# A Review and Testing of Fault Tolerance Levels of Anti-Poaching Cybersecurity System

**Isabelle Heyl, Julia Stone, Takudzwa Vincent Banda, Vian Smit and Dewald Blaauw**
Stellenbosch University, Stellenbosch, South Africa

isabelle@nomail.co.za
juliastonee@gmail.com
tadiwanashebanda74@gmail.com
viansmit@gmail.com
dnblaauw@sun.ac.za

**Abstract:** The development of anti-poaching networks and systems has created a new environment for animals in game reserves all over the world. Advanced technologies such as heat sensors, drones, and trip wires help prevent poachers from entering the property and therefore, creating a safer environment for animals to roam freely. Radio frequency identification (RFID) systems are used to track the location of animals. These networks are, however, susceptible to being hacked if not properly protected with cybersecurity tools, resulting in cyber-criminals gaining access into the network. Many attacks or threats can be executed on the RFID network due to some exposed vulnerabilities of elements within the anti-poaching network. The purpose of this paper is to explore the empirical methods of common attacks, used by cyber-criminals, to attack the anti-poaching network, and whether these methods used are effective in identifying weaknesses within the network. This will be executed by creating an experimental structure of the anti-poaching system with a specialised focus on the RFID elements, using quantitative research methods to produce findings. GNS3, an open-source software application that has specifically been chosen to conduct this research, is used to build the network simulation in order to analyse the weaknesses of the network. Cybersecurity protocols are implemented to protect the network and aim to protect the animals. The attacks performed, such as Flood and Scapy attacks, have shown that the anti-poaching network is vulnerable to penetration from cyber-criminals. A hypothesis test was conducted to determine whether the attacks had a significant effect on the network, by using the average ping time from specific nodes to Google. It was found that the average ping time increased by 2.0020 units, therefore stating that the elements of the network were successfully attacked. The fault tolerance test shows that the availability of the anti-poaching network is roughly 90 percent which concludes that the network is configured to deliver quality performance and handle failures, should there be any intervention. This will allow game reserves to implement and have information on a better and safer RFID system for the animals.

**Keywords**: Anti-Poaching, Cybersecurity, GNS3, Radio-Frequency Identification, RFID, Cyber-Criminals

## 1. Introduction

The illegal activity of wildlife poaching has been active for years, killing innocent animals almost every day to generate money. Poaching statistics for 2022 released by the government of South Africa has shown an increase, and a worrying change in wildlife poaching. Anti-poaching units utilize highly developed technology to protect the wildlife from poachers and to help them fight against these organized crime units. Magnetic sensors are used to capture weapon and gun sounds to locate criminals, as well as a virtual net, which is created around the reserves with networks using the Internet of Things (IoT) to catch and identify poachers rather than animals (Pozniak. H, 2018). Thermal cameras prove to be advantageous as poachers can be seen in low visibility environments, and electric fences are covered with acoustic fibres that alert the staff if it has been tampered with. An active wi-fi connection allows staff to communicate with each other and watch live data while on patrol. Some animals are fitted with tracking devices so their location can always be traced and monitored. These tracking devices, called RFID tags, are connected to an encrypted RFID reader (Pozniak. H, 2018). A RFID network consists of RFID tags and RFID readers which forms part of the anti-poaching cybersecurity system. It is vital to consider the extend of the security of the RFID network in an anti-poaching situation. Anti-poaching units have implemented extensive technology to stand guard against cyber-criminals in the cyber warfare of animal poaching. Therefore, the purpose of this study is to test the fault tolerance levels within an anti-poaching cybersecurity system which is used to protect animals in reserves. This is done by demonstrating a cybersecurity anti-poaching network, performing a critical review of the fault tolerance levels and resulting in an analysis of the system.

## 2. Research Question

This paper aims to critically review and test the fault tolerance levels of an antipoaching cybersecurity system.

### 2.1 Problem Statement

Many high-tech systems are in place to prevent poaching, but unfortunately, they all experience some level of faults. Poachers use this information to gain entry into the anti-poaching system. The system must be able to protect against attacks and safeguard information to maintain efficient functioning. A denial of service (DDOS) attack is mostly performed by cyber-criminals which is executed by multiple packets of information sent to the communication channel thereby increasing the information load and reducing the performance of the reader. Reducing these cyber risks present in this cybersecurity system becomes of utmost importance.

### 2.2 Aims and Hypothesis

The aim of this paper is to critically review and perform tests to assess the fault tolerance levels within the anti-poaching cybersecurity system. Animal protection units are fighting a cyber warfare against hackers who want to penetrate anti-poaching networks to locate animals as part of their poaching tactic. A hypothesis test is conducted to determine whether the attacks have had a significant effect on the system by testing if the nodes can connect to each other or the internet. This is orchestrated by testing the ping time from each node to the internet, specifically Google, and whether it has increased. This allows us to determine whether our defence mechanisms have helped mitigate the outcome of attacks and protect the safety of animals in the context of poaching.

## 3. Literature review

### 3.1 Relevance of Cybersecurity components for anti-poaching

The importance of wildlife protection is greatly emphasised by both local and global government and wildlife conservation societies to prevent the poaching of animals (Tan et al, 2016). Countries such as, South Africa has passed the Animals Protection Act 71 of 1962, as well as in India, the Wildlife (Protection) Act 53 of 1972 was passed. There are many other laws in place in different countries. These laws were set in place to protect and conserve the ecological and environmental security of all countries. Diminishing wildlife has the possibility of impacting the tourism sector which would put a dent on the nation's long-term environmental and economic prosperity. Wildlife protection will aid the tourism sector (Anderson and Jooste, 2014) which contributed around 3.7 percent of South Africa's GDP in 2021 (South Africa Statista, 2022). Currently, much of the anti-poaching equipment is technologized, and is therefore, considered as major assets of South Africa. RFID systems are one of the main technologies used in anti-poaching systems to conserve wildlife. RFID networks are helpful in protecting the wildlife as they have a constant update on the animal's location. Other components such as, drones, motion sensors and cameras contribute immensely to their different aspects. Hence, maintaining a secure cybersecurity system around the anti-poaching components is fundamental in every game reserve.

### 3.2 Threats/Attacks to the anti-poaching system

This table describes some of the attacks performed by cyber-criminals when wanting to poach animals.

**Table 1: The attacks and threats performed on an anti-poaching system**

| Type of Attack | Description |
|---|---|
| Jamming | Preventing communication from the reader to the tag by redirecting the connection to a malicious reader. |
| Tag cloning | Cybercriminals will snoop the data of the tag and write it to another tag. Thereby, cloning the tag. (Kumar et al, 2021) |
| Replay attacks | The criminal will duplicate packets and send them to the reader multiple times. The reader then accepts the packets thinking it is the authentic tag. |
| Passive attacks | Also known as eavesdropping. Hackers gaining an entry into the communication channel by intercepting the signal. |

# 5. Methodology

## 5.1 Design proposed model

The systems and technologies used in the RFID reader will be investigated, along with the extent to their cybersecurity. A quantitative approach to research will be used to understand this real-life phenomenon whilst exploring the cyber security aspects of anti-poaching. GNS3 has been chosen as the simulation software because of its many features and vast capabilities. An adapted model is created, using the GNS3 platform, to show the flexibility of the relationship between the RFID reader and the rest of the system, by replicating an anti-poaching cybersecurity system. Kali Linux and various tools will be used through GNS3 to penetrate the simulated RFID system network to expose the weaknesses and threats of the reader as well as the network. The simulated network is an adapted design of a large-scale conventional anti-poaching system. This model, Figure 1, was used to validate the attacks on the network.

The RFID readers are modelled as nodes, while the tags are modelled as disconnected from the system to show how the animals roam around the reserve. The office control room represents a space where the network security management team is based, and where the security technologies are controlled. The room comprises of a network router, switches, RFID servers, management PCs, and a Honeypot. Redundant network design is employed to add additional communication pathways and provide standby routes for when, and if, a connection fails. This is modelled as the standbyRouter, standbyServer, standbyPC, standbyPC2, standbySwitch and loadbalancer. The active system and the standby system are protected with a Cisco Adaptive Security Appliance (ASA) firewall.

IP addresses of all the network nodes are Dynamic Host Configuration Protocol (DHCP) allowing them to use network services such as Domain Name System (DNS), Network Time Protocol (NTP) and Transmission Control Protocol (TCP). The field is a protected area where the wild animals are located and surrounded by wireless connected technological safeguards such as cameras, drones, motion sensors, and smoke detectors. Readers, tags, and backend servers are the three main players in the RFID system.

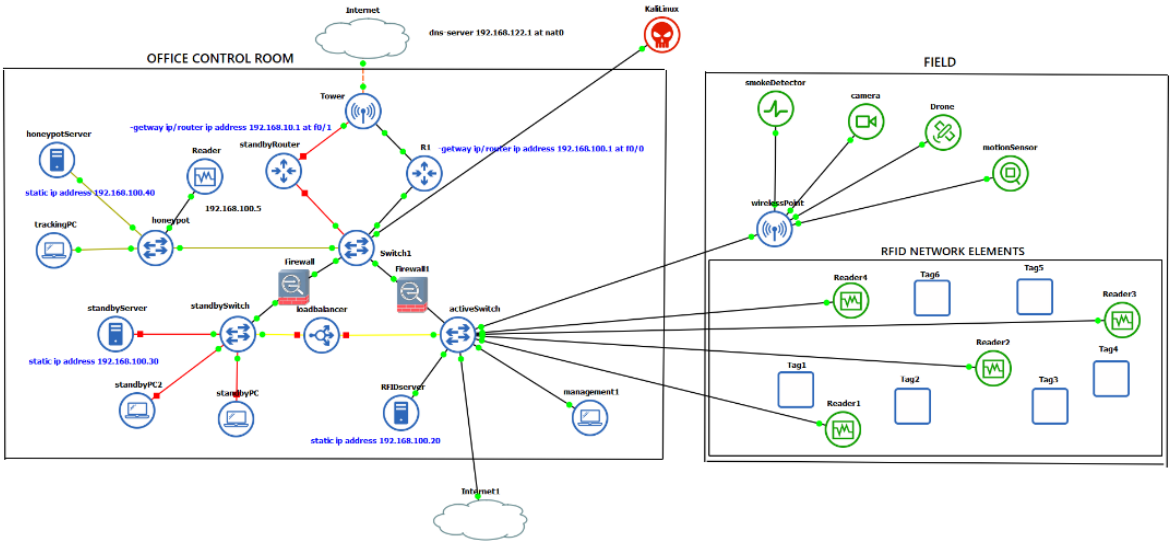


**Figure 1: Adapted design of the Anti-poaching system**

## 5.2 Overview of Router configuration

a) Network router (192.168.100.1)

b) Configure IP DHCP pool which assigns and manages IP addresses from network 192.168.100.0/24 within the router to DHCP clients.

c) DNS server (192.168.120.1)

All devices not protected by Cisco ASA firewall are IP DHCP 192.168.100.0 /24 network pool.

All devices protected by Cisco ASA firewall are IP DHCP 192.168.122.0 /24 network pool.

## 5.3 Implementation

In this phase, Kali Linux will be used to perform network attacks such as, Secure Socket Layer (SSL) STRIP, Address Resolution Protocol (ARP) poisoning, Flood attack, Scapy attack and Macof attack.

### *5.3..1 SSLSTRIP*

SSLSTRIP manipulates the internet traffic of the RFID system, by performing a man-in-the-middle attack. The Tracking PC with IP address 192.168.100.3, was attacked, as shown in Figure 2.


**Figure 2: Conducting the SSLSTRIP attack**

A Honeypot is set in place to lure network attackers, detect, deflect, and study hacking attempts. The console log did not come up with any data on the login details due to the Honeypot preventing the connection from the attacker to the management pc, as shown in Figure 3. This concludes that the RFID system is secure from cyber-criminals wanting to get access of passwords or sensitive information about the network and bypass the Honeypot.

`

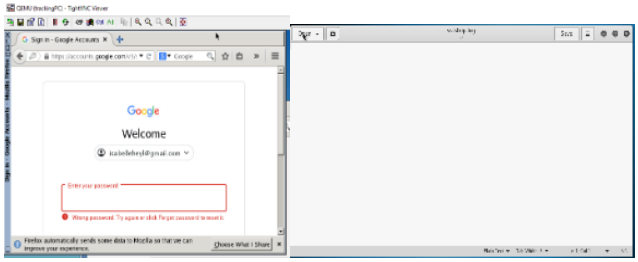


**Figure 3: Unsuccessful penetration of the attack**

### *4.3.2 ARP poisoning*

The purpose of the Address Resolution Protocol (ARP) attack was to redirect network traffic to the Kali machine (attacker) and therefore, disable the traffic flow for Reader (192.168.100.5). The attack, as shown in Figure 4, was configured to have the default gateway and IP address credentials of the reader.

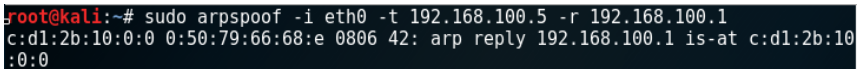


**Figure 4: Launching the ARP attack**

The Reader was unable to ping Google, as shown in Figure 5, due to Kali (attacker) redirecting the traffic from Reader to the Kali machine. Thereby stating that this attack was successful. The Reader is only protected by the Honeypot and not a firewall which shows that the Honeypot does not protect the network through packet manipulation, thereby Kali has used the Honeypot as an entry point into the network.

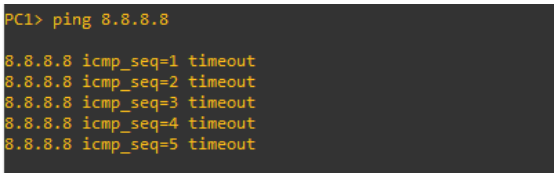


**Figure 5: Ping statistics of google from Reader**

### *4.3.3 Flood attack*

A very high volume of traffic is sent to the system in a Flood attack which is also known as a Denial of Service (DoS) attack. Figure 6 shows how 15000 packets (-c 15000) at a size of 120 bytes (-d 120) are being sent to port 80 (-p 80). The flood flag (--flood) is being used in conjunction with a transmission control protocol (TCP) sized at 64 (-w 64). The flood attack is executed on the Honeypot (192.168.100.2).

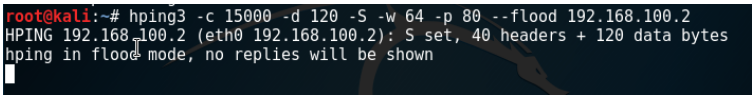


**Figure 6: Flood attack on Honeypot**

The Management1 node (192.168.100.6) was pinged by the Honeypot (192.168.100.2) as shown in Figure 7, and the destination was unreachable due to previous attacks performed on the Honeypot. This concludes that the flood attack was successful.

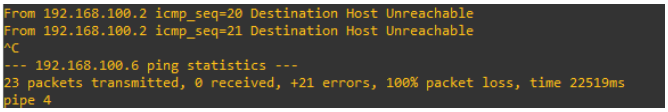


**Figure 7: Ping statistics of Honeypot and Management1**

When the Honeypot tried to connect to Node (192.168.100.4) it was successful but when Node (192.168.100.4) tried to ping the Honeypot, it was unsuccessful. Figure 8 shows that the Honeypot is still connected to the network yet unable to get a response to the other nodes due to the attack. The Honeypot is protecting the network by rejecting all communication from other nodes.

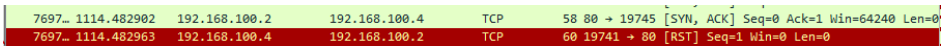


**Figure 8: Ping statics on Wireshark**

### *4.3.4 Scapy attack*

Scapy is a packet manipulation tool. The goal is to trick Reader3 (192.168.122.212) in the network into sending a legitimate packet to Management1 (192.168.122.181). To do that the attacker will impersonate the reader. Figure 9 shows the execution of the attack.

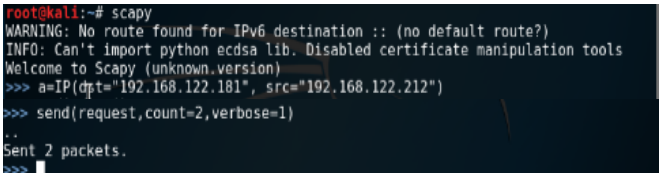


**Figure 9: Launching Scapy attack**

Figure 10 shows the analysis in Wireshark, this states that the source and destination was computed from Reader3 to Management1, which was completed by Kali, the attacker. This attack was successful, and Kali has broken through Firewall1 due to vulnerabilities present in the firewall.

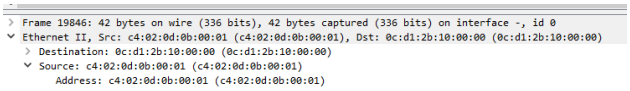


**Figure 10: MAC Addresses of Management1 and Reader3**

### *4.3.5 Macof attack*

This attack floods a switch with fake mac addresses. The switch doesn't know where exactly to send out the information, so it starts acting like a hub. Anyone listening into the network can then track the information. Figure 11 shows the attack performed on the network.

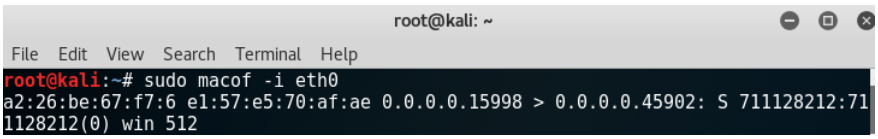


**Figure 11: Macof attack executed**

Wireshark, in Figure 12, has shown that fake MAC addresses were used as the source of sending many packets of information to the switch. This attack was successful in completing an execution by sending multiple packets and manipulating the switch into thinking they are authentic. This shows that packets are able to move freely around the network.

| No. | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 19782 | 650.727442 | 145.225.13.91 | 110.246.106.66 | IPv4 | 60 | |
| 19783 | 650.727648 | 222.148.188.78 | 56.29.209.74 | IPv4 | 60 | |
| 19784 | 650.727876 | 84.35.96.18 | 36.82.112.38 | IPv4 | 60 | |
| 19785 | 650.728066 | 249.69.255.97 | 133.2.109.89 | IPv4 | 60 | |
| 19786 | 650.733255 | 31.93.94.66 | 150.47.237.76 | IPv4 | 60 | |
| 19787 | 650.733553 | 27.149.112.77 | 14.96.203.25 | IPv4 | 60 | |
| 19788 | 650.733900 | 61.89.242.73 | 102.169.22.121 | IPv4 | 60 | |
| 19789 | 650.734390 | 97.227.170.52 | 1.21.22.1 | IPv4 | 60 | |
| 19790 | 650.734699 | 229.27.15.7 | 180.55.17.10 | IPv4 | 60 | |
| 19791 | 650.735034 | 232.67.5.78 | 121.84.73.108 | IPv4 | 60 | |

**Figure 12: The result shows the fake MAC Addresses**

### 5.4 Attack Summary

These attacks have shown that the RFID system is susceptible to penetration from cyber-criminals and poachers wanting to get information on the animal. Although, if the criminal wanted to get sensitive information of the network system, the system was strong enough to hold, due to the Honeypot preventing the SSLSTRIP attack.

## 6. Findings

### 6.1 Hypothesis testing

R was used to perform an analysis on the datasets. The first step was to determine whether the data are normally distributed. The Shapiro-Wilk normality test was used to test for normality. It was found that the Honeypot data are normally distributed (p-value = 0.614 > α = 0.05), the Tracking PC data are normally distributed (p-value = 0.1115 > α = 0.05), meaning that the majority of the recorded times show similarities. The data of Reader3 are not normally distributed (p-value = 0.002271 < α = 0.05). As a result, we used the paired samples t-test for the Honeypot and Tracking PC datasets, and the Mann-Whitney U test for the Reader3 dataset. The average of five pings to Google per node was taken, before and after an attack. Since the Reader had an output of "timeout" when pinging Google, 0 was used to indicate that nothing happened, as shown in Figure 13. The average ping time for the Honeypot increased by 0.9930 units. The average ping time for the Tracking PC increased by 283.3812 units. The average ping time for the Reader3 increased by 2.0020 units. There was a slight increase in the ping time, as shown in Figure 13.

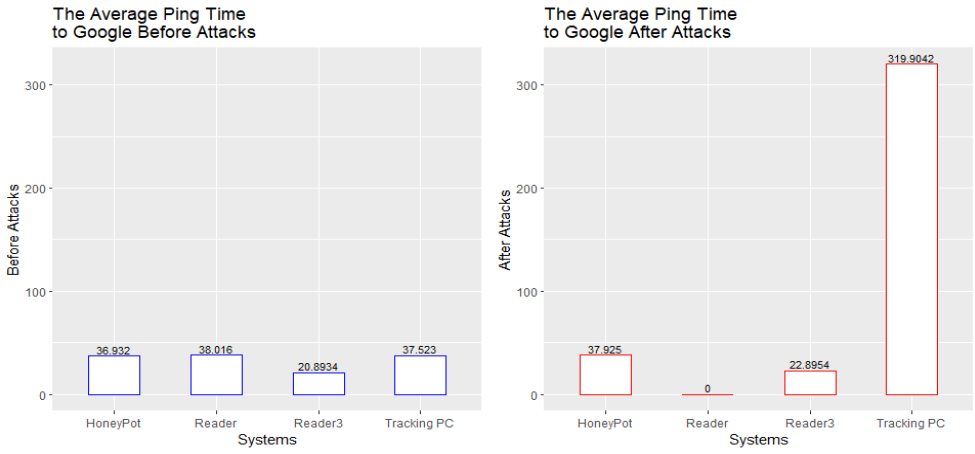


**Figure 13: Graphs of the ping-time taken before and after the attacks**

#### *5.1.1 Honeypot hypothesis test*

Let m = the mean difference in the ping times before and after an attack

$$H_0: m = 0$$

$$H_a: m \neq 0$$

significance level $\alpha$=0.05

Since the p-value = 0.836 > $\alpha = 0.05$, we do not reject the null hypothesis, we can conclude that the average ping time after the attacks is not significantly different to the average ping time before the attacks.

```
data:  PingTimes by TypeofAttack
t = 0.22087, df = 4, p-value = 0.836
```

**Figure 14: p-value for Honeypot**

*5.1.2 PC hypothesis test*

Let m = the mean difference in the ping times before and after an attack

$$H_0: m = 0$$

$$H_a: m \neq 0$$

significance level $\alpha$=0.05

Since the p-value = 0.0621 > $\alpha = 0.05$, we do not reject the null hypothesis, we can conclude that the average ping time after the attacks is not significantly different to the average ping time before the attacks.

```
data:  PingTimes2 by TypeofAttack2
t = 2.5682, df = 4, p-value = 0.0621
```

**Figure 15: p-value for Tracking PC**

*5.1.3 Reader3 hypothesis test*

$$H_0: The\ distribution\ of\ the\ ping\ times\ are\ approximately\ equal$$

$$H_a: The\ distribution\ of\ the\ ping\ times\ are\ not\ equal$$

significance level $\alpha = 0.05$

Since the p-value = 0.4034 > $\alpha = 0.05$, we do not reject the null hypothesis. We can conclude that there is not a significant difference between the distribution of the ping times before attacks and after attacks.

```
W = 17, p-value = 0.4034
alternative hypothesis: true location shift is not equal to 0
```

**Figure 16: p-value for Reader3**

Even though Figure 13 shows that there is an increase in the ping time after an attack, our hypotheses conclude that there is no significant evidence to support that.

### 6.2 Fault Tolerance Testing

MTBF (Mean time before fail) = number of hours the system is in use/number of failures encountered

$$MTBF = \frac{28}{2} = 14$$

MTTR (Mean Time Taken to Repair) = number of minutes spent repairing the system/number of repairs

$$MTTR = \frac{3}{2} = 1.5$$

Availability = MTBF/(MTTR + MTBF)

$$Availability = \frac{14}{(14 + 1.5)} = 0.9032$$

We can conclude that the availability of our network is 90.32%

## 7. Conclusion

The implementation of cybersecurity within game reserves is desperately needed to protect wildlife and reduce the illegal trade of rhino horns on the black market. Although, this paper has emphasised that attacks on the network can easily be performed, cyber-criminals are proved to not always be successful. This is achieved due to firewalls and Honeypots preventing network penetration, for example, in the SSLSTRIP attack. It is important to note that performing such attacks help in identifying the fault tolerance levels of the RFID system as it pointed out the weaknesses present in the system, and therefore analyses the protection of the network. The fault

tolerance test produced an availability of 90.32 percent which concludes that the anti-poaching network is able to operate continuously at a rate of 90.32 percent without failure. GNS3 is an effective tool in providing the network's security system to be adapted while performing and attempting attacks. The research has concluded that the adapted anti-poaching cybersecurity RFID system is secure and safe from cyber-criminals if proper tools are used to prevent these attacks, such as firewalls. R played an important role in analysing the network while visualising the attack performance through graphs.

## 8. Recommendations for Further Research

This paper proposes that additional research must be done to further protect the animals from cyber-criminals. In order to perform a complete hypothesis on whether the ping time increased or not, a larger dataset should be used so that there is a lower estimation variance thus a better predictive model. The results gathered yield sufficient evidence to support the notion that fault tolerance is critical for technological systems. Hardware solutions and software solutions such as the use of Cyber Honeypots, Load Balancing, and the use of firewalls are hereafter recommended for extra protection of the cybersecurity anti-poaching system. A RFID tag could be developed with a larger frequency range to strengthen the connection to the reader, therefore preventing interception from a cyber-criminal. We recommend that further research and more advanced protection tools should be implemented to prevent attackers from gaining access into the RFID network, to further prevent poaching from all aspects.

## References

Anderson, B. and Jooste, J. (2014) *Wildlife poaching: Africa's surging trafficking threat*. National Défense Univ Fort Mcnair dc Africa Center for Strategic Studies.

Edwards, J. (2014) *World Wildlife Fund Uses RFID to Foil Poachers-A real-time tracking and monitoring solution helps protect endangered rhinos and other animals in Namibia*. Radio frequency identification (RFID) Journal newsletter.

Ibrahim, A.A.A., Nisar, K., Hzou, Y.K. and Welch, I. (2019) Review and analyzing RFID technology tags and applications. In *2019 IEEE 13th International Conference on Application of Information and Communication Technologies (AICT)* (pp. 1-4). IEEE.

Kumar, A., Jain, A.K. and Dua, M. (2021) *A comprehensive taxonomy of security and privacy issues in RFID*. Complex & Intelligent Systems, 7(3), pp.1327-1347.

Nieto Jiménez, A. and López-Muñoz, F.J. (2019) *GNS3 for Security Practitioners*. Diseño y Configuración de Sistemas Seguros en Red/Design and Configuration of Secure Network Systems.

O'Donoghue, P., and Rutz, C. (2016) Real-time anti-poaching tags could help prevent imminent species extinctions. *Journal Of Applied Ecology*, *53*(1), 5-10. https://doi.org/10.1111/1365-2664.12452

Pozniak, H. (2018) The tech battle we must not lose. *Engineering & Technology*, 13(5), pp.30-35.

Save The Rhino. (2022) *South Africa 2022 poaching stats | Save The Rhino*. [Online] Available at: <https://www.savetherhino.org/member/news/south-africa-2022-poaching-stats/>

Statista. (2022) South Africa: contribution of tourism to GDP | Statista. [Online] Available at: <https://www.statista.com/statistics/1290545/contribution-of-travel-and-tourism-to-gdp-in-southafrica/#:~:text=In%202020%2C%20travel%20and%20tourism,(GDP)%20of%20South%20Africa.>

Tan, T.F., Teoh, S.S., Fow, J.E. and Yen, K.S. (2016) Embedded human detection system based on thermal and infrared sensors for anti-poaching application. In *2016 IEEE Conference on Systems, Process and Control (ICSPC)* (pp. 37-42). IEEE.