Performance Evaluation of 802.11 IoT devices for Data Collection in the Forest with Drones

Caroline Maul de A. Lima*, Eduardo A. da Silva*, Pedro B. Velloso*
*Universidade Federal do Rio de Janeiro, Brazil

***Abstract*—IoT solutions, in order to reduce power consumption, assume severe constraints on the transmission rate, which limit their use to applications with small amounts of collected data per device. Thus, these solutions are not suitable for monitoring wild animals, which requires transmitting large amounts of photos captured by cameras, installed in the middle of the forest. In addition, the forest environment also impairs the transmission capacity. Therefore, this work proposes collecting data from devices in the forest with the aid of unmanned aerial vehicles - drones. Hence, this paper aims at evaluating the performance of a wireless network between the device attached to the drone and the cameras. To achieve our goal, we evaluate traditional network metrics, such as maximum range, transmission rate, and packet loss. To compare and better characterize the transmission in the forest, we also assess the performance of those devices in different scenarios: indoor, outdoor, and inside the forest. The most important result is the feasibility of using low-complexity IoT devices for collection large amounts of data in forest applications.**

I. Introduction

Traditionally, wildlife monitoring is accomplished using camera traps placed inside the forest, on previously set locations, to capture images of wild animals with little human interference [1]. These cameras are equipped with a motion sensor to trigger whenever an animal is detected. Even though largely used, this monitoring procedure implies a high operational cost due to camera placement and data collection. Typically, the monitored areas are located on broad and remote areas in conservation units, with difficult access. Usually, data collection is entirely manual, which requires retrieving each camera to download the data collected. This procedure is not only costly, but also inefficient since it does not take into account whether a specific camera has captured any photo at all, nor if it has been damaged or even if it has run out of battery. Finally, depending on the size of the monitored area, this procedure can take many days. Thus, this work proposes a data collection system for monitoring wildlife in conservation units, with as little human intervention as possible.

The main idea focuses on applying the IoT paradigm, which means, to equip the cameras with low-cost communication devices, allowing the images to be sent to a drone that hovers the forest collecting all photos. However, IoT applications usually assume that IoT sensor devices collect small amounts of data, such as temperature, pressure, humidity, coordinates, etc. In that case, there is no need for a high transmission rate. This assumption suits the power consumption limitation of IoT devices. Accordingly, most recent IoT solutions such as Lora [2] or SigFox [3], ensure years of battery capacity, with a low transmission rate. Clearly, this type of communication technology is not the most suitable for collecting a large amount of data as in our application.

Using drones for data collection in sensor networks has been proposed before in the literature [4], [5], [6], [7]. However, to the best of our knowledge, this is the first attempt to collect a large amount of information using low-cost devices in the middle of a tropical forest. Consequently, our main challenge consists of achieving a high bit rate transmission with power restricted devices in a hostile scenario for data communication. It is important to notice that tropical rainforests are commonly characterized by several layers of dense vegetation which impairs the communication between the cameras and the drones. Therefore, the main goal of this paper is to characterize the transmission capacity of low cost IEEE 802.11 devices with low power consumption and low computational power. For this purpose, we evaluate a Wi-Fi module while transmitting from a location inside the forest to a drone located above the tree canopy. Also, in order to better understand the effect of the tropical rainforest on the transmission capacity of such low cost modules, we compare its performance in different scenarios, such as indoors and outdoors. Few works have already measured IEEE 802.11 transmission capacity in the woods, but in different kinds of forests and none with low computational power devices transmitting to drones. Thus, we have not found any studies in the literature that assess the communication between a restricted IEEE 802.11 IoT device and a drone flying above a tropical forest, collecting large amounts of date.

The rest of this paper is organized as follows. Section II, presents the main related work. The main idea of the wild animal data collection system is briefly presented in Section III. Section IV details our experiments. The main results are presented and analyzed in Section V. Finally, Section VI concludes the paper and presents future work.

II. Related Work

Extensive studies on wireless networks can be found in the literature assessing different technologies in diverse scenarios. For instance, Petajajarvi *et al.* [8] evaluate the performance and reach of a LPWAN (Low-Power Wide-Area Network) in the city, while Kriara *et al.* [9] test 802.11ac networks in an office environment, analyzing the fairness in the transmission by changing protocol settings. Another interesting work [10] evaluates the link capacity of an 802.11b/g network built on a football field.

978-1-5386-4727-1/18/$31.00 ©2018 IEEE

Although the existence of a vast literature on the transmission capacity of wireless networks, few works study its performance in forest areas, especially 802.11 networks. In [11] the authors investigate the effect of vegetation on an 802.11n network in a tropical forest in Malaysia. Using directional antennas, 3 devices were arranged in the forest at 40 m, 108 m and 174 m away from the access point. The objective of this study was to evaluate the viability of building a network to bring Internet access to rural areas of the region. Dressler *et al.* [12], study the performance of an 802.11a/b/g sensor network to monitor bats. The authors evaluate the network in forest scenarios with none, little and dense vegetation. Their main conclusion is that vegetation has a much greater effect on network performance than distance. In [13], the authors evaluate the performance of a mesh network, which sends data of monitoring sensors in a watershed inside the forest to a university *campus* with a total distance of 8 km, using 802.11a/b/g and 802.15.4 technologies. Ding *et al.* [14] evaluate an 802.15.4 network in three different types of forests, showing the effect of each scenario on the quality of the links.

In the context of monitoring using IoT devices with battery and processing constrains, similar to our work, the authors in [15] propose a low cost monitoring application that uses $RaspberryPi$ as a data hub of sensor nodes, however using communication based on the IEEE 802.15.4 standard. In another system, proposed in [16], a $RaspberryPi$ is also used for monitoring, but it is associated with a camera that transmits real-time images of a surveillance system to the Internet. Another interesting work is the application proposed in [17], where it is possible to see the use of unmanned vehicles to aid in the monitoring and prediction of data for cultivation and cattle ranching. However, this application considers small amounts of data collected by sensors. In addition, the drone is not used to collect sensor data, but to film the farm. Data collection is performed by IoT base stations.

Despite all the effort mentioned above, to the best of our knowledge, this is the first attempt to use drones to collect large amounts of monitoring data in rainforest areas using low cost and low power IoT devices, and thus with severe limitations of processing and transmission capacity. Consequently, no precedent performance evaluation has considered low power 802.11 devices transmitting to a drone with several layers of dense and wet vegetation separating the two communication devices.

III. IoT-Wild: IoT Solution for Data Collection in the Forest

The research of wild animals is a very important subject in the area of ecology, not only to know and understand the behavior of these animals, but mainly to preserve their existence. Therefore, monitoring wildlife is fundamental to enable the study and preservation of these animals lives. Several works and projects use information to record the occurrence of species, estimate population sizes or even keep track of specific animals of priority species, gathering knowledge about habits, activity schedules, living areas and others that subsidize decisions on management and conservation of species [1].

Traditionally, wildlife monitoring uses camera traps placed all over the monitored area. As explained before, this system imposes a high cost for collecting all the information captured. In this context, the IoT-Wild project aims at developing an experimental application to automate the work of collecting wildlife data in the forest with the aid of drones. The main goal is to build a data collecting system adding little extra cost to the camera trap system already used in conservation units, not only financially, but most of all, in terms of energy consumption. In this kind of scenario, alternative energy sources are unfeasible due to several layers of dense vegetation. Hence, these cameras are designed to work almost 12 months without any recharge. Thus, the impact of any additional equipment on the battery life should be minimized. As a consequence, we must use low-cost devices to extract the images from the camera and low cost wireless modules to send the photos to another device coupled to a drone. Figure 1 illustrates the basic idea of our collecting system.

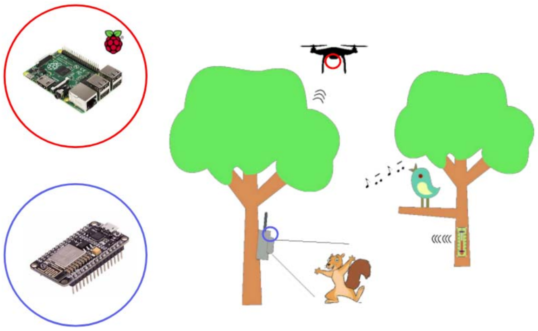


Fig. 1. IoT-Wild application basic scenario

In general, the application will work as follows: the drone plays the role of the Access Point (AP), that flies over the tree canopies until some device identifies it and connects to its network by exchanging credential information. Once the drone identifies a new connection, it stops and stabilizes in the air, and begin to receive the data. The drone remain still until: (i) the device on the camera reports that there is no more data to send or (ii) its battery indicates low charge, whichever occurs first. For this application to work, several challenges must be overcome, such as:

- the power consumption of the communication device cannot reduce significantly the overall lifetime of the monitoring system;
- the battery life of the drone, which is approximately 15 to 20 minutes of flight, in professional devices. The drone must receive as many images as possible in one single trip to minimize the delay of data collection
- transmitting a large amount of data considering the wireless network efficiency in a forest area, built with low power consumption devices and therefore low processing

capacity and transmission rate.

This paper focus on the last challenge, and thus, we analyze the performance of a wireless network composed of a low cost device inside the forest and another device above the trees. Understanding the capacity of this network it is fundamental to estimate whether the flight time of the drone will be sufficient for the application to be minimally efficient. In addition, the characterization of the network might lead to new insights and propositions of new mechanisms and protocols to increase the transmission capacity.

IV. IEEE 802.11 Performance Evaluation

The main reason for using the IEEE 802.11 standard is to offer a higher rate than other low-power IoT technologies, such as IEEE 802.15.4, Lora, and SigFox. However, we had to decide for low power devices, as required by our application. It is worth mentioning that each photo ranges from 500 kB to 1 MB in size, and a given camera may capture more than 3,000 photos. Figure 2a illustrates an example of one of these photos. Therefore, to evaluate the performance, we carried out five types of tests divided into three different scenarios for the purpose of characterization and understanding the performance of these devices communicating with a drone above several layers of dense vegetation. The goal of analyzing indoor and outdoor scenarios is to compare and evaluate the actual effects of forest areas on the capacity of IEEE 802.11 networks. In the experiments, we measure standard wireless network metrics: transmission rate, maximum range, packet loss rate and RSSI (Received Signal Strength Indication).

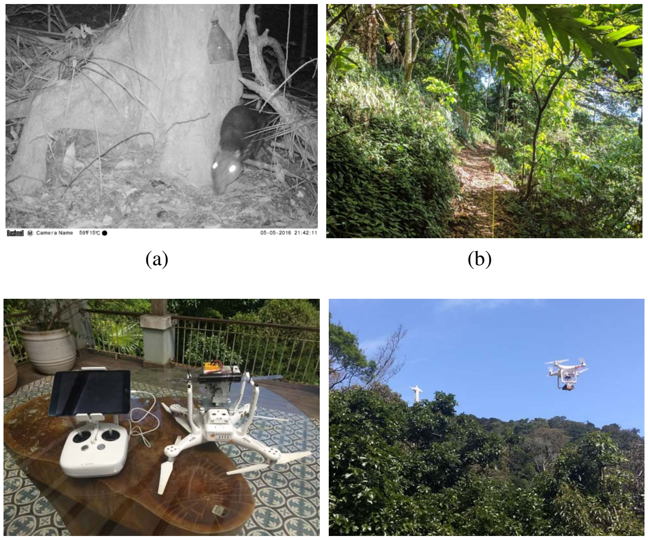


Fig. 2. (a) Wild animal captured by a camera trap in the Tijuca Forest. (b) Track where the tests were performed. (c) Drone with Raspberry Pi docked. (d) Drone flying over the trees in the Tijuca Forest

A. Scenario: Forest

The experiments in the forest scenario took place at the Tijuca National Park, which is the largest urban forest in the world located in Rio de Janeiro, Brazil. The park owns 50 camera traps to monitor wild animals in an area of 3,200 hectares that is covered by tropical rainforest. The climate in such forests is tropical, as the name suggests, and is characterized by rainy summers and dry winters. In general, the temperature in the park ranges from 18°C to 22°C and the relative humidity is between 77% and 88%. In the forest, there are several tree species that form a dense and continuous canopy in this area [18]. It is worth mentioning that the park is situated in the mountains of Rio de Janeiro, and the tests were conducted in a place approximately 600 meters of altitude. Figure 2b shows part of the trail where the tests of transmission with the drone above the canopy trees were realized, as well as a second test with both devices of the network inside the forest.

B. Scenarios: Outdoor and Indoor

The indoor experiments were carried out in the *campus* of the Federal University of Rio de Janeiro. The first one was conducted in a 170-meter-long hall surrounded by classrooms and laboratories, without any obstruction in the line-of-sight of the two devices. In the second experiment 6swty, the transmission occurred between two classrooms, 20 m long each. Each room is furnished with chairs, tables and other furniture common to this kind of environment. Initially, we placed the two devices in the same room, then one device was moved to the second room, placed at the opposite wall from the wall that separates the two rooms, as illustrated in Figure 3. This scenario is important to evaluate an indoor scenario with obstacles.

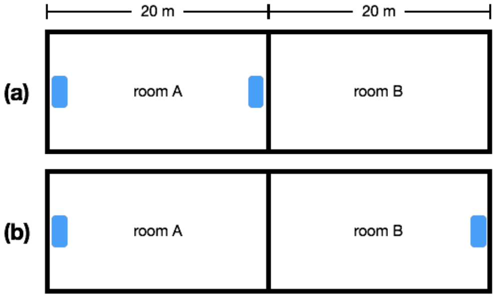


Fig. 3. Indoor scenario in two classrooms.

The outdoor scenario was an empty and isolated street in the city of Petrópolis, Rio de Janeiro. Wide and open, this street does not suffer interference from wireless networks of the neighborhood, since there are no houses on the surroundings.

C. Devices Setup

Our goal is to collect images from the cameras and send them, taking advantage of the monitoring system already installed in the park. The three main requirements to choose the communication device are: (i) high transmission rate; (ii) low energy consumption; and (iii) low cost. Low cost is important because our application requires one equipment per camera and, as already mentioned, the Tijuca National Park, for instance, has 50 cameras trap scattered in the forest. Therefore, using more expensive devices would increase the cost for monitoring the park, and for larger areas the cost could be prohibitive. Thus, we evaluated 3 versions of the ESP8266 WiFi module due to their cost-effectiveness: ESP-01, ESP-201 and ESP-12E. Although all three present similar architectures, with on-board PCB antennas and with gain of 3 dBi, EPS-12E presented better results when compared to the other two versions. Therefore, we use this module in our experiments. The module ESP-12E NodeMCU DOIT supports 802.11b/n/g standards and integrates TCP/IP and UDP stacks. The ESP-12E module in the experiments worked as a client, connecting and sending the data to the access point. According to our preliminary tests, with a cellphone-like battery (2200 mAh), this module works without recharging for over a year, transmitting once a day for 15 minutes. Thus, its battery lasts longer than the battery lifetime of the camera trap, and as consequence, it would not add extra recharge visits. We use the $RaspberryPi$ 3 microcomputer as an access point, due to its superior processing and storage capacity, since our application aims at collecting images from several cameras. In addition, $Rasperry$ does not represent a bottleneck in terms of power consumption, since the server is attached to a drone that has significant less autonomy than the $Raspberry$. The $RaspberryPi$ 3 supports the IEEE 802.11n standard.

The experiments consist of sending 250 fixed-length packets using UDP and TCP protocols from the ESP8266 module to the $Raspberry$, via sockets, and repeated several times. The implementation of the TCP and UDP protocols in the module is limited. We observed that when using the TCP protocol, the maximum packet size is limited to 2 times the MTU, that is, approximately 3,000 bytes, otherwise, the wireless module restart spontaneously. When using the UDP protocol, the limitation is more severe: the module was not able to fragment the packet, and thus, packets larger than the MTU (1,500 bytes) generate the same fault. Another restriction related to the UDP protocol that caused a spontaneous restart of the module was the necessity of a inter-packet interval. This means that it is necessary to add a minimum period of time between the transmission of two consecutive packets. We tested different values to find the minimum inter-packet interval of 10 ms, which does not depend on the packet size.

In all tests, to avoid the soil influence, the wireless module was placed at 1.30 m above the ground. The access point ($RaspberryPi$) was also placed in the same distance from the ground, except for the scenario with the drone, in which the $RaspberryPi$ was attached to it. To evaluate the TCP protocol we used 6 different packet sizes: 128, 512, 1024, 1460, 2000, and 2920-bytes. The same sizes were used for the UDP protocol, but due to module limitations, packets larger than the MTU, (2000 and 2920 bytes) were not evaluated. All the tests were conducted on similar conditions: on sunny days and/or without strong winds and rains. However, since most of the park is on a mountain in Rio de Janeiro, it was not possible to completely avoid sudden wind bursts, which displaced the drone from its collecting position. Another important observation is that the drone can fly for 15 minutes after each recharge, that takes more than 1 hour. Therefore, the wind condition varied significantly even in experiments carried out in the same day.

For each test, except for the one with the drone, we use the following procedure: (i) to move the devices away until they could not communicate due to the distance; (ii) to register the longest distance as the communication range at which the two devices are able to communicate; (iii) to place closer the modules to verify the effects of the distance on the transmission capacity. In all tests, we measured the $RSSI$, the transmission rate, and the packet loss.

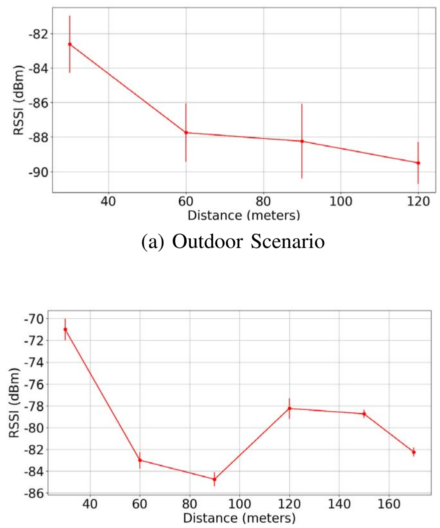
The park owns a $Phantom\ 3\ professional$ drone model, to which we attached the $Raspberry\ Pi$ that plays the role of the server, as shown in Figure 2c, to perform the collection tests above the tree canopy. Unlike the other experiments, the maximum communication range was not evaluated. The drone flew close to the treetops with a safe distance, stabilizing before the beginning of data transmission, to simulate the proposed IoT-Wild application.

V. Results

In this section we present the main results for each scenario. All measurements represent averages with a confidence interval of 95%.

A. Maximum communication range

First, we evaluate the signal-to-noise ratio in order to determine the communication range of each scenario, except for the scenario with the drone. Figure 4 presents the results of two of the evaluated scenarios. In the outdoor scenario, it is possible to observe the decrease of the $RSSI$ value as the distance increases, as expected. In the corridor scenario the $RSSI$ value presents a different behavior, as it has already been shown in previous works. In such case, corridors carry the propagating energy and act as a guided wave, improving propagation in this scenario.



(a) Outdoor Scenario

(b) Indoor Scenario (corridor)

Fig. 4. RSSI

Table I shows the range of each scenario we evaluated. It can be seen that the 802.11 network within the forest presents a similar range to an indoor scenario.

TABLE I
MAXIMUM RANGE

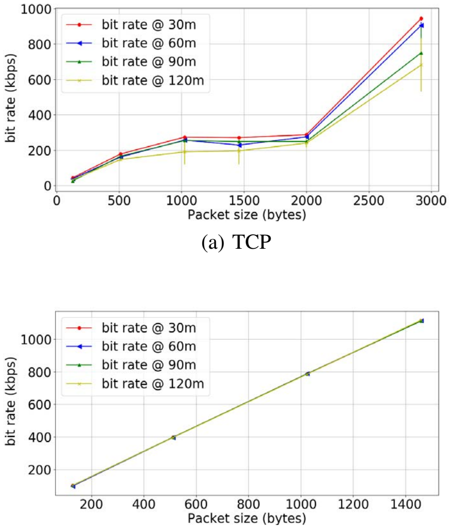
Experiment	Description	Range (meters)
1	Outdoor	120
2	Indoor (corridor)	170
3	Indoor with hurdle	40
4	Outdoor inside the forest	40

In the forest with the drone, the average $RSSI$ measured is -80.75 dBm with standard deviation of 2.82, at a distance of 30 meters. As mentioned earlier, in this scenario we do not evaluate the maximum range, since it does not make sense to our wildlife monitoring application.

B. Network throughput

In these experiments, we evaluate the network throughput using the UDP and TCP protocols. The tests with the UDP protocol are important to show an upper bound of the throughput capacity, and to serve as reference for other works that evaluate IEEE 802.11 networks. In addition, it is possible to characterize packet losses. However, the transmission of the photos captured by the camera requires reliability in the transmission and, therefore, the use of the TCP protocol. Thus, the performance of TCP is critical to estimate the bit rate that the wireless module can achieve in our application scenario.

Figure 5 illustrates the performance of the module in the outdoor scenario, where it is possible to notice a great difference from the performance of traditional IEEE-802.11 devices, that is, without processing and power consumption constraints. Both the throughput and the range measured are inferior to the results usually obtained [9], [19].

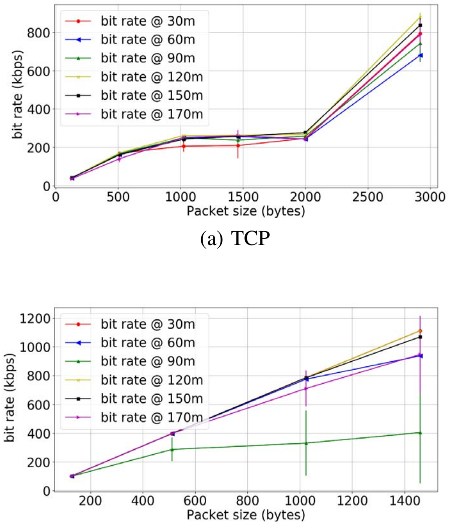


(a) TCP

(b) UDP

Fig. 5. Bit rate x packet size on External Area

Another important point is to verify the effect of the restriction of a minimum time interval between the transmission of two consecutive packets, as imposed by the module. With UDP (Figure 5b) the effect is clear, since the addition of 10 ms after each packet transmission makes the transmission time almost negligible, and as a consequence, the curve is a straight line, proportional to the size of the package. Figure 5a displays the result for TCP. In this case, it is interesting to notice that although there is no restriction of setting a minimum time interval between consecutive packets, the impact of the module limitation regarding its capacity of transmitting two consecutive packets remains. This impact is clearer when we set the maximum packet size allowed by the module. In this case, packet fragmentation occurs, but there is clearly no increase in the minimum packet interval for the two fragments, and therefore, the throughput reaches its maximum. This phenomenon occurs in all other scenarios. Conclusively, we observe that there were no significant variations in the throughput measured for the different distances, even with the decrease of the $RSSI$ value, as shown in Figure 4a. This reduction in the $RSSI$ value usually entails a change of the modulation scheme in IEEE 802.11 networks, implying a lower transmission rate. However, this reduction does not affect the throughput of the module, since the bottleneck is the module itself that cannot achieve high transmission rates.



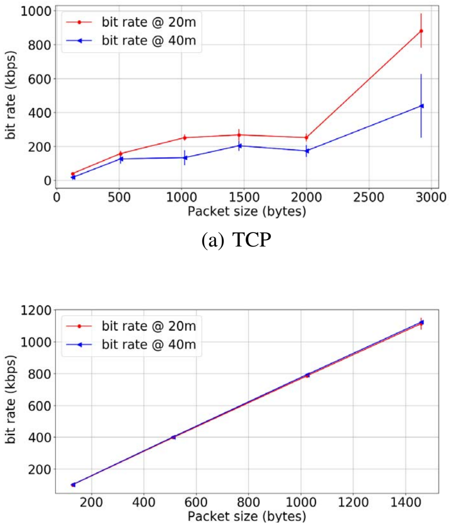
(a) TCP

(b) UDP

Fig. 6. Bit Rate x packet size in an internal scenario

Figures 6 and 7 present the results for the indoor scenarios. The first interesting result is the throughput in the corridor, shown in Figure 6. Despite being an indoor environment, the throughput is similar to the outdoor scenario, where the wireless transmission presents a better performance, because it is not susceptible to so many reflections. As explained in Figure 4b, the propagation in a corridor scenario can be considered as a guided wave, and therefore reaches equal or higher throughput than outdoor scenarios.

Figure 7 shows clearly that the indoor scenario, with obstacles, presents a smaller throughput than the previous scenarios. This result confirms that the presence of obstacles, namely, furnitures and walls between the rooms, affects considerably the throughput, especially for TCP that decreases its congestion window at each packet loss.

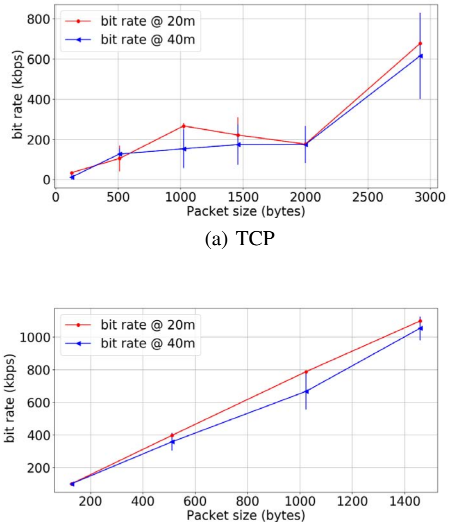


(a) TCP

(b) UDP

Fig. 7. Bit Rate x packet size internal scenario with barrier

Figures 8 and 9 show the results obtained in the tropical forest. In the first experiment, where client and server were inside the forest, the throughput and communication range achieved similar values to the indoor scenario with obstacles. Except for the performance of TCP that was impaired by the existence of a wall (Figure 7a - 40 meters). It means that the performance of data transmission in dense forests can be as poor as in indoor scenarios.

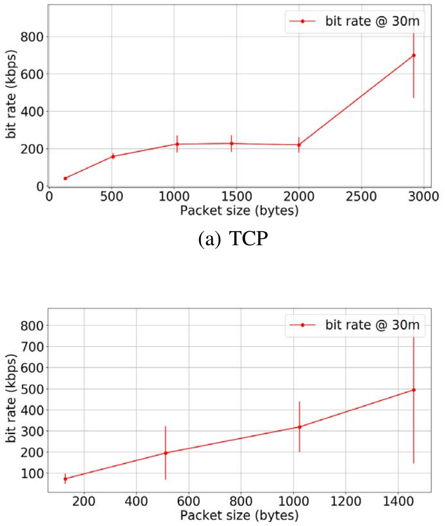


(a) TCP

(b) UDP

Fig. 8. Bit rate x packet size inside the forest

Finally, Figure 9 shows the performance of TCP and UDP in the communication between the drone and the IEEE 802.11 module inside the forest. The first important result is that UDP performance was significantly lower than the other scenarios. This result is mainly due to the occurrence of a larger number of packet losses in this scenario, as shown in Section V-C. One of the reasons for this result is related to the stability of the drone, which consists of keeping its exactly position during the communication. The stability might be affected by the wind condition and the extra weight of the communication equipment. The TCP throughput result, shown in Figure 9a, demonstrates the feasibility of communication above the tree canopy, performing similarly to the indoor scenario.



(a) TCP

(b) UDP

Fig. 9. Bit rate x packet size test with drone

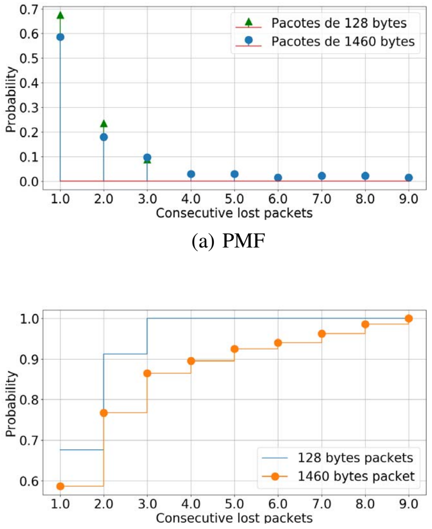
C. Packet Loss Rate

From the experiments of UDP transmission with the drone, we observed that the packet loss in this scenario was significant. Table II shows the average loss percentage for each packet size. It is interesting to note the high packet loss rate for all sizes, which increases according to the packet size, as expected, due to the Bit Error Rate (BER). Except for the larger packet size, which suffered fewer losses than packets of 512 and 1024 bytes. In this particular case, the wind had decreased considerably, and as a result, the drone pilot managed to make it more stable. It is worth to mention that the results of losses present great variation, with rounds with few losses and others with a significant amount of packet losses. This is mainly due to the drone position variation.

TABLE II
EXPERIMENT 5: INSIDE THE FOREST WITH DRONE

Packet Size (bytes)	Average Losses
128	4,8%
512	39,4%
1024	44,8%
1460	27,8%

In order to better characterize the packet loss in the forest, we analyze consecutive packet losses. Figure 10 presents the Probability Mass Function (PMF) and Cumulative Distribution Function (CDF) of consecutive losses for packets of 128 and 1460 bytes. First, it is interesting to note that the vast majority of lost packets are not consecutive. For small packets, the consecutive losses are no more than three packets, whereas for larger packets this can reach nine packets. However, less than 14% of packet losses of 1460 bytes are greater than three consecutive packets. From these results it is possible to consider the hypothesis that TCP congestion control in this scenario may not be efficient, as has already been studied for wireless networks [20].



(a) PMF

(b) CDF

Fig. 10. Losses for the smallest and largest packet size

VI. Conclusion

This paper evaluates the performance of an 802.11 network in the forest assembled purely with IoT devices. We focus is to characterize this type of network in such environment and verify its viability for collecting large amounts of data from cameras with the aid of drones. We also evaluate these IoT devices, for comparison purposes, in other types of scenarios: outdoor and indoor. Results show that device limitations restrict significantly the performance of the wireless network. These limitations associated with the influence of dense vegetation imply a decrease in the transmission rate and an increase of packet losses. Even though, our results demonstrate the feasibility of automating the collection of large volumes of data in dense forests with 802.11 IoT devices. Future work includes evaluating the energy consumption added by the 802.11 module to the camera trap system and to study adaptations to the TCP congestion control model that can be implemented in IoT devices to improve the communication performance between the module and the drone.

Acknowledgment

The authors thank Ernesto de Castro, Tijuca National Park director, who provided all the necessary infrastructure to carry out the measures, Katyucha V. e Silva, management and research coordinator and ICMBIO employees, drone pilots, Marcelo Mendes and Guilherme Medeiros. This work was supported partially by CNPq, CAPES, FAPERJ and grant #15/24494-8, São Paulo Research Foundation (FAPESP).

References

[1] R. Steenweg and et al., "Scaling-up camera traps: monitoring the planet's biodiversity with networks of remote sensors," *Frontiers in Ecology and the Environment*, vol. 15, no. 1, pp. 26–34, feb 2017.

[2] "Lora alliance," 2015, accessed in: Jan/2017. [Online]. Available: https://lora-alliance.org

[3] "Sigfox," 2015, accessed in: Jan/2017. [Online]. Available: https://www.sigfox.com/en

[4] Z. Gu, Q.-S. Hua, Y. Wang, and F. C. Lau, "Reducing information gathering latency through mobile aerial sensor network," in *IEEE INFOCOM'13*, 2013.

[5] A. E. A. A. Abdulla, Z. M. Fadlullah, H. Nishiyama, N. Kato, F. Ono, and R. Miura, "An optimal data collection technique for improved utility in uas-aided networks," in *IEEE INFOCOM'14*, 2014.

[6] H. Jeong, C. Lee, J. Ryu, B.-C. Choi, and J. Ko, "Communicating "in the air" - studying the impact of uavs on sensor network data collection," in *SenSys'15*, 2015.

[7] S. Say, H. Inata, J. Liu, , and S. Shimamoto, "Priority-based data gathering framework in uav-assisted wireless sensor networks," *IEEE Sensors Journal*, vol. 16, no. 14, pp. 5785–5794, 2016.

[8] J. Petajajarvi, K. Mikhaylov, A. Roivainen, T. Hanninen, and M. Pettissalo, "On the coverage of LPWANs: range evaluation and channel attenuation model for LoRa technology," in *International Conference on ITS Telecommunications (ITST'15)*, 2015.

[9] L. Kriara, E. C. Molero, and T. R. Gross, "Evaluating 802.11ac features in indoor WLAN," in *ACM WiNTECH'16*, 2016.

[10] M. Juang, Kuang-Ching Wang, and J. Martin, "A Measurement Study on Link Capacity of a High Stress IEEE 802.11b/g Network," in *IEEE ICCCN'08*, 2008.

[11] H. S. Lim, K. K. Lo, M. Abbas, K. H. Kwong, F. Hashim, A. Ngoh, and S. Torshizi, "An Investigation of Vegetation Effect on the Performance of IEEE 802.11n Technology at 5.18 GHz," in *International Conference on Wireless Communications and Applications (ICWCA 2012)*, 2012.

[12] M. Mutschlechner, P. Baldemaier, P. Handle, and F. Dressler, "Wireless in the woods: Experimental evaluation of IEEE 802.11 a/b/g in forested environments," in *GI/ITG FGSN'13*, 2013.

[13] K.-C. Wang, G. Venkatesh, S. Pradhananga, S. Lokala, S. Carter, J. Isenhower, and J. Vaughn, "Building wireless mesh networks in forests," in *ACM WiNTECH'08*, 2008.

[14] X. Ding, G. Sun, G. Yang, and X. Shang, "Link investigation of IEEE 802.15.4 wireless sensor networks in forests," *Sensors*, vol. 16, no. 7, 2016.

[15] S. G. Nikhade, "Wireless sensor network system using Raspberry Pi and Zigbee for environmental monitoring applications," in *International Conference on Smart Technologies and Management for Computing, Communication, Controls, Energy and Materials (ICSTM'15)*, 2015.

[16] Huu-Quoc Nguyen, Ton Thi Kim Loan, Bui Dinh Mao, and Eui-Nam Huh, "Low cost real-time system monitoring using Raspberry Pi," in *International Conference on Ubiquitous and Future Networks*, 2015.

[17] D. Vasisht, Z. Kapetanovic, J. Won, X. Jin, R. Chandra, S. Sinha, A. Kapoor, M. Sudarshan, and S. Stratman, "FarmBeats: An IoT Platform for Data-Driven Agriculture," in *USENIX NSDI'17*, 2017.

[18] S. R. Freitas, C. L. Neves, and P. Chernicharo, "Tijuca national park: two pioneering restorationist initiatives in atlantic forest in southeastern brazil," *Brazilian Journal of Biology*, vol. 66, no. 4, pp. 975–982, 2006.

[19] A. de J. dos Santos, L. M. K. Costa, M. de L. Braga, P. B. Velloso, and Y. Ghamri-Doudane, "Characterization of a delay and disruption tolerant network in the amazon basin," *Vehicular Communications*, no. 5, pp. 35–43, 2016.

[20] B. Francis, V. Narasimhan, A. Nayak, and I. Stojmenovic, "Techniques for enhancing tcp performance in wireless networks," in *ICDCSW'12*, 2012.