POSTER: Unprotected geo-localisation data through ARGOS satellite signals: The risk of cyberpoaching

Jean Sebastien Finger
fingerj@eurecom.fr
Eurecom
Biot, France

Aurelien Francillon
aurelien.francillon@eurecom.fr
Eurecom
Biot, France

ABSTRACT

Biologists often need to rely on satellite transmitters to obtain otherwise inaccessible data on animal movements. This data is critical for the understanding and conservation of endangered species. In parallel, in the cybersecurity world, satellites have often been found to have low level of security, and transmit unprotected sensitive data. A junction of these two worlds could reveal a potential security breach that would present a real danger to already struggling animals. We have investigated one of the most widespread tracking system, ARGOS, to identify potential attack surfaces, with conservation biology in mind. We first describe ARGOS communications and localization mechanisms, from the transmitters to the reception stations. We identify the main threat model as being the possibility to decode the communications. Then, we mention tools already publicly available to receive and reverse-engineer the ARGOS signal. Intercepting this data could greatly facilitate the localization of protected animals for poachers. Then, we briefly discuss two other potential attacks (jamming and injection) that should be further considered. We finally discuss potential solutions to prevent these attacks. It is troubling that by tracking endangered animals for conservation efforts, security issues in the design of the trackers reveals their location and makes them easy prey for poachers.

KEYWORDS

ARGOS, Endangered, Reverse-engineering, Satellite

ACM Reference Format:
Jean Sebastien Finger and Aurelien Francillon. 2020. POSTER: Unprotected geo-localisation data through ARGOS satellite signals: The risk of cyberpoaching. In *13th ACM Conference on Security and Privacy in Wirelessand Mobile Networks (WiSec '20), July 8–10, 2020, Linz (Virtual Event),Austria.* ACM, New York, NY, USA, 2 pages. https://doi.org/10.1145/3395351.3401706

1 TRACKING

A transmitter is attached to an animal using methods such as collars, glue (e.g., turtles) or screws (e.g., sharks). The transmitter will send positional data to a receiver that will treat and provide the information to the user. The main methods are radio tracking (directional antenna) and satellite tracking (GPS or Doppler shift effect).

1.1 Satellite transmitters

While radio tracking is performed usually with a directional antenna on land or water, satellite tracking send data to the user autonomously. Different type of satellite transmitters are available, but we will focus on the most common. These transmitters send data at regular interval or when possible to the satellites (uplink signal) then the satellites send the message back to ground stations (downlink) where the data is processed and forwarded to clients.

1.2 Cyberpoaching

while useful to scientists, location data could also be of interest to unauthorized users [3]. This goes from nature passionates who acquired tracking material to find animals, to hunters (e.g., radio collared wolf in yellow stone) and poachers (e.g., hacking accounts containing tiger GPS localization). All these activities can have negative impact on wildlife with poaching being the most worrying.

Poaching is defined as illegal procurement of protected wildlife. Poaching can be done to kill what is perceived as a nuisance (e.g., wolves) or for feeding (e.g., whales). However the main reason is economical gain. For instance a Rhinoceros horn can sell for tens of thousand of dollars per kg. Unfortunately, such activities generally lead to the death of the animal. This can have dramatic consequences on species already endangered.

Although insecurity of satellite communications have been investigated in the past [4, 7], the risk of wildlife localization from reverse-engineering satellite signals seem largely unexplored ([3] discusses other tracking technologies). It is therefore important to understand the different vectors of attacks that could allow interception or tampering of tracking data going through these signals.

2 ARGOS

2.1 INTRODUCTION

ARGOS is a tracking system installed on low polar orbit satellites with worldwide coverage (Table 1). It specializes in location and environmental data collection, including animal tracking, and it is widely used by biologists. Therefore, ARGOS is an important system to characterize in the context of cyberpoaching. Other services such as Iridium and Globalstar are also used. If some studies have shown the possibility to reverse-engineer signals of some of theses other systems (e.g. [4]), the risk of cyberpoaching was not discussed. More research in this direction could lead to a more global understanding of this risk.

In the ARGOS system, an uplink signal is sent from the transmitter to the satellite. The received messages are then both immediately re-transmitted and saved for later transmission. The immediately

Permission to make digital or hard copies of part or all of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for third-party components of this work must be honored. For all other uses, contact the owner/author(s).
WiSec '20, July 8–10, 2020, Linz (Virtual Event),Austria
© 2020 Copyright held by the owner/author(s).
ACM ISBN 978-1-4503-8006-5/20/07.
https://doi.org/10.1145/3395351.3401706

Table 1: Satellites carrying ARGOS systems and the approximate frequencies of ARGOS data transmission

Satellites	VHF (137 MHz)	L-BAND (1700 MHz)
NOAA-15, 18, 19	DSB/TIP	?
METOP-A, B, C	?	HRPT
SARAL	-	L-Band: RTTM
ANGELS	-	L-Band

re-transmitted messages can be received by one of the (approximately) 60 ground stations around the globe. Because sometimes these stations miss some of the live messages, all saved messages are sent to three ground stations: Wallops Island (Virginia, US), Fairbanks (Alaska, US) and Svalbard (Norway) [2]. The main signals that carry the ARGOS data are the TIP/DSB signal at 137.35 MHz and 137.33 MHz and HRPT signal between 1680 MHz and 1707 MHz (Table 1, [1, 2, 8]).

2.2 ARGOS localization

2.2.1 Doppler effect. Localization with ARGOS is mostly performed by using the Doppler Shift Effect (DSE). The transmitter's emitted frequency is received at higher frequency by the satellite as it comes closer and lower frequency as it goes away.The received frequency equals the emitted frequency when the satellite is perpendicular to the transmitter. The distance is estimated by the slope around the carrier frequency. This method provides 2 possible positions which are then filtered with two possible algorithms: least square analyses or Kalman filtering. In case of high variation, these tools can mark locations as invalid [2]. With this method, the geo-localization data are only present in the downlink message.

2.2.2 Global Positioning System. On devices that have a GPS receiver, ARGOS units can also transmit the GPS localisation in the message payload. This has the advantage of increasing accuracy of data and reduce localization errors. However, the inclusion of GPS is likely to use more battery and GPS do not work well with species that are infrequently detectable (e.g. dense jungle). The GPS data is included in the data part of uplink message [2]. In this case the geo-localization data are included both in uplink message (GPS data) and in the downlink message (GPS plus DSE data).

3 INTERCEPTION OF THE ARGOS MESSAGES

Intercepting the geo-localization is the easiest attack and most likely to be performed. This can significantly simplify the hunt of animals. To do so, it appears that capturing both the uplink and downlink signals would be useful.

3.1 Uplink signal interception

One option to localize an emitter is by finding the signal and localizing the source using the signal strength. We do not detail it here, but this vector of attack should be considered in future studies.

Information on the protocol details is easily found on the web and show that data are sent in the clear [5]. With the provided step by step description given by Jasper Nance [5], it is possible to reverse-engineer the uplink message without difficulty. Intercepting the uplink message is valuable only if the GPS data are available or to obtain an ID for later retrieval.

3.2 Downlink signal interception

Tools to locate transmitters from the DSB/TIP downlink message have been developed by Jasper Nance [6]. Downlink signal always include localisation data (DSE or DSE+GPS) and will likely provide a larger coverage for less efforts than searching for transmitters uplink signals. Therefore making it the easiest solution for finding animals. Even if a multitude of other objects will also be localized, a program could easily filter out animal movements from other sources.

4 JAMMING AND INJECTION

We question whether jamming and injection attacks are feasible. Simulating an existing transmitter and sending fake signals could confuse the localization algorithms creating invalid data. Injecting fake locations might also be possible, however, it is very likely that scientists will detect differences between simulated and real movement.

Preventing proper data to reach scientists could also have negative impact on conservation effort. Space use and movement data are needed to design protected areas and advocate for international protections. It is therefore easy to imagine groups of people with economic/cultural interests in poaching to employ such techniques.

5 PREVENTION

We think that stream ciphers could provide enough protection when applied to the upstream and downstream messages protecting GPS position, the ID of the transmitter and preferably the DSE data. It is unclear if encrypting the DSE data is possible in already deployed systems. Still, preventing the association of multiple locations with the same transmitter (thanks to the stream cipher) might prevent attackers to distinguish between animal movements and the multitude of other transmitting objects, greatly reducing the usefulness of intercepting this signal.

We are now attempting to capture and decode the ARGOS signal using material readily available on the web to further investigate this potential threat.

REFERENCES

[1] Bosma, J., Carlier, S., Neri, E., Stojkovic, I., and Fransen, C. Hrpt/lrpt direct broadcast service specification. *EUMETSAT* (2000).

[2] CLS. Argos user's manual, 2016.

[3] Cooke, S. J., Nguyen, V. M., Kessel, S. T., Hussey, N. E., Young, N., and Ford, A. T. Troubling issues at the frontier of animal tracking for conservation and management. *Conservation Biology 31*, 5 (2017), 1205–1207.

[4] Moore, C. Spread spectrum satcom hacking: Attacking the globalstar simplex data service, 2015.

[5] Nance, J. Noaa argos tx, 2016.

[6] Nance, J. Noaa poes tip demodulation, 2016.

[7] Pavur, J., Moser, D., Lenders, V., and Martinovic, I. Secrets in the sky: on privacy and infrastructure security in dvb-s satellite broadband. In *Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks* (2019), pp. 277–284.

[8] Robel, J., Graumann, A., Kidwell, K., Aleman, R., Ruff, I., Muckle, B., and Kleespies, T. Noaa klm user's guide with noaa-n, n prime, and metop supplements. *National Oceanic and Atmospheric Administration, Washington.* (2014).