional use of multi-factor authentication. The protocol does not require human intervention. All keys can therefore be chosen randomly distributed, thus avoiding Brute-Force and Dictionary attacks. A major concern in authentication protocols for MANETs, is the prevention of \textit{man-in-the-middle} attacks. The assumption of pre-shared keys in our protocol facilitates a permanent secure communication, thus avoiding a weakness for a man-in-the-middle attack. Since nodes in a Tactical MANET might get compromised, forward security is a further design goal. Forward security could be achieved by refreshing the symmetric keys of all nodes in certain time periods. The required keys might be distributed by UAVs. This method however takes the risk, that the UAV gets compromised or can not reach all nodes in the network. Another approach is to incorporate techniques for forward security in the authentication protocol itself. This can be achieved by performing a Diffie-Hellman key exchange during every authentication as described in the DHE-PSK key exchange algorithm in [19]. Our authentication protocols is based on the DHE-PSK protocol, yet slightly adapted for our application and mutual authentication. The following paragraphs discuss the required key exchange, the communication during the authentication, and the negotiation phase.

Key Exchange: As described in the scenario paragraph, we assume the SNs to be equipped with the key material in advance. In case of an UAV this can happen before the start of the UAV at the base station. A suitable scheme to store these keys is a non-interactive key distribution scheme. Thus schemes have been proposed by Eschenauer and Gligor [20] and Ramkumar et al. [21], and especially for MANETs by Gennaro et al. [22]. In [22] two non-interactive hierarchical key distribution schemes with different strengths according key size and computational effort are proposed. If the key material of the platoon-nodes remains unchanged all the time, we propose the usage of the subset based and computationally more efficient scheme. If the key material is refreshed for forward security during the mission, their polynomial based scheme with smaller key sizes is the privileged one. Since forward security is already incorporated in our authentication protocol, and refreshing of keys for backward-security over the same potentially compromised channel is useless, we use the subset based scheme without key refreshing.

Authentication: Our proposed mutual authentication protocol is illustrated in Fig. 1. The protocol is either started by the SN, that eavesdrops the communication on the ground and sends a HELLO signal when in communication range, or a ground node actively starts the communication either initialized manually or because the SN is expected to be nearby due to the mission plan.

Once a ground node responds to a HELLO message from a SN, or the SN receives the active communication request from a ground node, it checks its policy for the authorization of this node. Furthermore, the ground node needs to attach at least one identifier for a symmetric key in his initial message. This is necessary, since the ground node and the SN might share several secrets. If the SN does not know the requesting node’s identity, or the node is not authorized to start the authentication, it stops the communication. If the node has permission to start the authentication process, the SN chooses one of the ground nodes proposed symmetric keys. It generates a parameter for Diffie-Hellman key exchange, concatenates
the respective public Diffie-Hellman pa with its ID, creates a hash value from the resulting string, and finally encrypts the hash value with the chosen symmetric key. The SN then sends a HELLO message containing the encrypted hash value, its public Diffie-Hellman parameter and the identifier of the chosen symmetric key to the ground node. With the knowledge of the Diffie-Hellman parameter and the symmetric key for the received key identifier, the ground node can now calculate the same encrypted hash value. If it matches with the received one, the SN was successfully authenticated. According to the nodes capabilities and the mission policy, additional multi-authentication mechanism such as radio frequency fingerprint [6] can be used as a second authentication instance. A compromised node, which is sending the right signature, but from a different device might be detected by this.

After a successful authentication of the SN, the ground node performs the same procedure to authenticate itself at the SN. Finally, the SN and the ground node are mutually authenticated and can use the established Diffie-Hellman key as the symmetric key for the current session.

**Negotiation and Services:** After the successful authentication, the ground node can start to request services from the SN. Service requests might include:

- Allowing nodes with certain identities (typically squad leaders) to use the SN as a relay node. Only a certain number of nodes should be able to route through the SN to avoid traffic jam.
- Forwarding messages to, or requesting information from the base station.
- Asking for enhanced connectivity support in general or connectivity support at a specific time period later in the mission.

The SN will comply with the requests within the constraints of its policy, which allow the forwarding of data or adjustment in case of an UAV the UAVs flight pattern. Possibilities for slight modification of UAVs flight pattern for connectivity support are investigated in section IV.

**IV. SIMULATING CONNECTIVITY SUPPORT**

In this section we investigate the connectivity improvement by pre-installed antennas and UAVs flying over a platoon in a city. To this end we run one simulation with pre-installed antennas, and then simulate two different strategies to support the connectivity by UAVs. In the fist of these two strategies, the UAVs fly in a height of 200 meters with 35 MPH to monitor the area. Each time when the UAV is passing the group, it can be used to connect split parts of the platoon on the ground. In the second strategy drones flying in a height of 50 meters are used to actively support the connectivity of the platoon. In all simulations a platoon is moving through a city area and split several times in three squads, separated by buildings. Figure 2 shows the city area, and Fig. 6 a snapshot of the platoon. Simulations were performed in NS-2, using the group mobility model CMM [23] to simulate the platoon’s movements, and the ray optical radio propagation model [24] to calculate transmission ranges in a city area (considering obstacles, reflections and deflections on buildings). The connectivity graphs in Fig. 3, 4(b), 5(b) and 7 show the sizes of groups, in which the platoon is separated. The top (blue) line in Fig. 7 for example shows that all 37 nodes of the platoon plus the three UAVs are connected all the time, i.e. the connectivity graph shows from second 0 to 1300 only one group of size 40. The connectivity between the nodes is computed by the said propagation model. Details of the connectivity graph can unfortunately only be identified on a colored print, the main results however are also described in the text.

**A. Pre-installed Antennas on house walls**

Pre-installing antennas is the technically easiest solution to enhance the connectivity of a MANET moving through this area at a later point in time. Figure 2 shows pre-installed antennas (green crosses), which might be installed intuitively by soldiers, i.e. without using an optimization algorithm for the positioning of the antennas. Indeed, the positions were chosen intuitively, only ensuring that the network of antennas is connected.

![Simulation area with pre-installed antennas (green crosses). The line shows the paths of the three squads building the platoon.](image)

![Connectivity graph (thick black line shows original connectivity, thin blue line the connectivity using pre-installed antennas.). x-axis: time in seconds, y-axis: group size.](image)

The thick black line in Fig. 3 shows the group sizes of the platoon during the simulation. The platoon is connected at the beginning and at the end, yielding only one group of size 37 between second 0 to 150 and 1000 to 1300. Between second 150 and 1000 the squads of the platoon are splitting in between the building and disconnected several times, often resulting in two groups of sizes 26 and 11. The thin blue line then shows the group size of the network including the pre-installed antennas. Since 21 antennas were...
installed, the total network size is now 58. Although, a sufficient number of antennas was installed to perfectly ensure the connectivity of the network, the group is split a view times, especially at second 1000 for approximately one minute. This can be explained by the intuitive placement of the antennas, which does not take shadowing effects by buildings perfectly into consideration. A further drawback of pre-installed antennas is, that failures of single devices can substantially compromise the connectivity. For perfectly reliable connectivity support, exploiting the technical capabilities of todays missions, we therefore investigate the usage of drones in section IV-C.

B. Passive Connectivity Support

UAVs such as the Orbiter UAV [17] are used in today’s missions to monitor special points of interest or whole areas. To this end, UAVs are usually equipped with a camera underneath. Autonomous way point navigation facilitates to control the UAVs either remotely or by pre-defining the way points.

Monitoring Strategies: In order to achieve routes that suite the physical constraints of an UAV (e.g. flight radius), we use B-Splines to define smooth routes. In our NS-2 simulations we examine the connectivity support by an UAV flying above a platoon to monitor the city area. Based on B-Splines, we create the two different monitoring patterns parallel and Hes. The parallel pattern is illustrated by the green line in Fig. 4(a), and the Hes pattern by the green line in Fig. 5(a). The pattern Hes is named by the letter ”H”, since it looks like ”H” concatenated a view times. The blue or red line in Fig. 4(a) and 5(a) show slight modifications of these flight patterns, which aim at getting the UAV close to the platoon for longer time periods, while still fulfilling the mission to monitor the area within certain constraints.

The parallel pattern is modified by slightly bending its flight routes towards the platoon on the ground, as shown by the red and blue line in Fig 4(a). In the simulation belonging to the blue lines, the UAV furthermore adjusted its speed to stay close to the platoon for a longer time. Therefore, the UAV slowed down to 25 MPH when it is able to reach more than 50% of the group, and accelerate to 45 MPH when it is totally out of the platoon’s communication range.

The Hes pattern is stronger modified by flying a extra half-loop above the platoon when it is close to it. Again the red and blue line show these modification, while in the simulations illustrated by the blue line the speed is adjusted similar to the parallel simulations.

Simulations: The results of these simulations are illustrated in Fig. 4(b). The black line represents the connectivity of the network without the support of any UAV. Between second 150 and 1000 the platoon is split most of the time in two groups of 11 and 26 nodes. A view times the group of 26 is furthermore split in groups of 10 and 16 nodes. In the simulations represented by the green, red and blue line one UAV is flying continuously its routing pattern, i.e. approximately three times in theses simulations. The green lines in the connectivity graphs in Fig. 4(b) and 5(b) show the connectivity if the the UAV follows its respective unmodified route. For both patterns the unmodified route already connects the network between the critical phase between second 200 and 1000 nearly 50% of the time. The modified route (red) for the parallel pattern shows only minor changes in the connectivity graph compared to the unmodified route (green). In case of the Hes pattern however, which includes extra half-loops when close to the platoon, the platoon remains connected approximately 70% of the time. The speed adjustment finally (blue line) brings an additional considerable benefit for both routing patterns.

The simulations show the potential of UAVs to support the connectivity of soldiers on the ground, while still fulfilling their own mission. Slight modifications of the monitoring pattern as done for the parallel pattern in Fig. 4(a) appeared to have minor influence on the connectivity support. Flying extra half loops in the Hes pattern, and especially the speed adjustment appeared to keep the UAV for a longer time close the platoon, thus facilitating a better connectivity support. Such modifications however need to be performed within the constraints of the UAVs mission.

C. Active Connectivity Support

In the simulations described in this section, we assume agile UAVs that are also able to stand in the air, i.e. fly with a speed of 0 to 10 MPH. Helicopter-like UAVs such as the drone MD4-200 [25] have this capability and can be controlled by autonomous way-point navigation. In our simulations the UAV will choose these way-points itself, i.e. fully autonomously determine its own route. We first
introduce the non-interactive protocol that enables the UAV to calculate its route, depending on the positions of the nodes in the network. Simulation results then demonstrate the efficacy of this method in supporting the connectivity of the network.

"Hover Above" Movement Protocol: The protocol determines the positions of the UAVs, which aim for flying above the nodes on the ground, is motivated by swarm intelligence techniques. In a swarm intelligence protocol, every node decides autonomously, i.e. without any communication with other nodes, about its movements. The only information that is required is the distance to the nodes on the ground. Let now \( d_m \) be a desired mesh distance, \( UV_s \) the set of all UAVs, and \( UVS \subseteq UV_s \) the UAVs that are closer to \( n \) than \( d_m \), then \( p_{new}(n) \) is calculated by:

\[
p_{new}(n) = \sum_{u \in UV_s} \frac{w_{UV}(n,u)}{sum_{weights}} \cdot p_{UV}(n,u) + \sum_{u \in UVS} d(n, p_{UV}(n,u)) \cdot p_{UV}(n,u)
\]

with

\[
p_{UV}(n,u) = p(n) + \frac{(p(n) - p(u))(d_m - d(n,u))}{d(n,u)}
\]

\[
w_{GN}(n,u) = \begin{cases} d(n,u) & \text{if } d(n,u) \leq \min_{v \in UV_s} \{d(v,u)\} \\ 0 & \text{else} \end{cases}
\]

\[
sum_{weights} = \sum_{u \in GNs} w_{GN} + \sum_{u \in UVS} d(n, p_{UV}(n,u))
\]

If \( \sum_{u \in GNs} w_{GN}(n,u) = 0 \), i.e. the new targeted position of \( n \) is not influenced by any ground node, then \( p_{new}(n) \) is calculated only based on other UAVs’ positions. Let now \( d_m \) be a desired mesh distance, \( UV_s \) the set of all UAVs, and \( UVS \subseteq UV_s \) the UAVs that are closer to \( n \) than \( d_m \), then \( p_{new}(n) \) is calculated by:

\[
p_{new}(n) = \sum_{u \in UVS} \frac{w_{UV}(n,u)}{sum_{weights}} \cdot p(n) \]

Thus, the next targeted position of an UAV is determined as a Barycentric coordinate in the space spanned by the coordinates of the other nodes. More informally, an UAV is attracted or distracted by other UAV and ground nodes. We distinguish two cases: In the first case, the UAV is the closest UAV to a certain non empty set of ground nodes. The UAV tries to position itself above the respective nodes, determining its next position with equation 1. Thus, the UAV is attracted by every ground node proportional to the distance, and distracted by UAVs that are closer than 10m.

In the second case, the UAV considers itself obsolete for the support of the ground nodes, since every ground node is closer to another UAV. In this case the spare UAVs will span a mesh around the other UAVs by calculating their next targeted positions by equation 2. By using equation 2 a UAV is distracted by its closest UAV neighbors, if these are closer than \( d_m \), and attracted otherwise. UAVs that are closer to a neighboring UAV are by the definition of \( w_{UV} \) almost ignored. Considering every UAV with a small weight of 1 in the definition of \( w_{UV} \) ensures a minimum attraction by the whole group of UAVs, thus avoiding single nodes to fall behind the group.

Simulations with different numbers of UAVs show that the UAVs hover above a splitting group in an intelligent way, which facilitates an effective connectivity support of the group on the ground.
Simulation: To validate the Hover Above movement protocol and to examine its influence on the connectivity of the network, we ran simulations in which one to three UAVs support a platoon of 37 nodes as in the former simulations. The platoon is moving through a city area, splitting in up to three groups which are separated by buildings several times. Figure 6 shows a snapshot of the simulation with three UAVs hovering above the platoon in a height of 50m. As in the former simulations, the radio propagation between the ground nodes is calculated by the ray optical propagation model [24], and the communication between ground and UAVs is calculated by the Free-Space model under the consideration of buildings as obstacles is used.

Figure 7 shows the connectivity of the network during the simulation. Again the black line shows the connectivity without any UAV, i.e. the platoon is splitting in groups of 11 and 26, and a view times even in groups of the sizes 11, 10 and 16. The green line then shows the result under the support of one UAV hovering above the platoon. It starts therefore with 38 nodes, since the UAV and the 37 nodes from the platoon are connected at the beginning. For most of the time 80% one UAV is sufficient to keep the platoon connected. Only at second 400, 600, 800 and 1000 the platoon is split into two groups of size 27 and 11 for approximately 30 to 50 seconds. During these periods the UAV is still in communication range of the group of size 26, while it lost the connection to the group of size 11. This seems reasonable, since the UAV is stronger "attracted" by the bigger group. A second UAV as shown by the red line, is then almost sufficient to keep the platoon connected all the time. Only at second 1000 it gets disconnected for 50 seconds. As expected, the support of three UAVs keeps the platoon, that is splitting in up to three subgroups (squads), connected all the time.

V. Conclusion

In this paper we have investigated the connectivity augmentation of platoon size groups by UAVs. To this end an authentication and negotiation protocol is proposed, which allows a bidirecional authentication between nodes on the ground and an UAV. Simulations illustrate the considerable impact of UAVs to the connectivity of a split platoon in a city area. Future work will develop movement protocols for tactical autonomous robots, and investigate the feasibility of security protocols, such as key distribution and distributed signatures, under the connectivity characteristics in Tactical MANETs.

Acknowledgment

Research was sponsored by the U.S. Army Research Laboratory and the U.K. Ministry of Defence and was accomplished under Agreement Number W911NF-06-3-0001. The views and conclusions contained in this document are those of the authors and should not be interpreted as representing the official policies, either expressed or implied, of the U.S. Army Research Laboratory, the U.S. Government, the U.K. Ministry of Defence or the U.K. Government. The U.S. and U.K. Governments are authorized to reproduce and distribute reprints for Government purposes notwithstanding any copyright notation hereon.

References
