Using Internet of Things for Wildlife Tracking

Collin R. Beane
beane039@morris.umn.edu
Division of Science and Mathematics
University of Minnesota, Morris
Morris, Minnesota, USA

Abstract

The intersection of biologging and Internet of Things (IoT) technologies has revolutionized wildlife tracking, offering unprecedented insights into animal behavior and ecology. This paper provides a comprehensive overview of biologging and IoT concepts, exploring their integration in wildlife tracking applications. We delve into traditional wildlife tracking methods and emerging IoT solutions, analyzing the operational mechanisms, comparative advantages, and limitations of each. Specifically, we examine the use of Low Power Wide Area Networks (LPWAN) such as SigFox and LoRa, alongside traditional WiFi networks, highlighting their respective benefits and considerations in biologging systems. Furthermore, we discuss the critical role of security measures in safeguarding sensitive data transmitted by biologging devices. By elucidating these technologies' capabilities and challenges, this paper aims to provide researchers and conservationists with a framework for evaluating and implementing IoT-enabled biologging systems in ecological research and conservation efforts.

Keywords: IoT, networking, data transmission, animal trackers, Sigfox, LoRa, WildFi, Biologging, ecology

1 Introduction

The proliferation of the Internet of Things has sparked innovation across various domains, including wildlife tracking. Understanding the convergence of biologging and IoT technologies is pivotal in comprehending their applications in monitoring animal behavior and ecology. This paper provides a comprehensive overview of the foundational concepts behind biologging and IoT, delving into their intersection and exploring the myriad technologies employed in wildlife tracking. By examining traditional methods alongside emerging IoT solutions, I aim to establish a framework for evaluating the efficacy of IoT-enabled biologging systems in ecological research and conservation efforts.

2 Background

Comprehending the foundational technology behind the IoT is paramount in grasping its applications in wildlife tracking. This section aims to furnish a concise overview of biologging, IoT, and how data is transmitted over wireless networks. Additionally, it will explore current and past technologies employed in biologging, shedding light on their operational mechanisms and differences in order to compare them to a modern IoT based biologging system.

2.1 What is Biologging?

Biologging is a concept that gained popularity in the early 2000's and has continued to play a pivotal role in understanding animal behavior and ecology. Biologging can be defined as "The investigation of phenomena in or around free-ranging organisms that are beyond the boundary of our visibility or experience. [2]" Biologging provides insights into the behavior and functions of various organisms in environments that can be hostile or difficult to reach for the observer [2]. It is a method of tracking animals in the wild using electronic devices that are attached to the animal. These devices can be used to track the animal's movements, monitor its behavior, and collect data on its environment. This data has been used to study animal behavior, migration patterns, and the effects of climate change on various species [3]. The data collected from biologging devices is also useful for informing conservation efforts and helping protect endangered species [4]. Importantly, biologging is merely the collection of data, and the interpretation of the data is up to the ecologists and conservationists.

2.2 What are the Other Biologging Methods?

Various strategies have been used in the past to track animals in the wild. Many implement variations of the same technology within the tracking sensors; GPS, accelerometers, magnetometers, and thermometers are the most common sensors used in biologging devices. These data from these sensors help researchers understand the animal's speed, direction, and position, which allows for a 3D mapping of positions[10]. I recommend looking at a study done by the Smithsonian's National Zoo and Conservation Biology Institute, which tracks the movements of a prairie dogs [10]. The data transmission methods from these devices can vary greatly. One popular method for transmitting data is the use of cellular networks. A study conducted by a professor from UC Irvine tested the use of cellular networks to analyze the pollution levels in the San Jose area by using pigeons equipped with GPS and automotive emissions sensors [13]. Professor Da Costa had to pay about 250 dollars per device, and 10 cents for each message transmitted [13]. This leads into one of the biggest disadvantages of using cellular networks: cost. Another obvious disadvantage is that cellular

networks are not available in all areas and it is practically impossible for researchers to improve the range of cellular networks by adding more cell towers to cover their study area. Radio frequency is another technology that has been used to transmit data from biologging devices for decades. The use of radio frequency to transmit data from biologging devices requires a handheld receiver to be within range of the transmitter, and the range of the transmitter is limited by the power of the transmitter and the frequency of the radio waves. The receiver and transmitter used by Cooke et al. on marine animals had an effective range of 5 to 1000m and is only able to transmit periodic tracking records or time stamped data from loggers [5]. This falls short of the capabilities of IoT enabled biologging devices that are discussed in section 4.

2.3 How do Wireless Networks Transmit Data?

Understanding the basics of how a wireless networks transmits data is important to understanding how IoT based biologging devices transmit data. Wireless internet networks work by encoding data into binary form. The ones and zeroes are then represented by different amplitudes of radio waves that are sent out to be received by other devices [7]. There are many frequencies that can be used as a medium to send this data; 2.4GHz and sub 1GHz frequencies will be explored in section 4. In general, as frequency increases, range is sacrificed for higher data rates[16]. Data rates are higher because the radio waves are being received in higher frequency, meaning more ones and zeroes are being received every second. In some cases, speed is not everything, and range is more important, in this case, a lower frequency is a better choice.

2.4 What is the Internet of Things?

The Internet of Things (IoT) represents a transformative shift in the realm of technology, encompassing a vast array of physical objects empowered with sensors and software for autonomous interaction. In essence, IoT devices, ranging from commonplace gadgets to sophisticated systems, have the capability to interface with the internet or communicate wirelessly, thereby facilitating seamless integration into various facets of daily life. The IoT has been applied to a wide range of fields, including healthcare, agriculture, manufacturing, and most important to this paper, wildlife monitoring. The fundamental structure of an IoT system is comprised of three interconnected layers: the perception layer, the network layer, and the application layer [11]. The perception layer is responsible for collecting data from the environment, which is then transmitted to the application layer via the network layer. The network layer can use a variety of different methods to transmit data, the two most common being ethernet/WiFi, and cellular networks [9]. Lastly, the application layer is responsible for doing something with the data, such as graph positional data from an animals GPS sensor. The physical implementation of these layers can vary greatly, but in general, the perception layer consists of a sensor or device that can output a signal to be received by a network layer device (most commonly a wireless router). The gateway device is connected to the internet, and is responsible for transmitting it to the application layer, which could be a database to store the data, or a web application to display the data [11]. These three theoretical layers are important in understanding the IoT, and how it can be used in wildlife tracking. The Wild-Fi biologging tag, is a prime example of how these three layers are implemented in a biologging device and is visually explained by figure 4.

3 Components of an IoT Biologging System

The architecture of an Internet of Things (IoT) biologging system is comprised of various components that work in tandem to facilitate the collection, transmission, and analysis of data from wildlife in their natural habitats. At the core of such systems are the physical devices responsible for collecting and transmitting data, these devices are sensor and gateway devices. The design of the hardware that powers these devices is important to understand the limitations and capabilities of a greater biologging system.

3.1 Sensor Devices

The sensor devices of an IoT based biologging system falls within the perception layer of the IoT structure discussed in section 2.4. This means it is responsible for interacting with the environment to collect data and sending it to the network layer. To complete these tasks, four main hardware components work together: antenna, microcontroller, battery and of course, sensor(s). Theses devices can also have optional components that improve it's performance, two that will be discussed in this section are solar energy harvesters and extra local storage. An antenna is a piece of hardware that captures or transmits a radio frequency. These antenna are designed to be compatible with specific frequencies[17], and there are many different designs available for purchase with varying prices. The antenna that is used will be determined by what frequency the network of choice uses, the frequencies relevant to the biologging systems discussed in this paper can be found in sections 4.2 and 4.1. A microcontroller is necessary in a sensor device so that all the components can work together effectively. The microcontroller is effectively a small computer that receives the data that is collected by the sensors and in many cases supplies power to the sensors as well. When the microcontroller recieves the data from the sensors it is responsible for encrypting and packaging it into the required format to be sent to the attached antenna for transmission to a gateway device. A visual aide for the microcontroller acting as a hub for the other components can be seen in figure 1, [1], where an ESP32 Pico D4 is used as the microcontroller for the WildFi tag. Most microcontrollers

will have flash memory to work with, however, extra local storage can also be added on to act as a temporary holding space for data that is unable to be transmitted due to lack of connection to a gateway, an example can be seen in figure 1, [16]. A power source is required for all of the components

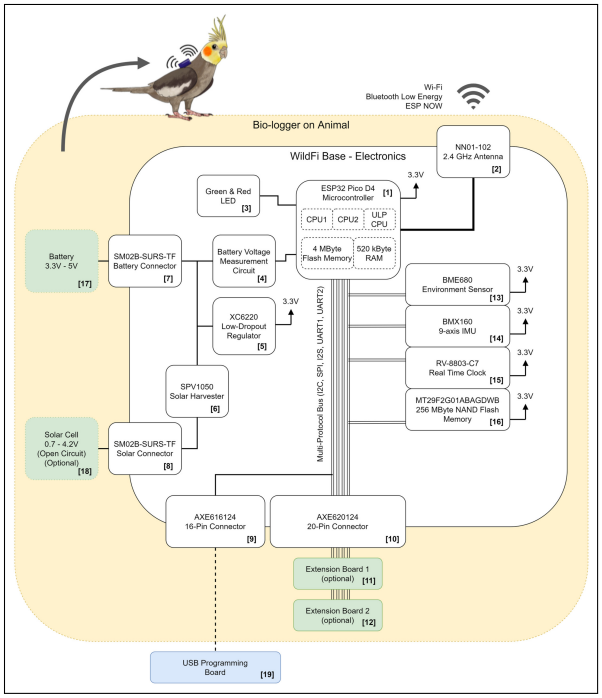

Figure 1. SigFox network infrastructure[20]

to work. Lithium polymer (LiPo) rechargeable batteries and dry batteries like AA/AAA/AAA can all be used to power the sensor devices. As long as a battery connector exists for the microcontroller of choice, anything can be used. Size and capacity are important factors to take into consideration when choosing a battery. A small battery format is likely to be preferred to reduce the effects the sensor devices may have on the animals function, but a sufficient capacity is also important in order to maintain operation for an extended period of time. A popular strategy used to address this problem is the use of solar energy harvesters to recharge the batteries; rechargeable batteries are a prerequisite for this setup. This allows for a smaller battery to be used while still maintaining an impressive battery life. How a solar harvester connects with a greater sensor system can be seen in figure 1, [18]. A biologging device is just a small computer without at least one sensor attached. There are many different types of sensors with different functions that can be attached to a microcontroller; so long as a given sensor has a way to be connected to a specific microcontroller, it can likely be used. The purpose of all of the various sensors is to collect data on the environment of the animal wearing the sensor device. This could mean locational data via GPS, temperature, air pressure and other meteorologic data via environment sensors and more. The number and types of sensors used in a sensor device will depend on what is of interest and there is a consideration of how many sensors can be implemented while maintaining a reasonable size. How sensors connect with a greater sensor device system can be seen in figure 1, [13, 14, 15].

3.2 Gateway Devices

The gateway devices of an IoT based biologging system falls within the networking layer of the IoT structure discussed in section 2.4. This means it is responsible for shuttling information to and from the perception and application layers. To complete this task, four main hardware components and requirements must be met: RF receiver/transmitter, data forwarding engine, power source, and connection to internet or greater local storage. The RF (Radio Frequency) receiver/transmitter is a crucial component of the gateway device in a biologging system. It serves the purpose of communicating wirelessly with the sensor devices attached to the animals or objects being tracked. These RF modules receive data from the sensor devices and transmit commands or data to them as needed. These devices operate on specific frequencies that will depend on the network that is being used, the frequencies relevant to the biologging systems discussed in this paper can be found in sections 4.2 and 4.1. The data forwarding engine within the gateway device manages the flow of data between the sensor devices and the external networks or storage systems. In some cases, the data forwarding engine may dump data into a local storage device or send it to the cloud via an internet connection. It processes incoming data from the RF receiver/transmitter, applies any necessary protocols or formatting, and forwards it to the appropriate destination. This component may include microcontrollers or specialized chips designed for efficient data handling and network communication. A reliable power source is essential for the uninterrupted operation of the gateway device in a biologging system. Depending on the deployment scenario, power may be supplied through various means, including batteries, solar panels, or grid based power. The choice of power source depends on factors such as the duration of deployment, environmental conditions, resource availability, and power consumption of the gateway device. Efficient power management strategies are employed to maximize the device's uptime while minimizing energy consumption and the need for frequent maintenance. The designers of the WildFi tags utilized USB power banks and car batteries to power a gateway device for weeks[20]. The gateway device must have connectivity to either the internet or local storage to facilitate the transmission and storage of data collected from the sensor devices. In scenarios where real-time monitoring or remote access is required, an internet connection is necessary for transmitting data to cloud-based servers or remote databases. Alternatively, in environments with

limited or intermittent internet access, the gateway device may store data locally on onboard storage devices such as flash memory or hard drives. This local storage option ensures data integrity and allows for later retrieval and analysis when connectivity is restored. For example, the ESP32 CAM development boards that the creators of the WildFi devices used as a foundation for a gateway device can store data locally on a SDHC memory card (up to 16GB) [20].

4 Networking

The networking of a IoT based biologging system is crucial in ensuring safe and efficient data transmission. The networks used in a biologging system are responsible for transmitting data from the sensor device to the application layer, and are also responsible for ensuring that the data is transmitted safely and securely. The two most popular types of networking protocols used in biologging systems are Low Power Wide Area Networks (LPWAN) and Traditional Wifi. These two types of networks have their own advantages and disadvantages, and the choice of which network to use is dependent on the specific use case. No matter what method is used, the networking must be able to transmit data over long distances, and they must be able to do so in a secure way. The security of the data is especially important in a biologging system, as the data being transmitted is often sensitive and can be used to track the location of an animal, which in the hand of an illegal hunter, could be disastrous.

4.1 Low Power Wide Area Networks (LPWAN)

LPWAN networks provide a few benefits compared to a traditional mesh wifi network, the primary benefit being that LPWAN networks are able to transmit data over much longer distances than a traditional mesh wifi network. This is especially important in a biologging system, as the animals being tracked are often in vast, remote areas where a 200m range would not be sufficient. LPWAN networks typically utilize sub GHz frequencies and ultra-narrow band modulation to transmit data over long distances [21]. Proprietary LPWAN networks like the SigFox network are popular and designed to handle up to a million IoT devices using only a single gateway. These services are subscription based, and the cost of the service is based on the number of devices that are used in the network. On the other hand, there are LPWAN standards that exist to allow in house development of an LPWAN network. The LoRaWAN protocol is one of the most popular LPWAN standards, and it is used by many to implement their own LPWAN networks[1]. Both of these network solutions are explored further in subsections 4.1.1 and 4.1.2.

4.1.1 SigFox. The SigFox network is a proprietary LPWAN network that is used for IoT systems, and it can be used to cover an area as big as Belgium ($30,600 km^2$) with only seven base stations [19]. The node device in a SigFox network is able to transmit 6 messages per hour, each having a maximum size of 12 bytes. While 12 bytes may seem limiting, it is sufficient for transmitting the GPS coordinates of an animal, as well as other sensor data such as temperature[19]. The SigFox company also offers the Atlas technology which uses the signal strength and location of the receiving base station to calculate an approximate location of the node device, which frees up the node device from having to explicitly send GPS data, allowing for other sensor data to be sent instead[19]. Ultra-Narrow bands (UNB) are used in the SigFox network

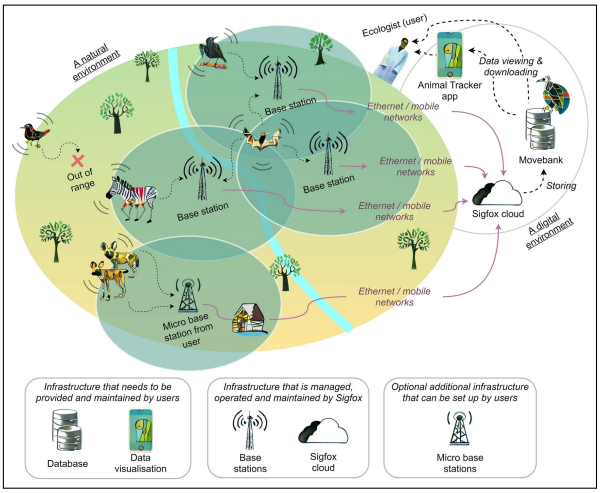

Figure 2. SigFox network infrastructure[19]

and many other LPWAN networks, which allows for the transmission of data over long distances, and the use of UNB also allows for the use of low power transmitters, which is important in a biologging system, as the devices are often attached to animals and must be as small and light as possible. UNB works by using a low radio frequency(868.034MHz to 868.226MHz), and transmits data three times on different channels at different times, which ensures a message is received and robustness to interferences[12]. One of the greatest benefits of UNB is that it allows for the use of low power transmitters, which are able to have incredibly long battery lives. Using the specifications of SigFox's UNB network, a node is able to send 140 packets per day, and the power consumption is between 19 and 49 mA, two AAA batteries are able to power a node up to 6.5 years [12]. Because SigFox is a proprietary network, end users do not maintain the base stations or connection to the SigFox cloud: they only need to design their devices within the SigFox specifications and connect them to the SigFox network. An overview of the SigFox infrastructure and how it can be applied to biologging is shown in Figure 2.

4.1.2 LoRa. The LoRa and SigFox networks have many similarities in how they are structured and operated, however

there are some key differences. The transmission modulation technique used by LoRa is called CHIRP(Compressed High Intensity Radar Pulse) spread spectrum, and it is different from the frequency hopping technique that the SigFox network uses. Where frequency hopping transmits signals at a constant frequency before hopping to a different frequency, chirp modulates by increasing or decreasing it's frequency over time, this can be done both linearly or not[8]. The spreading factor determines how quickly this modulation takes place; LoRa uses spreading factors SF7 to SF12, the larger the spreading factor, the slower the modulation. How these spreading factors compare to each other is shown in Figure 3. The main tradeoffs between spreading factors is the range and data rate of the network, as the spreading factor increases, the range of the network increases, but the data rate decreases[6]. The spreading factor then becomes a critical factor in the design of a LoRa network, as the spreading factor is directly related to the range and data rate of the network, so it should be chosen wisely to fit the needs of the specific use case. Because the frequency is constantly changing, chirp is able to tolerate interference better than that of the frequency hopping technique that the SigFox network uses.

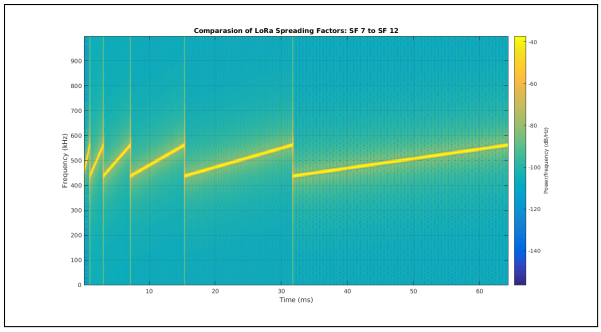

Figure 3. Chirp Spread Spectrum Spreading factors[8]

4.2 Traditional Wifi (WLAN)

A more traditional Wifi network is another method that is used by some companies to implement biologging systems. There are some useful benefits to using a traditional Wifi network over an alternative like LoRa or LPWAN; The biggest of which is data transfer rate. However, because traditional Wifi uses 2.4/5/6 GHz frequencies, the range is much more limited than that of a LPWAN network, and the power consumption is higher. The WildFi biologging system designed by Timm Wild and his colleagues is just one example of a device that uses traditional WLAN to collect data from a biologging device. Wild is also the leading member of the team that studied the use of the SigFox network for a IoT based biologging system, and claimed that the data transmission capacity was one of the reasons that they chose to investigate the use of a traditional Wifi network for biologging[20].

The WildFi tags and others like it, connect and communicate by using a traditional wireless local area network (WLAN), which provides a versatile way for tags to offload collected data. As seen in Figure 4, the WildFi tag has the capability to connect to a WLAN router, smartphone hotspot, specially designed gateway, and more. When the tags establish a connection to one of these devices, data is packaged, encrypted, and transmitted to the receiving device. From there, the data can either be stored on device to be physically collected, or uploaded to a remote database. When connected to a ESP32 CAM gateway and the data is stored locally, a transmission rate of 230 kByte/s can be achieved at a distance up to 200m and only consume 108mA using a WildFi tag[20]. This is more power consumption than a LPWAN based device, however the energy cost per byte transmitted is lower than a LPWAN based device. Wild et. al claim that using a traditional Wifi network with a logging device that has a 70mAh battery and a small solar panel, data can be transmitted 24 hours a day for an entire lifetime of an animal[20].

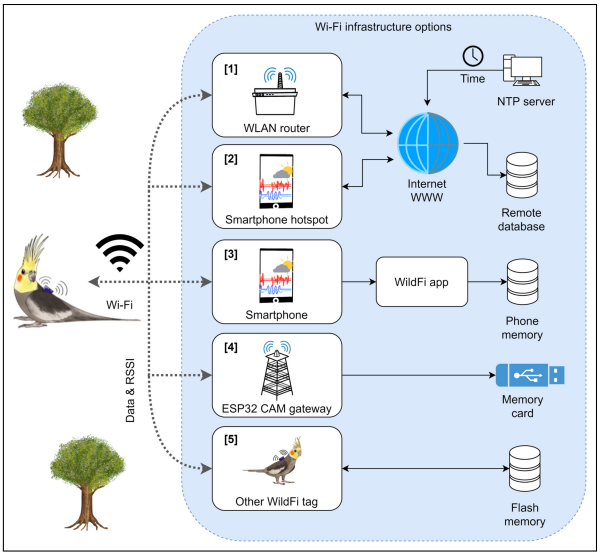

Figure 4. Wild-fi IoT infrastructure overview [20]

4.3 Security

The security of these networks is a critical factor in the design of a biologging system, as the data being transmitted is often sensitive and can be used to track the location of an animal, which in the hand of an illegal hunter, could be disastrous. While much of the security of the data is in the design of the physical device and it's software, the networks being used also need to be secure and safe. The security of the physical device is important in the event that a node device is lost or stolen.

4.3.1 SigFox and LoRa Security. Both the SigFox and LoRa network ensure safe data transmission by using AES

(Advanced Encryption Standard) 128 for end-to-end encryption. With this encryption method, a 128 bit key is used to encrypt the data from node device and a key is shared with the application server to so that it can decrypt the data[18]. This ensures that the data is encrypted at the source, and the data is decrypted at the destination, and the data is encrypted in transit. This is important for the security of the data, as it prevents the data from being readable by anyone who has access to the data, and it also prevents the data from being tampered with in transit. There are many benefits to using AES 128 for end-to-end encryption, including it's proven track record for being secure and efficient. Compared to other encryption methods, AES 128 has a small encryption key which makes it less computationally intensive; This leads into another reason why it was chosen for use in these two LPWAN networks. Due to it being computationally efficient, it is a great choice for a system designed around being low power. For a deeper dive into AES 128 encryption and how it is used in LPWAN networks refer to Kun-Lin Tsai's article on the matter[18].

4.3.2 Traditional Wifi (WLAN) Security. The security mechanisms of a IoT based biologging device that uses a traditional Wifi network can vary depending on the developer of each device and their own preference on how to safely transmit data to the gateway device. In the case of the WildFi devices discussed in section 4.2, data transmissions are encrypted with WPA2 and HTTPS[20]. These two methods allow for ease of use for the developer because they are widely supported by most WLAN devices that would be used as gateway devices. WPA2 and HTTPS, similar to the LPWAN networks, uses AES 128 encryption, this provides the same benefits as previously discussed[15].

4.4 Comparison and Selection Criteria

Examining the benefits and pitfalls of each IoT network in relation to what is important in a biologging system is important to understand what network to choose for a given application. While many factors are important when accessing these networks for capabilities as IoT network solutions, range, data rate, battery life and security will be the focus of this comparison because they are the most critical for a biologging system. Each network discussed in section 4 offers different levels of ability in each of these categories: I rank their abilities in figure 5. This figure gives a good idea of how the three networks compare to each other in the five critical categories. Ultimately, the best network will depend on availability of public networks and the technical knowhow and ability of the user. If the user is not capable of creating their own network and devices, then a solution like SigFox or LoRa may be a better choice. On the other hand, if a user can develop their own system, there are some serious benefits to using LoRa or WLAN, mainly data rate and cost. Each use case for a biologging system is unique and the network of choice will mostly depend on what is needed to meet the demands of the specific use case.

	SigFox	LoRa	WiFi
Frequency	868MHz(EU) / 915MHz(NA) / 433MHz(AS)	868MHz(EU) / 915MHz(NA) / 433MHz(AS)	2.4GHz/ 5GHz/ 6GHz
Data Rate	100bps	50kbps	1840kbps
Maximum messages/day	140	Unlimited	Unlimited
Range	10 km (urban), 40 km (rural)	5 km (urban), 20 km (rural)	200m
Security	AES-128	AES-128	WPA2/ HTTPS (AES128)

Table 1. Characteristics of explored networks, data from [14] and [20]

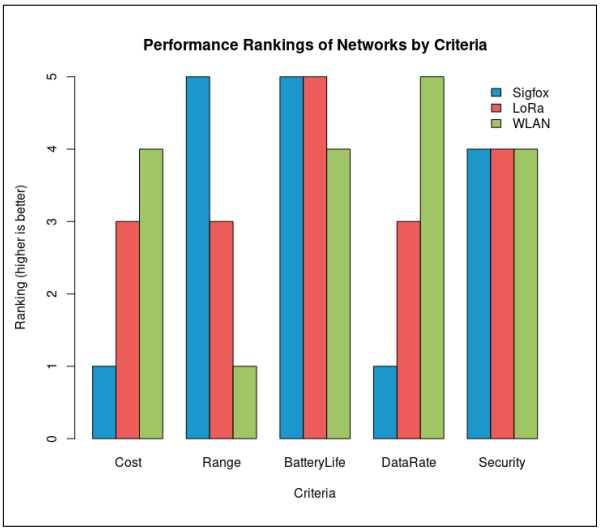

Figure 5. Rankings of discussed networks under 5 critical criteria (5=better, 1=worse)

5 Conclusion

In conclusion, the integration of IoT technologies with biologging systems presents unprecedented opportunities for advancing wildlife tracking and ecological research. The exploration of Low Power Wide Area Networks (LPWAN) such as SigFox and LoRa, alongside traditional WiFi networks, underscores the importance of selecting the most suitable networking protocol based on the specific requirements of the application. Moreover, robust security measures, coupled

with advancements in sensor technology and data transmission, offer promising avenues for enhancing the efficiency and reliability of biologging systems. As we continue to innovate and refine these technologies, the future of wildlife monitoring holds immense potential for gaining deeper insights into animal behavior, and contributing to conservation initiatives.

Acknowledgments

TODO

References

[1] 2023. About LoRaWAN. https://lora-alliance.org/about-lorawan/

[2] Ian L. Boyd, Akiko Kato, and Yan Ropert-Coudert. 2004. Bio-logging science: sensing beyond the boundaries. *Memoirs of National Institute of Polar Research. Special issue* 58 (Mar 2004), 1–14.

[3] Helen E. Chmura, Thomas W. Glass, and Cory T. Williams. 2018. Biologging Physiological and Ecological Responses to Climatic Variation: New Tools for the Climate Change Era. *Frontiers in Ecology and Evolution* 6 (2018). https://doi.org/10.3389/fevo.2018.00092

[4] Steven J Cooke. 2008. Biotelemetry and biologging in endangered species research and animal conservation: relevance to regional, national, and IUCN Red List threat assessments. *Endangered species research* 4, 1-2 (2008), 165–185.

[5] Steven J Cooke, SG Hinch, Martyn C LuCaS, and M Lutcavage. 2012. Biotelemetry and biologging. *Fisheries techniques, 3rd edition. American Fisheries Society, Bethesda, Maryland* (2012), 819–860.

[6] Mehmet Ali Ertürk, Muhammed Ali Aydın, Muhammet Talha Büyükakkaşlar, and Hayrettin Evirgen. 2019. A survey on LoRaWAN architecture, protocol and technologies. *Future internet* 11, 10 (2019), 216.

[7] Ajay Ghimire. 2023. How does the internet actually work? https://www.linkedin.com/pulse/how-does-internet-actually-work-ajay-ghimire/

[8] Sakshama Ghoslya. 2017. LoRa: Symbol Generation. *All About LoRa and LoRaWAN* (2017).

[9] Samuel Greengard. 2021. *The internet of things*. MIT press.

[10] Abhishyant Kidangoor. 2024. New trackers bring Prairie Dogs' little-known underground life to light. https://news.mongabay.com/2024/03/new-trackers-bring-prairie-dogs-little-known-underground-life-to-light/#:~:text=While%20accelerometers%20measure%20if%20and,the%20direction%20of%20their%20movements.

[11] Sachin Kumar, Prayag Tiwari, and Mikhail Zymbler. 2019. Internet of Things is a revolutionary approach for future technology enhancement: a review. *Journal of Big data* 6, 1 (2019), 1–21.

[12] Alexandru Lavric, Adrian I. Petrariu, and Valentin Popa. 2019. Long Range SigFox Communication Protocol Scalability Analysis Under Large-Scale, High-Density Conditions. *IEEE Access* 7 (2019), 35816–35825. https://doi.org/10.1109/ACCESS.2019.2903157

[13] Glen Martin. 2006. San Jose / in studying pollution, this professor will wing it / ... https://www.sfgate.com/bayarea/article/SAN-JOSE-In-studying-pollution-this-professor-2542456.php

[14] Kais Mekki, Eddy Bajic, Frederic Chaxel, and Fernand Meyer. 2019. A comparative study of LPWAN technologies for large-scale IoT deployment. *ICT express* 5, 1 (2019), 1–7.

[15] Kyle Moissinac, David Ramos, Giovanna Rendon, and Abdelrahman Elleithy. 2021. Wireless Encryption and WPA2 Weaknesses. In *2021 IEEE 11th Annual Computing and Communication Workshop and Conference (CCWC)*. 1007–1015. https://doi.org/10.1109/CCWC51732.2021.9376023

[16] Netgear. [n. d.]. What is the difference between 2.4 GHz, 5 GHz, and 6 GHz wireless frequencies? https://kb.netgear.com/29396/What-is-the-difference-between-2-4-GHz-5-GHz-and-6-GHz-wireless-frequencies

[17] Robert Sheldon. 2023. What are antennas and how do they work? – TechTarget definition. https://www.techtarget.com/searchmobilecomputing/definition/antenna#:~:text=Antennas%20are%20designed%20to%20transmit,many%20different%20shapes%20and%20sizes.

[18] Kun-Lin Tsai, Yi-Li Huang, Fang-Yie Leu, Ilsun You, Yu-Ling Huang, and Cheng-Han Tsai. 2018. AES-128 Based Secure Low Power Communication for LoRaWAN IoT Environments. *IEEE Access* 6 (2018), 45325–45334. https://doi.org/10.1109/ACCESS.2018.2852563

[19] Timm A Wild, Louis van Schalkwyk, Pauli Viljoen, Georg Heine, Nina Richter, Bernd Vorneweg, Jens C Koblitz, Dina KN Dechmann, Will Rogers, Jesko Partecke, et al. 2023. A multi-species evaluation of digital wildlife monitoring using the Sigfox IoT network. *Animal Biotelemetry* 11, 1 (2023), 1–17. https://doi.org/10.1186/s40317-023-00326-1

[20] Timm A Wild, Martin Wikelski, Stephen Tyndel, Gustavo Alarcón-Nieto, Barbara C Klump, Lucy M Aplin, Mirko Meboldt, and Hannah J Williams. 2023. Internet on animals: Wi-Fi-enabled devices provide a solution for big data transmission in biologging. *Methods in Ecology and Evolution* 14, 1 (2023), 87–102. https://doi.org/10.1111/2041-210X.13798

[21] Asif M Yousuf, Edward M Rochester, Behnam Ousat, and Majid Ghaderi. 2018. Throughput, coverage and scalability of LoRa LPWAN for internet of things. In *2018 IEEE/ACM 26th International Symposium on Quality of Service (IWQoS)*. IEEE, 1–10.