Tanzania Journal of Engineering and Technology 2023, **42(2)**: 113-133

Websites: https://ajol.org/tjet; https://tjet.udsm.ac.tz

ISSN 1821-536X (**print**); ISSN 2619-8789 (**electronic**)
https://doi.org/10.52339/tjet.v42i2.837

Regular Research Manuscript

On the Use of Wireless Technologies for Wildlife Monitoring: Wireless Sensor Network Routing Protocols

Lilian C. Mutalemwa

Department of Mathematics and Information Communication Technology, The Open University of Tanzania, Dar es Salaam, Tanzania

†Corresponding author: lilian.mutalemwa@out.ac.tz

ORCID: https://orcid.org/0000-0003-4342-5562

ABSTRACT

Traditional methods for wildlife monitoring are labor-intensive and time-consuming. Therefore, advanced technologies and remote monitoring methods are becoming increasingly popular. This paper presents a study on wireless technologies for wildlife monitoring. In the study, a review of the literature was done to identify the most commonly used wireless technologies. Various technologies were explored including unmanned aerial vehicles (UAVs), Internet of Things (IoT), wireless sensor networks (WSNs), artificial intelligence (AI), global positioning system (GPS), and very high frequency (VHF) radio. Then, a more detailed study was done on WSN technology. Investigations were done to observe the performance of routing protocols in WSNs. The use of source location privacy (SLP) routing protocols was considered for secure wildlife monitoring in areas such as game reserves. In such areas, sensor node energy consumption minimization and battery lifetime maximization are crucial. Hence, energy-efficient SLP protocols are more suitable for deployment. Using MATLAB simulation environment, performance analysis of various phantom-based SLP protocols was done to identify effective and energy-efficient SLP protocols. Simulation results show that two-level phantom with a backbone route protocol (TBP) and phantom with angle protocol (PAP) exhibit advantageous performance features in terms of SLP protection, energy efficiency, effective long-term SLP protection, and scalability. Thus, TBP and PAP are suitable for deployment in wildlife monitoring WSNs.

ARTICLE INFO

First submitted: Nov. 29, 2022

Revised: Mar. 1, 2023

Accepted: Apr. 19, 2023

Published: June, 2023

Keywords: *Wildlife Monitoring, Wireless Sensor Network, Source Location Privacy Protection, Routing Protocol, Security, and Location Privacy*

INTRODUCTION

Illegal wildlife poaching is an international problem that threatens biodiversity, ecological balance, and ecotourism (Razaque et al., 2018; Xu et al., 2020). Exploitation of wildlife is highlighted as the second greatest threat to global diversity (Nijman et al., 2022). Therefore, it is important to devise effective mechanisms for wildlife protection to preserve biodiversity and ecosystems. An assessment of the global ecosystem services estimated the value of ecosystem

services to be 125 billion USD per year (Caballero et al., 2017). This indicates that conservation of ecosystems is both environmentally and economically profitable (Caballero et al., 2017; Ibrahim et al., 2021). Wildlife protection contributes to the United Nations Sustainable Development Goals (SDGs) which aim to make the world sustainable (Isabelle and Westerlund, 2022; Yoshida et al., 2019).

In Razaque et al. (2018) and Yue et al. (2021), it was presented that the global illegal wildlife trade directly threatens biodiversity and leads to disease outbreaks and epidemics. Wild animals can become virus banks and cause spreading of infectious diseases. For example, it was suspected that COVID-19 originated from wildlife sources (Koh et al., 2021; Yue et al., 2021). Also, several epidemiological studies suggest that bats or pangolins could be the intermediate hosts during virus transmission and mutation. Furthermore, most new infectious diseases such as SARS, Ebola, and MERS were zoonotic diseases (Yue et al., 2021). It is believed that the outbreak of Ebola was caused by the Zaire Ebola virus which may have originated from certain species of bats (Razaque et al., 2018). Based on academic statistics, 60.3% of 335 new infectious diseases broke out in the world between the year 1940 and 2004, and 71.8% of them originated from wild animals (Yue et al., 2021).

Despite the significant challenges caused by illegal wildlife poaching, wildlife trade is on the rise. It was presented in Nijman et al. (2022) and Razaque et al. (2018) that a lot of wildlife criminal activities and illegal sale of wild animals are being conducted over the Internet. According to the 2020 World Wildlife Fund (WWF) report, wildlife populations have declined by 68% since the year 1970 (Ibrahim et al., 2021). The decline in wildlife populations is mainly due to their over-consumption by poor local people living in or near national parks. Thus, poverty is one of the main reasons for illegal wildlife hunting by locals, who then sell the hunted wildlife at high prices as a source of income (Ibrahim et al., 2021).

Illegal hunting of wildlife is a significant challenge in Africa. Massawe et al. (2017) reported that the reduction in African elephant population has been observed since the year 1979. In the year 2013 nearly 450 elephants were killed in Cameroon's national park. Poaching of elephants is also a serious problem in countries such as Congo, Zimbabwe, Zambia, Mozambique, Tanzania, and Kenya (Razaque et al., 2018). In the case of Tanzania, illegal hunting of elephants is a serious problem in game reserves such as the Ugalla Game Reserve (UGR) (Wilfred, 2020) and Serous Game Reserve (Razaque et al., 2018).

The study in Wilfred (2020) reported that more than 160 animals were removed by poachers from the UGR between the year 2007 and 2017. The most hunted animal species were common duiker, hippopotamus, African elephant, and impala. About 70% of the species affected by the poaching were hunted primarily for bushmeat. Therefore, a lot of work is being done by the Tanzania Wildlife Management Authority (TAWA) to ensure wildlife protection in UGR. TAWA employs rangers as part of their contribution to conservation. Anti-poaching patrols are conducted both on foot and in vehicles. However, wildlife poaching remains a problem in UGR. Therefore, it is important to devise sustainable methods to help address the challenges of poaching while meeting conservation objectives.

In many cases, law enforcement is the predominant method used to promote wildlife conservation and reduce the effects of wildlife consumption (Wilfred, 2020). For example, after it was suspected that COVID-19 originated from animals sold in a market in Wuhan, China, the Standing Committee of the National People's Congress adopted an urgent decision to expand the scope of China's Wildlife

Protection Law to ban the consumption of almost all wild animals (Koh et al., 2021).

To effectively address the problem, in addition to law enforcement, methods such as integrated conservation and development are used to provide a balance between conservation and poverty reduction (Wilfred, 2020). Also, promotion of wild animal protection education improves the public consciousness of protecting wild animals (Razaque et al., 2018). Furthermore, emerging communication technologies are used. It was recently presented in Prosekov et al. (2022) and Lee et al. (2021) that a traditional method such as field survey is time-consuming and cost-intensive. Also, field surveys require field-skilled experts. Moreover, performing a traditional field survey can result in dangerous situations, such as an encounter with wild animals. Therefore, advanced technologies and remote monitoring methods are becoming increasingly popular in wildlife monitoring applications.

The content of this paper is organized in sections. The next section presents a review of the literature to identify the most commonly used technologies for wildlife protection and monitoring. Then, a more detailed discussion on the use of Internet of Things (IoT) and wireless sensor network (WSN) technologies is presented. Subsequently, analysis is done to investigate the performance of routing protocols in WSNs. Some of the important parameters to consider when WSNs are deployed in remote areas for wildlife monitoring are security and source location privacy (SLP) protection, energy consumption minimization, and battery lifetime maximization. This is mainly because SLP provides security and location privacy protection of the monitored animals (Han et al., 2018; Jiang et al., 2019; Wang et al., 2020). Also, WSNs have limited battery lifetime. Therefore, reducing the sensor node energy consumption and extending the lifetime of WSNs is critical (Liu et al., 2019; Mutalemwa & Shin, 2021a).

The study in Wilfred (2020) reported that wildlife poaching remains a problem in UGR. Therefore, this paper discusses the use of IoT and WSN technologies for wildlife monitoring in the UGR. It is assumed that UGR is a remote area. Therefore, sensor node energy consumption minimization and battery lifetime maximization are crucial. Hence, energy-efficient SLP protocols are more suitable for deployment in UGR to provide long-term monitoring and SLP protection. To identify SLP protocols appropriate for deployment in UGR, this paper includes a section that explains the materials and methods used in performance analysis and a section that discusses the results. Also, a summary of the observations and conclusion are presented.

LITERATURE REVIEW

The use of advanced technologies such as unmanned aerial vehicle (UAV), IoT, WSNs, and artificial intelligence (AI) frameworks enable timely detection and deterrence of illegal poaching activities (Arshad et al., 2020; Feng et al., 2019; He et al., 2016). Several wildlife monitoring technologies were discussed in Camal & Aksanli (2020) and He et al. (2016). Table 1 shows a summary of the commonly used technologies for wildlife monitoring. Also, it highlights various studies that employ the technologies.

Caballero *et al.* (2017), Nguyen *et al.* (2020), and Prosekov *et al.* (2022). In Caballero *et al.* (2017), a UAV was employed to extract data from an isolated multimedia WSN for wildlife monitoring in the Amazon rainforest. In Xiaohan *et al.* (2015), IoT technology was considered for wildlife monitoring to enable location tracking, habitat environment observation, and behavior recognition. Other technologies were also considered in Xiaohan *et al.* (2015) including sensor networks, satellite communications,

cellular networks, and mobile access points such as UAVs.

Table 1: Wildlife monitoring technologies

Technology	Study
Integrated camera and sensor nodes	(Chen et al., 2019; Feng et al., 2019; Haucke et al., 2022; Liu et al., 2019; Santosh K. et al., 2018; Zualkernan et al., 2022)
AI	(Arshad et al., 2020; Dominguez-Morales et al., 2021; Islam & Valles, 2020; Jia et al., 2022; Nguyen et al., 2017; Tuia et al., 2022; Xu et al., 2020; Zualkernan et al., 2022)
UAV and sensor nodes	(Bayram et al., 2016; Caballero et al., 2017; Ivanova et al., 2022; Lee et al., 2021; Nguyen et al., 2020; Prosekov et al., 2022; Santos et al., 2014; Torabi et al., 2018; Vera-Amaro et al., 2020; Xiaohan et al., 2015; Xu et al., 2016)
Satellite	(Krondorf et al., 2022; Salem et al., 2021; Tuia et al., 2022; Wang et al., 2019; Washburn et al., 2022; Xiaohan et al., 2015)
Multimedia camera	(Haucke et al., 2022; Islam & Valles, 2020; Nguyen et al., 2017; Yoshida et al., 2019; Jia et al., 2022)
IoT	(Begum et al., 2020; Dulari et al., 2020; Duran-Lopez et al., 2019; Elias et al., 2017; Ma, 2022; Martin et al., 2021; Mitra et al., 2021; Ojo et al., 2021; Ross et al., 2022; Terada et al., 2019; Wild et al., 2022; Yoshida et al., 2019; Zualkernan et al., 2022)
WSN	(Baig & Shastry, 2023; Camal & Aksanli, 2020; Chen et al., 2019; Dominguez-Morales et al., 2021; Massawe et al., 2017; Naureen et al., 2020; Xu et al., 2016; Vera-Amaro et al., 2020)
GPS tracking	(Dominguez-Morales et al., 2021; Lichtenstein & Elkaim, 2020; Naureen et al., 2020; Santos et al., 2014; Salem et al., 2021)
VHF	(Bayram et al., 2016; He et al., 2016; Nguyen et al., 2020; Santos et al., 2014; Torabi et al., 2018)

Furthermore, IoT, UAV, and WSN technologies were used in Xu *et al.* (2016) to detect locations of endangered species in large-scale wildlife areas and monitor movement of animals without any attached devices. It was shown that UAVs provide cost-effective and a flexible platform for WSN applications. The UAVs were able to play different roles such as actors, sensors, and mobile sinks. In Arshad *et al.* (2020); Islam & Valles (2020); Nguyen *et al.* (2017), AI-based frameworks were considered. The framework in Nguyen *et al.* (2017) devised an automated animal recognition system for wildlife monitoring. The system employed advanced digital technologies such as camera trapping to enable various projects including the Snapshot Serengeti project. Between the year 2010 and 2013, the project gathered millions of images through 225 camera traps across the Serengeti national park. The camera trapping technology was also considered in Islam & Valles (2020) for wildlife monitoring in Bastrop County, Texas.

In Santosh *et al.* (2018), an automated system was designed with two microphone sound detectors, an ultrasonic sensor, and a camera. The microphone sound detectors detect the animal sound or motion. Then, it turns on the camera and captures the animal image. To enable effective monitoring, the captured images are stored in memory or sent to the operator. In Yoshida *et al.* (2019), an IoT-based wildlife monitoring system was designed for rural and mountainous areas, in Japan. The system consists of cameras and a video collection server to capture data in the form of images

and videos. Also, it includes IoT platforms and cloud servers for IoT services. In Chen *et al.* (2019), WSN-based systems were presented for wildlife monitoring to prevent wildlife-vehicle collisions when wildlife cross roads. The systems contain networks of sensors and actuators in order to detect wildlife approaching the road and to warn the drivers in real-time by means of light signal devices. The nodes of the network are installed on the road sides in and wirelessly interconnected. A remote-control unit deals with the storage and the processing of the collected information.

The advantages and disadvantages of various wildlife monitoring technologies were presented in Islam & Valles (2020), and Liu *et al.* (2019). For instance, the use of camera trapping technology is gaining popularity. It is simple to deploy, flexible to operate, and easy to maintain in the field. Also, it allows capturing a rich set of information about animal appearance, actions, biometric features, and reveals the direction of the movements. However, camera trapping has a limitation that manual analysis of the captured image and video material is exceptionally monotonous, time-consuming, and cost-intensive. Also, there are many conditions that can deteriorate the image quality. In the case of satellite tracking, the technology is costly and comparatively less durable (Islam & Valles, 2020).

The technique of global positioning system (GPS) tracking is mostly effective when monitoring larger size mammals or birds (Islam & Valles, 2020). In sensor-based GPS tracking systems, sensor nodes are equipped with a GPS and a tracking collar is worn by an animal. The components of the sensor-based GPS tracking systems have large weight and high deployment cost. Also, they have increased energy and memory consumptions at the sensor node. When the tracking collar is heavy, it can significantly affect the movement of the animals. It has been recommended that the maximum weight of a tracking collar should be less than 5% of the body mass of the animal that wears the collar (Naureen *et al.*, 2020). Therefore, non-GPS (or ordinary) sensor nodes are better than GPS-equipped sensor nodes (Naureen *et al.*, 2020). In Lichtenstein & Elkaim (2020), and Naureen *et al.* (2020), GPS-based tracking technologies were considered. Then, (Naureen *et al.*, 2020) designed a GPS-less wildlife tracking solution using low-cost and lightweight sensor nodes.

The use of Very High Frequency (VHF) radio tracking technology is considered in many studies. It is reported that VHF has been used for wildlife monitoring for more than 50 years (Nguyen *et al.*, 2020). VHF requires a user to receive transmissions from a VHF transmitter, usually in a collar attached to the animal, by using a hand-held antenna. The process can be time-consuming and tedious (Santos *et al.*, 2014). Also, the performance of VHF can be affected by weather conditions (Islam & Valles, 2020). To address some of the challenges in a VHF system, (Santos *et al.*, 2014; Torabi *et al.*, 2018) employed UAVs to receive transmissions from VHF transmitters. The UAVs were enabled with a GPS unit.

IoT AND WSNs FOR WILDLIFE MONITORING

IoT is an emerging technology that enables smart applications. It is a technology that connects numerous devices at any time and in any place using wireless network and services (Butun *et al.*, 2020). Therefore, application areas of IoT will increase continuously and dramatically for every aspect of life. With the diverse installation of IoT devices, it is possible to remotely sense and act upon situations. IoT enables interconnectivity of devices to provide access to data which is collected by WSNs. To enable the use of IoT and WSNs for wildlife monitoring, tracking devices such as radio frequency identification (RFID) tags are attached to the monitored animals (Landaluce *et al.*, 2020). Thus, RFID and WSNs are two key enablers of IoT (Behera

et al., 2020; Landaluce *et al.*, 2020). RFID systems are able to identify and track animals, whilst WSNs cooperate to gather and provide data from interconnected sensor nodes which are deployed in the animal habitat. Real world implementation examples include monitoring badgers and the wildlife crime technology project (Gu *et al.*, 2019).

When WSNs are used in applications such as wildlife monitoring, SLP routing protocols are used for data transmission (Zhang & Zhang, 2022; Gu *et al.*, 2022; Kamarei *et al.*, 2020; Mutalemwa & Shin, 2020c). The use of SLP protocols provides security and location privacy protection of source nodes against traffic analysis attacks (Zhang & Zhang, 2022; Gu *et al.*, 2022; Han *et al.*, 2018; Jiang *et al.*, 2019; Wang *et al.*, 2020). A source node is the sensor node that is located at the animal location (Zhang & Zhang, 2022; Gu *et al.*, 2022; Jun *et al.*, 2014). To report about the animals, source nodes sense the animals and transmit the sensed data to the sink node. Therefore, in scenarios where adversaries (illegal hunters) perform traffic analysis attacks, SLP protocols are used to obfuscate the adversaries (Han *et al.*, 2018; Jiang *et al.*, 2019; Wang *et al.*, 2020). For example, in Wang *et al.* (2019), SLP protocols were considered to obfuscate adversaries in a WSN which monitors precious animals such as pandas, South China tigers, and golden monkeys. Pandas are a good example of high-value animals that need SLP protection. In 2003, a single piece of panda fur was sold in Chongqing, China for 66,500 USD (Mutalemwa & Shin, 2018; Wang *et al.*, 2019). Thus, SLP protocols are useful and they should be considered when WSNs are deployed for wildlife monitoring in UGR.

There exist many types of SLP protocols for deployment in monitoring WSNs (Zhang & Zhang, 2022; Gu *et al.*, 2022; Han *et al.*, 2018; Jiang *et al.*, 2019; Wang *et al.*, 2020). In Mutalemwa & Shin (2020b), the protocols were classified into many categories including phantom-based routing protocols, fake packet injection protocols, random walk routing protocols, ring routing protocols, protocols based on ring routing and fake packet injection, and protocols based on phantom routing and fake packet injection. Other categories of SLP protocols include tree-based routing protocols, angle-based routing protocols, network encoding protocols, directional communication protocols, intermediate node routing protocols, and cross-layer routing protocols. This study focuses on the performance features of phantom-based SLP protocols. In particular, three phantom-based SLP protocols are considered. The protocols are; the two-level phantom with a backbone route protocol (TBP) (Mutalemwa & Shin, 2020b), phantom with fake packet protocol (PFP) (Roy *et al.*, 2015), and phantom with angle protocol (PAP) (Mutalemwa & Shin, 2021b).

MATERIALS AND METHODS

MATLAB network simulation software was used to conduct the experiments, similar to (Mutalemwa & Shin, 2020a, 2021a). In the experiments, the performance of the protocols was measured in terms of SLP protection, energy efficiency, and network lifetime. Also, the end-to-end delay (EED) was measured. The EED is a critical parameter because it indicates the reliability of the protocols. When packets are transmitted with low EED, the packet delivery reliability of the protocol is improved. The performance of TBP, PFP, and PAP was investigated.

The network and adversary models are explained as follows. It is assumed that the WSN model is employed on the target field to monitor animal activities. Also, adversary uses a spectrum analyzer to perform traffic analysis attacks. Therefore, adversary is able to back trace the packet routes in the WSN (Wang *et al.*, 2020). Eventually, it can find the location of the source node (SN) which is located at the animal location. Thus, the main function of

the TBP, PFP, and PAP protocols is to obfuscate the adversary (Han *et al.*, 2018; Jiang *et al.*, 2019; Wang *et al.*, 2020). Figure 1 shows an illustration of the WSN for wildlife monitoring.

Wireless Sensor Network Model for Simulation

The WSN model is adopted from (Jun *et al.*, 2014; Wang *et al.*, 2020; Mutalemwa & Shin, 2021a, 2020b). The WSN is deployed to continuously monitor activities and locations of the animals. The network is event-triggered. A source node (SN) senses an animal then it sends packets periodically to the sink node using a SLP routing protocol. The sensor nodes and animals are randomly distributed in the WSN domain. The probability of each sensor node to monitor the animals is equal, and the probability of generating data to the sink is equal. The sensor nodes employ multi-hop communication for energy conservation. During the network deployment an

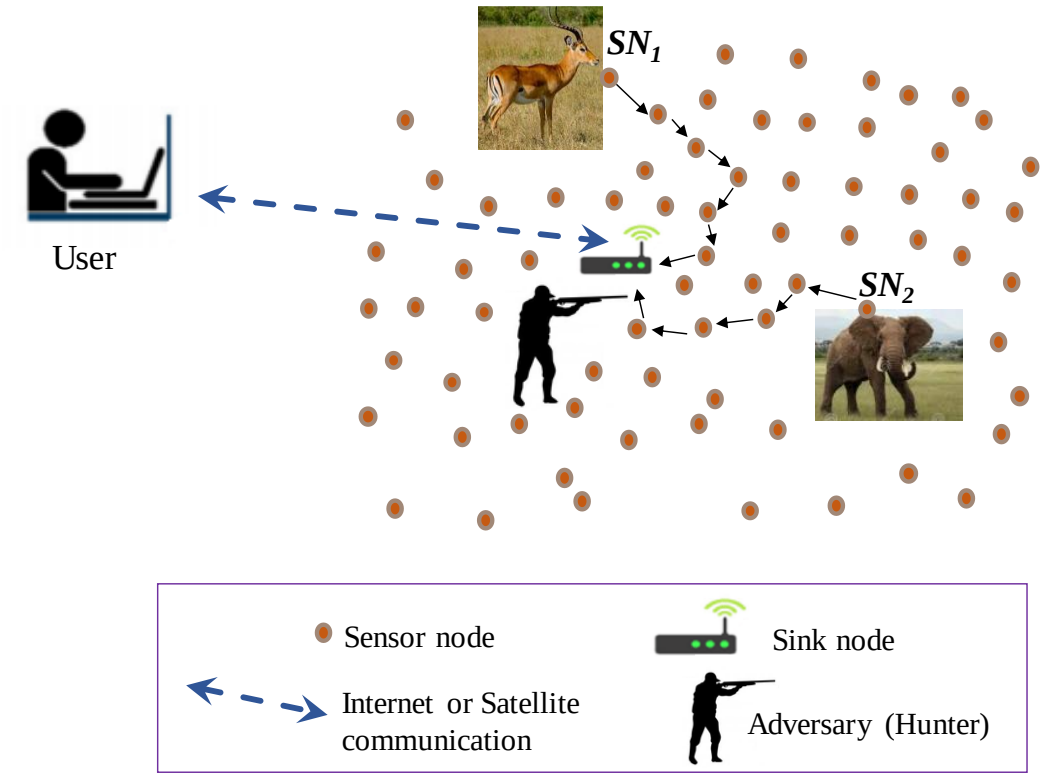

Figure 1: Illustration of a WSN for wildlife monitoring.

configuration phase, network initialization process is done for localization of the sensor nodes as shown in Jun et al. (2014), Wang et al. (2020), Mutalemwa & Shin (2021a), (2020b).

Adversary Model for Simulation

The adversary model is adopted from (Mutalemwa & Shin, 2020b, 2021a). The adversary is equipped with spectrum analyzers to enable traffic analysis attacks (Jun *et al.*, 2014; Wang *et al.*, 2019; Wang *et al.*, 2020). It is initially residing in the neighborhood of the sink node. It is capable of localizing an immediate sender node when a packet is received from a node within the adversary hearing range. It performs a hop-by-hop back tracing attack towards the source node, until it locates the source node which is located at the animal location. After the adversary arrives at the source node location, it can capture the animal (Zhang & Zhang, 2022; Gu *et al.*, 2022). The adversary is cautious. Thus, it has computational power to

limit its waiting time at any immediate sender node. To avoid being noticed or caught by the network administrator, the adversary does not interfere with the proper functioning of the network. Thus, adversary avoids actions such as modifying packets, altering the routing paths, or destroying the sensor devices (Jun *et al.*, 2014).

Network Simulation Environment

MATLAB simulation environment was used to simulate a WSN. In the initial experiments, network parameters similar to the ones used in Mutalemwa & Shin (2021a) were assumed. Then, considering a significantly large game reserve such as UGR, the network side length was increased to 5000 m and 6000 sensor nodes were randomly distributed in the network. Good network coverage was achieved when the sensor node communication range was set to 70 m. It is important to note that the assumed size of WSN is significantly smaller than the size of UGR. Therefore, during implementation, the network administrator should consider different configurations according to the target area. The adversary hearing range was set to 70 m, similar to the sensor node communication range, to ensure the adversary performs hop-by-hop back tracing attack. The cautious adversary waiting timer was set to 4 source packets to increase the chances of overhearing transmission of consecutive packets. The network simulation parameters are summarized in Table 2. The adversary hearing range was set similar to the sensor node communication range to ensure adversary performs hop-by-hop back tracing attack. To improve the accuracy of the simulation results, simulations were run for 500 iterations and average values were considered. Similar to (Gu *et al.*, 2019; Mutalemwa & Shin, 2021a), the security and privacy performance of the protocols were analyzed using path diversity, safety time, and capture ratio metrics. The energy efficiency of the protocols was measured using the energy ratio metric. Furthermore, the network lifetime and EED were measured.

For comparative analysis, the baseline phantom single-path routing protocol (PSP) was included in the performance analysis. In the PSP, packets are sent from the source nodes to the sink node through less random routing paths. Also, the routing paths are relatively short. Consequently, the adversary is not effectively obfuscated and PSP achieves low levels of SLP protection (Mutalemwa & Shin, 2021a).

Table 2: Network simulation parameters

Parameter	Value
Network side length (m)	5000
Number of nodes	6000
Sensor node communication range (m)	70
Adversary hearing range (m)	70
Adversary waiting timer (source packets)	4
Adversary initial location	In the vicinity of the sink node
Target monitoring scheme	k-nearest neighbor tracking
Packet size (bit)	1024
Source packet rate (packet/second)	1
Sensor node initial energy (J)	0.5

RESULTS AND DISCUSSIONS

Path Diversity (PD)

PD signifies the presence of route variation where successive packets from a source node (SN) follow different routing paths that are created between the SN and sink node (Mutalemwa & Shin, 2021a). High PD improves the adversary obfuscation effect, increases the complexity of the back-tracing attack, reduces the attack success rate of the adversary, and improves the security of the monitored animals. Therefore, high PD corresponds to high levels of SLP protection. The PD is measured by counting the number of alternative packet routes that are created between a SN and sink node (Mutalemwa & Shin, 2021a). In the simulations, PD was observed under varied sensor node density. The number of sensor nodes was varied between 6000 and 9000. Figure 2 shows the PD of the protocols. It shows that TBP and PAP achieve high PD.

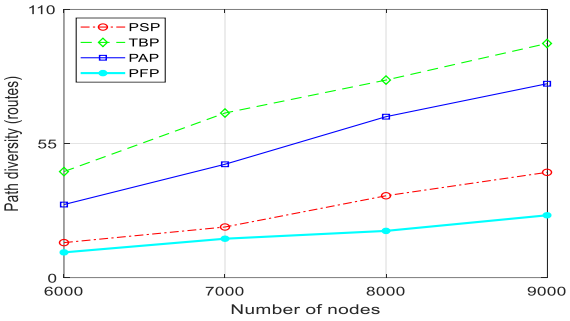

Figure 2: Path diversity under varied number of sensor nodes.

to outperform the baseline PSP protocol. The PD of TBP is high and it increases at a fast rate. This is mainly because TBP employs two levels of phantom nodes. To route packets, a random first-level phantom node is selected then packets are routed from SN to the selected first-level phantom node. Thereafter, a random second-level phantom node is selected then packets are routed from the first-level phantom node to the selected second-level phantom node. Furthermore, TBP selects new phantom nodes and backbone route for each successive packet routing. As a result, the route variation is high and high PD is achieved.

The PD in PAP is high because it employs a dynamic phantom node selection algorithm. PAP generates three candidate phantom nodes for each SN. Similar to TBP, PAP selects a new phantom node for each successive packet routing. As a result, the PD is higher than in PFP and PSP. The PD of PFP is low because the phantom node selection process of PFP is less random. Rather than generating random phantom nodes, PFP focuses on distributing fake packet traffic to obfuscate the adversary. Figure 2 also shows that the PD of the protocols tends to increase with the increase in number of sensor nodes. This is mainly because when a large number of sensor nodes is available, it generates a larger set of candidate phantom nodes for each SN. As a result, a greater number of routing paths is created using larger set of phantom nodes and the PD improves. However, for PFP, the PD improves at a slow rate.

Safety Period (SP)

SP is the time required for the adversary to back trace the packet routes and successfully locate the source node (Jun *et al.*, 2014). Longer SP corresponds to high levels of SLP protection (Gu *et al.*, 2019; Mutalemwa & Shin, 2021a). Thus, long SP indicates increased adversary obfuscation effect and strong security of the monitored animals. The SP is measured by counting the number of hops during the adversary back tracing attack (Mutalemwa & Shin, 2021a).

In the experiments, SP was measured at different source-sink distances. Figure 3 shows the SP of the protocols. It is shown that TBP, PFP, and PAP achieve longer SP to outperform the baseline PSP protocol. TBP and PAP achieve long SP mainly because they achieve high PD. For a successful back tracing attack, the adversary needs to intercept many packets. When the PD is high, it takes longer for the adversary to detect a great number of packets to intercept. Thus, high PD improves the adversary obfuscation effect, increases the complexity of the back-tracing

attack, and reduces the attack success rate of the adversary. As a result, the adversary requires long time to successfully back trace the packet routes and long SP is achieved.

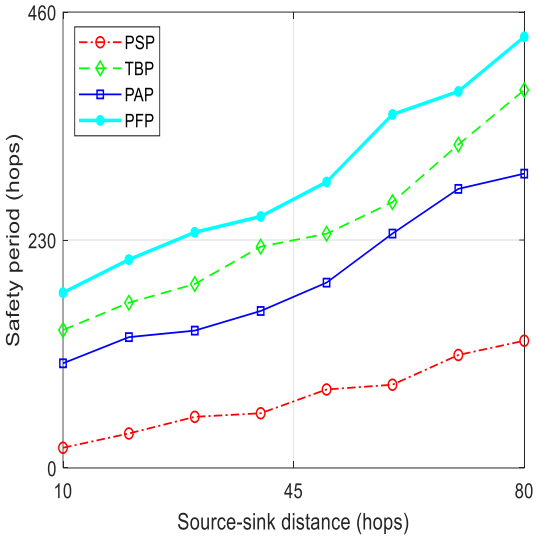

Figure 3: Safety period under varied source-sink distance.

Furthermore, Figure 3 shows that PFP is able to achieve long SP to outperform the other protocols. This is due to the fact that in addition to using phantom nodes, PFP distributes a considerable amount of fake packet traffic around the source node and phantom nodes. The fake packets are identical to the real source node packets. Consequently, during back tracing attack, the adversary detects both real and fake packets and finds it difficult to identify the exact immediate sender node of the real packets. Also, the adversary is tricked into back tracing the fake packet routes. As a result, adversary is steered away from the location of the real source node. Therefore, the back-tracing attack is made more complex and longer SP is achieved by PFP. Figure 3 also shows that SP of the protocols tends to increase with the increase in source-sink distance. The increase in SP is due to the fact that PD improves with the increase in source-sink distance. Thus, when the distance between the source node and sink is long, the adversary obfuscation effect improves and the back-tracing attack becomes more complex. As a result, the SP improves. These results suggest that the protocols are able to provide higher levels of SLP protection when the monitored animals are located at a long distance from the sink node.

Capture ratio (CR)

CR is the ratio between the number of experiments where the adversary ends in locating the source node and the total number of experiments. To locate the source node, adversary must back trace the packet routes and reach at the location of the source node. Thus, the adversary must co-locate with the source node. To compute CR, Equation (1) was assumed. Low CR corresponds to high levels of SLP protection.

$$CR = \frac{No.\,of\ experiments\ with\ located\ SN}{Total\ number\ \ of\ experiments} \quad (1)$$

Details of Equation (1) are available in Mutalemwa & Shin (2021a). To observe the scalability of the protocols, CR was measured under varied network size. The network side length was varied between 5000 and 7000 m. Source nodes were assumed at source-sink distance of 40 hops. Figure 4 shows the experiment results. It shows that TBP, PFP, and PAP achieve low CR to outperform the PSP protocol. TBP and PAP achieve low CR mainly because they achieve high PD. PFP achieves low CR because it distributes a considerable amount of fake packet traffic to obfuscate the adversary. It is also shown that the CR of TBP and PAP tend to decrease when network side length is increased while the CR of PFP and PSP incur insignificant change. In the experiments, the sink node was fixed at the center of the network and the location of phantom nodes remained the same despite the increase in network size. Therefore, for PFP and PSP, the routing path configurations remained the same and CR did not change. In the case of TBP, since the sink node was fixed at the center of the network, the distance between the sink node and

phantom nodes increased with the increase in network side length.

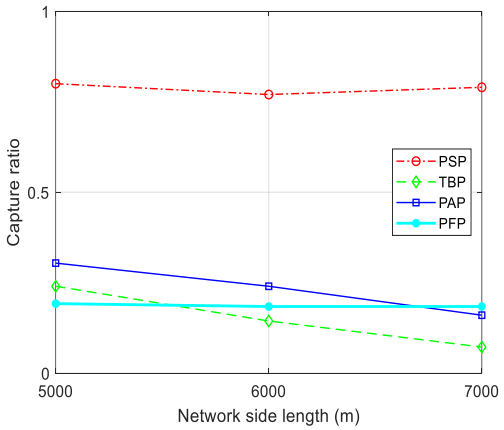

Figure 4: Capture ratio under varied network side length.

This is mainly because TBP locates the phantom nodes in the network border regions. Therefore, the distance between the source nodes, phantom nodes, and sink node increased with the increase in length. As a result, the routing paths became longer, the PD improved, and the CR of TBP was reduced.

Similarly, the CR of PAP tends to decrease with the increase in network size. This is mainly because PAP generates phantom regions which increase in size as the network size increases. Therefore, as the network size increases, the number of candidate phantom nodes increases, the routing paths become more dynamic to improve the PD, and the CR is reduced.

Attack Success Rate (ASR)

ASR is the measure of the rate of source node traceability when the adversary is back tracing against routing paths of a SLP routing protocol (Mutalemwa & Shin, 2020b). It is computed by counting the number of successful adversary attempts. Low ASR corresponds to high levels of SLP protection.

The ASR of the adversary was observed under varied source packet rate. The source nodes were randomly positioned at a source-sink distance of 38 hops. The source node packet rate was varied between 1 and 4 packet/second. Figure 5 shows the experiment results. It is shown that the ASR for all the protocols tends to increase when the source packet rate is increased. The main reason for the increase in ASR is that, when more packets are generated per second, the amount of packet traffic is increased.

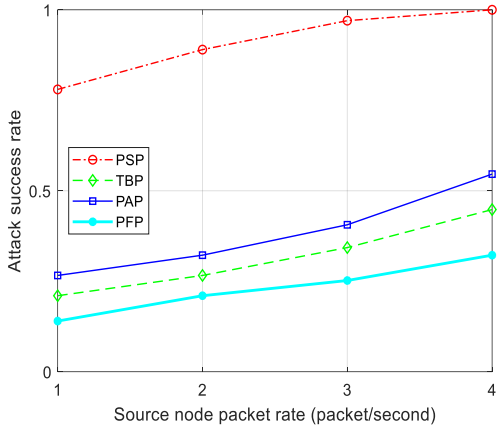

Figure 5: Attack success rate under varied source packet rate.

As a result, the adversary is able to capture an increased amount of successive packets within the specified waiting timer. Thus, at higher data rates, the adversary is capable of capturing enough number of successive packets to allow the adversary to make successful back tracing attacks. Consequently, the ASR increases. Figure 5 also shows that the ASR for PFP increases at a slow rate. This is due to the fact that PFP employs fake packet traffic to steer the adversary away from the real source node. As a result, adversary captures both real and fake packets and the back tracing attack remains complex. Hence, adversary makes less significant progress towards the real source node and ASR improves at a slow rate.

Energy Efficiency (ER)

The ER parameter was used to measure the energy efficiency of the protocols. ER is the ratio of the energy that is consumed by the sensor nodes in 600 rounds to the total energy (Mutalemwa & Shin, 2021a). Low ER corresponds to high energy efficiency.

The energy consumption of the sensor nodes was computed using the energy consumption model in Behera *et al.* (2020), Jun *et al.*

(2014), and Mutalemwa & Shin (2021a). Source nodes were assumed at different source-sink distances and packets were sent from source nodes to sink node. The ER was measured under varied source node packet rate. Figure 6 shows the ER of TBP, PFP, PAP, and PSP. It shows that PFP has the highest ER. The high ER of PFP is mainly because PFP generates a significant amount of fake packet traffic to obfuscate the adversary. When large amount of packet traffic is distributed in the network, the sensor nodes consume more energy to transmit the packet traffic. Consequently, the energy consumption of the sensor nodes and ER increase.

On the other hand, TBP, PAP, and PSP do not distribute fake packet traffic. Therefore, the ER of TBP, PAP, and PSP is lower than ER of PFP. However, the ER of TBP is higher than ER of PAP because TBP employs a two-level phantom routing algorithm. Thus, the routing paths in TBP are longer than in PAP. Therefore, packets in TBP are routed through long hop distances. Each hop consumes some energy. Consequently, TBP incurs high ER. The ER of PSP is low because the routing paths of PSP are relatively short. Figure 6 also shows that the ER of the protocols tends to increase with the increase in source packet rate.

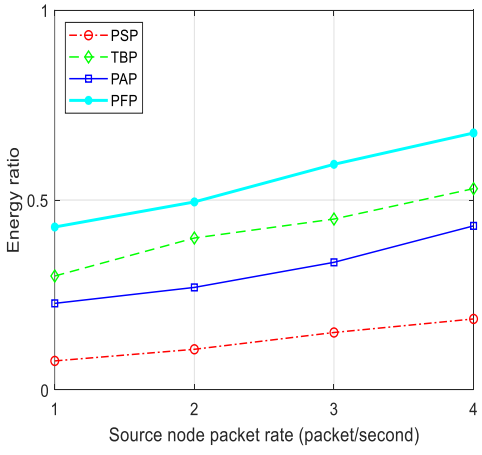

Figure 6: Energy efficiency of the protocols.

This is caused by the fact that when the packet rate is increased, more packets are generated per second. Therefore, energy consumption of the sensor nodes increases, resulting in high ER. Based on the results in Figure 6, it shows that PAP is more energy efficient than PFP and TBP.

Network Lifetime

Network lifetime is the period between the start of the network operation and the first sensor node power outage (Jun *et al.*, 2014; Mutalemwa & Shin, 2021a).

The network lifetime model in Jun *et al.* (2014) was used to compute the network lifetime. It was observed that ER and network lifetime are contradictory, especially for sensor nodes in the near-sink regions. When ER is high in the near-sink regions, the network lifetime is limited. Figure 7 shows that TBP, PFP, and PAP incur shorter network lifetime than PSP. The network lifetime of PFP is limited mainly because the ER of PFP is high. It is also shown that the network lifetime decreases with the increase in source node packet rate. This is because the ER increases with the increase in packet rate as shown in Figure 6.

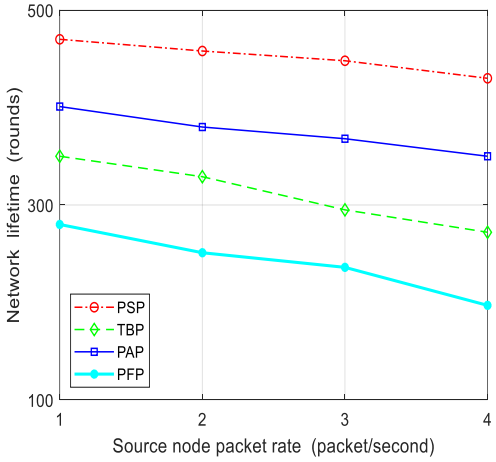

Figure 7: Network lifetime of the protocols.

Safety period reliability (R_{SP})

R_{SP} is the probability that the achieved SP is greater than or equal to the minimum required SP (Mutalemwa & Shin, 2021a). The R_{SP} was computed using Equation (2).

$$R_{SP} = \begin{cases} 1, & if\ e^{\Delta_{SP}} \geq 1 \\ 0, & otherwise. \end{cases} \quad (2)$$

The parameter Δ_{SP} represents the difference between the SP that is achieved by the protocols and the required SP according to the application-specific requirements (Mutalemwa & Shin, 2021a). More details of Equation (2) are available in Mutalemwa & Shin (2021a).

In the experiments, R_{SP} was observed for the mission duration of 1800 rounds. The source packet rate was fixed at 1 packet/second. Similar to (Mutalemwa & Shin, 2021a), it was assumed that the minimum required SP was 140 hops. Figure 8 shows the R_{SP} of the protocols. It is shown that the baseline PSP protocol is not able to provide the R_{SP}. Furthermore, it is shown that PAP and TBP are able to provide R_{SP} for long mission durations while PFP achieves short-term R_{SP}. PAP is the only protocol that is able to provide R_{SP} beyond 1500 rounds. PFP achieve short-term R_{SP} mainly because it incurs high ER and low energy efficiency. Beyond 1000 rounds, many of the sensor nodes in PFP incur power outage and the number of active sensor nodes is reduced. Consequently, fewer sensor nodes participate in the packet routing process and the amount of fake packet traffic is reduced. Therefore, the adversary obfuscation effect is reduced and the required SP is not achieved. The results indicate that although PFP is able to achieve high levels of SLP protection as

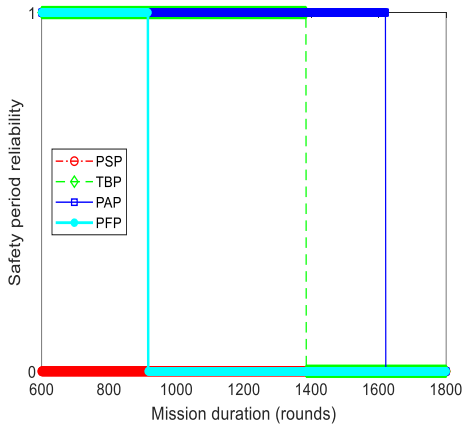

Figure 8: Safety period reliability of the protocols.

shown in Figure 3, due to low energy efficiency, PFP may be less practical when effective long-term SLP protection and R_{SP} are required.

End-to-end Delay (EED)

EED is the time taken for a packet to be transmitted across the network from a source node to the destination sink node (Mutalemwa & Shin, 2020b). Equation (3) was used to compute the EED.

$$EED = \frac{\sum_{i=1}^{P_{Rec_i}} (T_{Rec_i} - T_{Trans_i})}{P_{Rec}} \quad (3)$$

In the equation, T_{Rec} is the time when a data packet is received by the sink node. T_{Trans} is the time when a data packet is transmitted by a source node. P_{Rec} is the total number of data packets received at the destination sink node (Mutalemwa & Shin, 2020a).

Figure 9 shows the EED of the protocols. In the experiments, source nodes were assumed at various source-sink distances. The source packet rate was fixed at 1 packet/second. It is shown that the EED tends to increase with the increase in source-sink distance. This is mainly due to the fact that increased number of packet forwarding instances (hops) occur

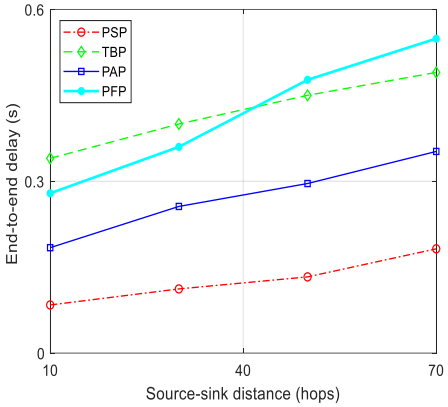

Figure 9: End-to-end delay of the protocols.

when the source-sink distance is long. Each hop involves some delay. Consequently, the EED increases with the increase in source-sink distance. TBP employs the longest routing paths because it locates the second-level phantom nodes in the network border regions. As a result, the EED of TBP is longer than the EED of the other protocols. However, the EED of PFP is longer when the source-sink distance is longer than 40 hops. This is due to the fact that PFP distributes a large amount of fake packet traffic. Consequently,

PFP incurs an increased number of packet collision, packet loss, and packet retransmission events. The EED increases when packet retransmission events occur for source nodes at long source-sink distances. Furthermore, PFP incurs long EED because it involves more computations during the route creation process.

SUMMARY OF THE OBSERVATIONS

Table 3 presents a summary of the observations from the simulation results above. It shows that for each protocol, there are some performance gains and limitations. Considering the location and size of UGR as shown in Wilfred (2020), it is assumed that scalability and energy efficiency are important parameters. Energy efficiency of the protocols is important to enable long network lifetime and effective long-term wildlife monitoring. Also, a protocol with good scalability is more practical because UGR is significantly large in size. Thus, based on the observations, TBP and PAP present practical performance features. To select between TBP and PAP, the network administrator may have to consider that TBP provides higher levels of SLP protection than PAP at a cost of reduced energy efficiency and increased EED.

Table 3: Summary of the observations

Protocol	Performance gains	Limitations
PFP	• Significantly high levels of SLP protection.	• Low energy efficiency. • Limited network lifetime • Short-term R_{SP}. • Poor scalability. • Long EED.
TBP	• High levels of SLP protection. • Good scalability. • Better energy efficiency and network lifetime than PFP. • Provides R_{SP} for longer mission duration than PFP.	• Long EED.
PAP	• High levels of SLP protection. • Good scalability. • Better energy efficiency and network lifetime than PFP and TBP. • Provides R_{SP} for longer mission duration than PFP and TBP. • EED is better than in PFP and TBP.	• Level of SLP is lower than in PFP and TBP.
PSP	• High energy efficiency and long network lifetime. • Low EED.	• Level of SLP is significantly lower than in PFP and TBP. • Poor scalability.

CONCLUSION

The exploitation of wildlife is highlighted as the second greatest threat to global diversity. Therefore, it is important to devise effective mechanisms for wildlife protection. Traditional methods for wildlife protection are labor-intensive, time-consuming, and less practical. Hence, advanced technologies and remote monitoring techniques are becoming increasingly popular for wildlife protection. In this study, it is observed that advanced technologies such as UAVs, VHF, GPS tracking, camera trapping, IoT, and WSNs present effective mechanisms for wildlife monitoring. SLP protection, sensor node energy consumption minimization, and network lifetime maximization are important parameters when SLP protocols in WSNs are

deployed to monitor wildlife in remote areas such as UGR. Simulation results show that the TBP and PAP protocols present advantageous performance features. Moreover, the simulation results indicate that TBP provides higher levels of SLP protection than PAP at a cost of reduced energy efficiency and network lifetime. Thus, PAP is better than TBP in terms of energy efficiency and network lifetime, and it is viable for long-term wildlife monitoring.

ACKNOWLEDGMENTS

The author used the facilities at the Open University of Tanzania to conduct this study. She greatly appreciates the support of the Open University of Tanzania.

REFERENCES

Arshad, B., Barthelemy, J., Pilton, E., & Perez, P. (2020). Where is my Deer?-Wildlife Tracking And Counting via Edge Computing And Deep Learning. *2020 IEEE SENSORS*, 1–4. https://doi.org/10.1109/SENSORS47125.2020.9278802

Baig z, T., & Shastry, C. (2023). Design of WSN Model with NS2 for Animal Tracking and Monitoring. *Procedia Computer Science*, *218*, 2563–2574. https://doi.org/10.1016/j.procs.2023.01.230

Bayram, H., Doddapaneni, K., Stefas, N., & Isler, V. (2016). Active localization of VHF collared animals with aerial robots. *2016 IEEE International Conference on Automation Science and Engineering (CASE)*, 934–939. https://doi.org/10.1109/COASE.2016.7743503

Begum H., M., Janeera, D. A., & Kumar. A.G, A. (2020). Internet of Things based Wild Animal Infringement Identification, Diversion and Alert System. *2020 International Conference on Inventive Computation Technologies (ICICT)*, 801–805. https://doi.org/10.1109/ICICT48043.2020.9112433

Behera, T. M., Mohapatra, S. K., Samal, U. C., Khan, M. S., Daneshmand, M., & Gandomi, A. H. (2020). I-SEP: An Improved Routing Protocol for Heterogeneous WSN for IoT-Based Environmental Monitoring. *IEEE Internet of Things Journal*, *7*(1), 710–717. https://doi.org/10.1109/JIOT.2019.2940988

Butun, I., Osterberg, P., & Song, H. (2020). Security of the Internet of Things: Vulnerabilities, Attacks, and Countermeasures. *IEEE Communications Surveys & Tutorials*, *22*(1), 616–644. https://doi.org/10.1109/COMST.2019.2953364

Caballero, L. C., Saito, C., Micheline, R. B., & Paredes, J. A. (2017). On the design of an UAV-based store and forward transport network for wildlife inventory in the western Amazon rainforest. *2017 IEEE XXIV International Conference on Electronics, Electrical Engineering and Computing (INTERCON)*, 1–4. https://doi.org/10.1109/INTERCON.2017.8079658

Camal, L., & Aksanli, B. (2020). Building an Energy-Efficient Ad-Hoc Network for Wildlife Observation. *Electronics*, *9*(6), 984. https://doi.org/10.3390/electronics9060984

Chen, J., Xu, H., Wu, J., Yue, R., Yuan, C., & Wang, L. (2019). Deer Crossing Road Detection With Roadside LiDAR Sensor. *IEEE Access*, *7*, 65944–65954. https://doi.org/10.1109/ACCESS.2019.2916718

Dominguez-Morales, J. P., Duran-Lopez, L., Gutierrez-Galan, D., Rios-Navarro, A., Linares-Barranco, A., & Jimenez-Fernandez, A. (2021). Wildlife Monitoring on the Edge: A Performance Evaluation of Embedded Neural Networks on Microcontrollers for Animal Behavior Classification. *Sensors*, *21*(9), 2975. https://doi.org/10.3390/s21092975

Dulari, P., Bhushan, A., Bhushan, B., & C. Chandel, V. (2020). Internet of Things (IoT) to Study the Wild Life: A Review. *Journal of Biological and Chemical Chronicles*, *6*(2), 11–15. https://doi.org/10.33980/jbcc.2020.v06i02.002

Duran-Lopez, L., Gutierrez-Galan, D., Dominguez-Morales, J., Rios-Navarro, A., Tapiador-Morales, R., Jimenez-Fernandez, A., Cascado-Caballero, D., & Linares-Barranco, A. (2019). A Low-power, Reachable, Wearable and Intelligent IoT Device for Animal Activity Monitoring: *Proceedings of the 11th International Joint Conference on Computational Intelligence*, 516–521. https://doi.org/10.5220/0008493505160521

Elias, A. R., Golubovic, N., Krintz, C., & Wolski, R. (2017). Where's The Bear?: Automating Wildlife Image Processing Using IoT and Edge Cloud Systems. *Proceedings of the Second International Conference on Internet-of-Things Design and Implementation*, 247–258. https://doi.org/10.1145/3054977.3054986

Feng, W., Ju, W., Li, A., Bao, W., & Zhang, J. (2019). High-Efficiency Progressive Transmission and Automatic Recognition of Wildlife Monitoring Images With WISNs. *IEEE Access*, *7*, 161412–161423. https://doi.org/10.1109/ACCESS.2019.2951596

Gu, C., Bradbury, M., & Jhumka, A. (2019). Phantom walkabouts: A customisable source location privacy aware routing protocol for wireless sensor networks. *Concurrency and Computation: Practice and Experience*, *31*(20). https://doi.org/10.1002/cpe.5304

Gu, C., Jhumka, A., & Maple, C. (2022). Silence is Golden: A Source Location Privacy Scheme for Wireless Sensor Networks Based on Silent Nodes. *Security and Communication Networks*, *2022*, 1–16. https://doi.org/10.1155/2022/5026549

Han, G., Wang, H., Jiang, J., Zhang, W., & Chan, S. (2018). CASLP: A Confused Arc-Based Source Location Privacy Protection Scheme in WSNs for IoT. *IEEE Communications Magazine*, *56*(9), 42–47. https://doi.org/10.1109/MCOM.2018.1701062

Haucke, T., Kühl, H. S., & Steinhage, V. (2022). SOCRATES: Introducing Depth in Visual Wildlife Monitoring Using Stereo Vision. *Sensors*, *22*(23), 9082. https://doi.org/10.3390/s22239082

He, Z., Kays, R., Zhang, Z., Ning, G., Huang, C., Han, T. X., Millspaugh, J., Forrester, T., & McShea, W. (2016). Visual Informatics Tools for Supporting Large-Scale Collaborative Wildlife Monitoring with Citizen Scientists. *IEEE Circuits and Systems Magazine*, *16*(1), 73–86. https://doi.org/10.1109/MCAS.2015.2510200

Ibrahim, H., Mariapan, M., Lin, E. L. A., & Bidin, S. (2021). Wildlife Conservation through Economically Responsible Ecotourist: The Mediator Roles of Attitude between Anticipated Emotion and Intention to Stay in Local Homestays. *Sustainability*, *13*(16), 9273. https://doi.org/10.3390/su13169273

Isabelle, D. A., & Westerlund, M. (2022). A Review and Categorization of Artificial Intelligence-Based Opportunities in Wildlife, Ocean and Land Conservation. *Sustainability*, *14*(4), 1979. https://doi.org/10.3390/su14041979

Islam, S. B., & Valles, D. (2020). Identification of Wild Species in Texas from Camera-trap Images using Deep Neural Network for Conservation Monitoring. *2020 10th Annual Computing and Communication Workshop and Conference (CCWC)*, 0537–0542. https://doi.org/10.1109/CCWC47524.2020.9031190

Ivanova, S., Prosekov, A., & Kaledin, A. (2022). A Survey on Monitoring of Wild Animals during Fires Using Drones. *Fire*, *5*(3), 60. https://doi.org/10.3390/fire5030060

Jia, L., Tian, Y., & Zhang, J. (2022). Identifying Animals in Camera Trap Images via Neural Architecture Search. *Computational Intelligence and Neuroscience*, *2022*, 1–15. https://doi.org/10.1155/2022/8615374

Jiang, J., Han, G., Wang, H., & Guizani, M. (2019). A survey on location privacy protection in Wireless Sensor Networks. *Journal of Network and Computer Applications*, *125*, 93–114. https://doi.org/10.1016/j.jnca.2018.10.008

Jun Long, Mianxiong Dong, Ota, K., & Anfeng Liu. (2014). Achieving Source Location Privacy and Network Lifetime Maximization Through Tree-Based Diversionary Routing in Wireless Sensor Networks. *IEEE Access*, *2*, 633–651. https://doi.org/10.1109/ACCESS.2014.2332817

Kamarei, M., Patooghy, A., Alsharif, A., & Hakami, V. (2020). SiMple: A Unified Single and Multi-Path Routing Algorithm for Wireless Sensor Networks With Source Location Privacy. *IEEE Access*, *8*, 33818–33829. https://doi.org/10.1109/ACCESS.2020.2972354

Koh, L. P., Li, Y., & Lee, J. S. H. (2021). The value of China's ban on wildlife trade and consumption. *Nature Sustainability*, *4*(1), 2–4. https://doi.org/10.1038/s41893-020-00677-0

Krondorf, M., Bittner, S., Plettemeier, D., Knopp, A., & Wikelski, M. (2022). ICARUS—Very Low Power Satellite-Based IoT. *Sensors*, *22*(17), 6329. https://doi.org/10.3390/s22176329

Landaluce, H., Arjona, L., Perallos, A., Falcone, F., Angulo, I., & Muralter, F. (2020). A Review of IoT Sensing Applications and Challenges Using RFID and Wireless Sensor Networks. *Sensors*, *20*(9), 2495. https://doi.org/10.3390/s20092495

Lee, S., Song, Y., & Kil, S.-H. (2021). Feasibility Analyses of Real-Time Detection of Wildlife Using UAV-Derived Thermal and RGB Images. *Remote Sensing*, *13*(11), 2169. https://doi.org/10.3390/rs13112169

Lichtenstein, M., & Elkaim, G. (2020). Efficient GPS Scheduling in Wildlife Tags using an Extended Kalman Filter-based Uncertainty Suppression Strategy. *2020 IEEE/ION Position, Location and Navigation Symposium (PLANS)*, 1472–1475. https://doi.org/10.1109/PLANS46316.2020.9110246

Liu, W., Liu, H., Wang, Y., Zheng, X., & Zhang, J. (2019). A Novel Extraction Method for Wildlife Monitoring Images with Wireless Multimedia Sensor Networks (WMSNs). *Applied Sciences*, *9*(11), 2276. https://doi.org/10.3390/app9112276

Ma, A. (2022). Smart Wildlife Sentinel (SWS): Preventing Wildlife-Vehicle Collisions and Monitoring Road Ecology with Embedded IoT Systems and Machine Learning. *2022 IEEE MIT Undergraduate Research Technology Conference (URTC)*, 1–4. https://doi.org/10.1109/URTC56832.2022.10002174

Martin, E., Raso, S., Rogoszinski, Y., Starr, R., Bhada, S. V., & Wyglinski, A. (2021). A Systems Approach to Developing an Outdoor IoT Network for Wildlife Image Capture. *2021 IEEE International Symposium on Systems Engineering (ISSE)*, 1–5. https://doi.org/10.1109/ISSE51541.2021.9582539

Massawe, E. A., Kisangiri, M., Kaijage, S., & Seshaiyer, P. (2017). An Intelligent Real-Time Wireless Sensor Network Tracking System for Monitoring Rhinos and Elephants in Tanzania National Parks: A Review. *International Journal of Advanced Smart Sensor Network Systems*, *7*(4), 1–11. https://doi.org/10.5121/ijassn.2017.7401

Mitra, A., Bera, B., & Das, A. K. (2021). Design and Testbed Experiments of Public Blockchain-Based Security Framework for IoT-Enabled Drone-Assisted Wildlife Monitoring. *IEEE INFOCOM 2021 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, 1–6. https://doi.org/10.1109/INFOCOMWKSHPS51825.2021.9484468

Mutalemwa, L. C., & Shin, S. (2020a). Comprehensive Performance Analysis of Privacy Protection Protocols Utilizing Fake Packet Injection Techniques. *IEEE Access*, *8*, 76935–76950. https://doi.org/10.1109/ACCESS.2020.2989434

Mutalemwa, L. C., & Shin, S. (2020b). Secure Routing Protocols for Source Node Privacy Protection in Multi-Hop Communication Wireless Networks. *Energies*, *13*(2), 292. https://doi.org/10.3390/en13020292

Mutalemwa, L. C., & Shin, S. (2020c). Improving the Packet Delivery Reliability and Privacy Protection in Monitoring Wireless Networks. *2020 International Conference on Information and*

Communication Technology Convergence (ICTC), 1083–1088. https://doi.org/10.1109/ICTC49870.2020.9289583

Mutalemwa, L. C., & Shin, S. (2021a). Novel Approaches to Realize the Reliability of Location Privacy Protocols in Monitoring Wireless Networks. *IEEE Access*, *9*, 104820–104836. https://doi.org/10.1109/ACCESS.2021.3099499

Mutalemwa, L. C., & Shin, S. (2021b). Energy Balancing and Source Node Privacy Protection in Event Monitoring Wireless Networks. *2021 International Conference on Information Networking (ICOIN)*, 792–797. https://doi.org/10.1109/ICOIN50884.2021.9333901

Mutalemwa, L., & Shin, S. (2018). Strategic Location-Based Random Routing for Source Location Privacy in Wireless Sensor Networks. *Sensors*, *18*(7), 2291. https://doi.org/10.3390/s18072291

Naureen, A., Zhang, N., Furber, S., & Shi, Q. (2020). A GPS-Less Localization and Mobility Modelling (LMM) System for Wildlife Tracking. *IEEE Access*, *8*, 102709–102732. https://doi.org/10.1109/ACCESS.2020.2997723

Nguyen, H., Maclagan, S. J., Nguyen, T. D., Nguyen, T., Flemons, P., Andrews, K., Ritchie, E. G., & Phung, D. (2017). Animal Recognition and Identification with Deep Convolutional Neural Networks for Automated Wildlife Monitoring. *2017 IEEE International Conference on Data Science and Advanced Analytics (DSAA)*, 40–49. https://doi.org/10.1109/DSAA.2017.31

Nguyen, H. V., Chen, F., Chesser, J., Rezatofighi, H., & Ranasinghe, D. (2020). LAVAPilot: Lightweight UAV Trajectory Planner with Situational Awareness for Embedded Autonomy to Track and Locate Radio-tags. *2020 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS)*, 2488–2495. https://doi.org/10.1109/IROS45743.2020.9341615

Nijman, V., Ardiansyah, A., Langgeng, A., Hendrik, R., Hedger, K., Foreman, G., Morcatty, T. Q., Siriwat, P., van Balen, S. (Bas), Eaton, J. A., Shepherd, C. R., Gomez, L., Imron, M. A., & Nekaris, K. A. I. (2022). Illegal Wildlife Trade in Traditional Markets, on Instagram and Facebook: Raptors as a Case Study. *Birds*, *3*(1), 99–116. https://doi.org/10.3390/birds3010008

Ojo, M. O., Adami, D., & Giordano, S. (2021). Experimental Evaluation of a LoRa Wildlife Monitoring Network in a Forest Vegetation Area. *Future Internet*, *13*(5), 115. https://doi.org/10.3390/fi13050115

Prosekov, A., Vesnina, A., Atuchin, V., & Kuznetsov, A. (2022). Robust Algorithms for Drone-Assisted Monitoring of Big Animals in Harsh Conditions of Siberian Winter Forests: Recovery of European elk (Alces alces) in Salair Mountains. *Animals*, *12*(12), 1483. https://doi.org/10.3390/ani12121483

Razaque, A., Kejun, D., Xueqi, Z., Wanyue, L., Hani, Q. B., & Khan, M. J. (2018). Survey: Wildlife trade and related criminal activities over the internet. *2018 IEEE Long Island Systems, Applications and Technology Conference (LISAT)*, 1–6. https://doi.org/10.1109/LISAT.2018.8378037

Ross, R., Anderson, B., Bienvenu, B., Scicluna, E. L., & Robert, K. A. (2022). WildTrack: An IoT System for Tracking Passive-RFID Microchipped Wildlife for Ecology Research. *Automation*, *3*(3), 426–438. https://doi.org/10.3390/automation3030022

Roy, P. K., Singh, J. P., Kumar, P., & Singh, M. P. (2015). Source Location Privacy Using Fake Source and Phantom Routing (FSAPR) Technique in Wireless Sensor Networks. *Procedia Computer Science*, *57*, 936–941. https://doi.org/10.1016/j.procs.2015.07.486

Salem, S. I., Fujisao, K., Maki, M., Okumura, T., & Oki, K. (2021). Detecting and Tracking the Positions of Wild Ungulates Using Sound Recordings. *Sensors*, *21*(3), 866. https://doi.org/10.3390/s21030866

Santos, G. A. M. dos, Barnes, Z., Lo, E., Ritoper, B., Nishizaki, L., Tejeda, X., Ke, A., Lin,

H., Schurgers, C., Lin, A., & Kastner, R. (2014). Small Unmanned Aerial Vehicle System for Wildlife Radio Collar Tracking. *2014 IEEE 11th International Conference on Mobile Ad Hoc and Sensor Systems*, 761–766. https://doi.org/10.1109/MASS.2014.48

Santosh Kumar, S., Sushmitha, M., Sirisha, P., Shilpa, J., & Roopashree, D. (2018). Sound Activated Wildlife Capturing. *2018 3rd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT)*, 2250–2253. https://doi.org/10.1109/RTEICT42901.2018.9012357

Terada, K., Yoshida, E., Ishibashi, K., Mukai, H., & Yokotani, T. (2019). Implementation of IoT Networks Based on MQTT for Wildlife Monitoring System. *2019 IEEE International Conference on Internet of Things and Intelligence System (IoTaIS)*, 161–166. https://doi.org/10.1109/IoTaIS47347.2019.8980436

Torabi, A., Shafer, M. W., Vega, G. S., & Rothfus, K. M. (2018). UAV-RT: An SDR Based Aerial Platform for Wildlife Tracking. *2018 IEEE 88th Vehicular Technology Conference (VTC-Fall)*, 1–6. https://doi.org/10.1109/VTCFall.2018.8690711

Tuia, D., Kellenberger, B., Beery, S., Costelloe, B. R., Zuffi, S., Risse, B., Mathis, A., Mathis, M. W., van Langevelde, F., Burghardt, T., Kays, R., Klinck, H., Wikelski, M., Couzin, I. D., van Horn, G., Crofoot, M. C., Stewart, C. V., & Berger-Wolf, T. (2022). Perspectives in machine learning for wildlife conservation. *Nature Communications*, *13*(1), 792. https://doi.org/10.1038/s41467-022-27980-y

Vera-Amaro, R., Rivero-Ángeles, M. E., & Luviano-Juárez, A. (2020). Data Collection Schemes for Animal Monitoring Using WSNs-Assisted by UAVs: WSNs-Oriented or UAV-Oriented. *Sensors*, *20*(1), 262. https://doi.org/10.3390/s20010262

Wang, D., Shao, Q., & Yue, H. (2019). Surveying Wild Animals from Satellites, Manned Aircraft and Unmanned Aerial Systems (UASs): A Review. *Remote Sensing*, *11*(11), 1308. https://doi.org/10.3390/rs11111308

Wang, N., Fu, J., Li, J., & Bhargava, B. K. (2020). Source-Location Privacy Protection Based on Anonymity Cloud in Wireless Sensor Networks. *IEEE Transactions on Information Forensics and Security*, *15*, 100–114. https://doi.org/10.1109/TIFS.2019.2919388

Wang, Q., Zhan, J., Ouyang, X., & Ren, Y. (2019). SPS and DPS: Two New Grid-Based Source Location Privacy Protection Schemes in Wireless Sensor Networks. *Sensors*, *19*(9), 2074. https://doi.org/10.3390/s19092074

Washburn, B. E., Maher, D., Beckerman, S. F., Majumdar, S., Pullins, C. K., & Guerrant, T. L. (2022). Monitoring Raptor Movements with Satellite Telemetry and Avian Radar Systems: An Evaluation for Synchronicity. *Remote Sensing*, *14*(11), 2658. https://doi.org/10.3390/rs14112658

Wild, T. A., Schalkwyk, L. van, Viljoen, P., Heine, G., Richter, N., Vorneweg, B., Koblitz, J. C., Dechmann, D. K. N., Rogers, W., Partecke, J., Linek, N., Volkmer, T., Gregersen, T., Havmøller, R. W., Morelle, K., Daim, A., Wiesner, M., Wolter, K., Fiedler, W., … Wikelski, M. (2022). *A multi-species evaluation of digital wildlife monitoring using the Sigfox IoT network* [Preprint]. In Review. https://doi.org/10.21203/rs.3.rs-2272694/v1

Wilfred, P. (2020). *Assessment of Wildlife Poaching in Ugalla Game Reserve, Western Tanzania: Preferred Animal Species and Products*. *3*, 15.

Xiaohan Liu, Tao Yang, & Baoping Yan. (2015). Internet of Things for wildlife monitoring. *2015 IEEE/CIC International Conference on Communications in China - Workshops (CIC/ICCC)*, 62–66. https://doi.org/10.1109/ICCChinaW.2015.7961581

Xu, J., Solmaz, G., Rahmatizadeh, R., Turgut, D., & Boloni, L. (2016). Internet of Things Applications: Animal Monitoring with Unmanned Aerial Vehicle. *ArXiv:1610.05287 [Cs]*. http://arxiv.org/abs/1610.05287

Xu, L., Gholami, S., McCarthy, S., Dilkina, B., Plumptre, A., Tambe, M., Singh, R., Nsubuga, M., Mabonga, J., Driciru, M., Wanyama, F., Rwetsiba, A., Okello, T., & Enyel, E. (2020). Stay Ahead of Poachers: Illegal Wildlife Poaching Prediction and Patrol Planning Under Uncertainty with Field Test Evaluations (Short Version). *2020 IEEE 36th International Conference on Data Engineering (ICDE)*, 1898–1901. https://doi.org/10.1109/ICDE48307.2020.00198

Yoshida, E., Yokotani, T., Terada, K., Ishibashi, K., & Mukai, H. (2019). Concept for and Implementation of Wildlife Monitoring to Contribute Sustainable Development Goals. *2019 International Conference on Innovation and Intelligence for Informatics, Computing, and Technologies (3ICT)*, 1–6. https://doi.org/10.1109/3ICT.2019.8910281

Yue, D., Tong, Z., Tian, J., Li, Y., Zhang, L., & Sun, Y. (2021). Anthropomorphic Strategies Promote Wildlife Conservation through Empathy: The Moderation Role of the Public Epidemic Situation. *International Journal of Environmental Research and Public Health*, *18*(7), 3565. https://doi.org/10.3390/ijerph18073565

Zhang, Q., & Zhang, K. (2022). Protecting Location Privacy in IoT Wireless Sensor Networks through Addresses Anonymity. *Security and Communication Networks*, *2022*, 1–12. https://doi.org/10.1155/2022/2440313

Zhihai He. (2009). Energy-efficient integrated camera and sensor system design for wildlife activity monitoring. *2009 IEEE International Conference on Multimedia and Expo*, 1580–1581. https://doi.org/10.1109/ICME.2009.5202816Baig z, T., & Shastry, C. (2023). Design of WSN Model with NS2 for Animal Tracking and Monitoring. *Procedia Computer Science*, *218*, 2563–2574. https://doi.org/10.1016/j.procs.2023.01.230

Camal, L., & Aksanli, B. (2020). Building an Energy-Efficient Ad-Hoc Network for Wildlife Observation. *Electronics*, *9*(6), 984. https://doi.org/10.3390/electronics9060984

Chen, J., Xu, H., Wu, J., Yue, R., Yuan, C., & Wang, L. (2019). Deer Crossing Road Detection With Roadside LiDAR Sensor. *IEEE Access*, *7*, 65944–65954. https://doi.org/10.1109/ACCESS.2019.2916718

Dominguez-Morales, J. P., Duran-Lopez, L., Gutierrez-Galan, D., Rios-Navarro, A., Linares-Barranco, A., & Jimenez-Fernandez, A. (2021). Wildlife Monitoring on the Edge: A Performance Evaluation of Embedded Neural Networks on Microcontrollers for Animal Behavior Classification. *Sensors*, *21*(9), 2975. https://doi.org/10.3390/s21092975

Ma, A. (2022). Smart Wildlife Sentinel (SWS): Preventing Wildlife-Vehicle Collisions and Monitoring Road Ecology with Embedded IoT Systems and Machine Learning. *2022 IEEE MIT Undergraduate Research Technology Conference (URTC)*, 1–4. https://doi.org/10.1109/URTC56832.2022.10002174

Martin, E., Raso, S., Rogoszinski, Y., Starr, R., Bhada, S. V., & Wyglinski, A. (2021). A Systems Approach to Developing an Outdoor IoT Network for Wildlife Image Capture. *2021 IEEE International Symposium on Systems Engineering (ISSE)*, 1–5. https://doi.org/10.1109/ISSE51541.2021.9582539

Massawe, E. A., Kisangiri, M., Kaijage, S., & Seshaiyer, P. (2017). An Intelligent Real-Time Wireless Sensor Network Tracking System for Monitoring Rhinos and Elephants in Tanzania National Parks: A Review. *International Journal of Advanced Smart Sensor Network Systems*, *7*(4), 1–11. https://doi.org/10.5121/ijassn.2017.7401

Mitra, A., Bera, B., & Das, A. K. (2021). Design and Testbed Experiments of Public Blockchain-Based Security Framework for IoT-Enabled Drone-Assisted Wildlife Monitoring. *IEEE INFOCOM 2021 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, 1–6.

https://doi.org/10.1109/INFOCOMWKSHPS51825.2021.9484468

Nijman, V., Ardiansyah, A., Langgeng, A., Hendrik, R., Hedger, K., Foreman, G., Morcatty, T. Q., Siriwat, P., van Balen, S. (Bas), Eaton, J. A., Shepherd, C. R., Gomez, L., Imron, M. A., & Nekaris, K. A. I. (2022). Illegal Wildlife Trade in Traditional Markets, on Instagram and Facebook: Raptors as a Case Study. *Birds*, *3*(1), 99–116. https://doi.org/10.3390/birds3010008

Terada, K., Yoshida, E., Ishibashi, K., Mukai, H., & Yokotani, T. (2019). Implementation of IoT Networks Based on MQTT for Wildlife Monitoring System. *2019 IEEE International Conference on Internet of Things and Intelligence System (IoTaIS)*, 161–166. https://doi.org/10.1109/IoTaIS47347.2019.8980436

Zualkernan, I., Dhou, S., Judas, J., Sajun, A. R., Gomez, B. R., & Hussain, L. A. (2022). An IoT System Using Deep Learning to Classify Camera Trap Images on the Edge. *Computers*, *11*(1), 13. https://doi.org/10.3390/computers11010013