

# AUTHENTICATION VIA CHANNEL CRAFTING IN UNDERWATER ACOUSTIC NETWORKS



Davide Eccher, Paolo Casari  
University of Trento

## INTRODUCTION

### CONTEXT AND CHALLENGES

Underwater wireless acoustic communications and networks can enable many key applications, including security-critical operations, that require **security primitives**

It is **not** possible to adopt typical methods used in terrestrial wireless networks, which primarily rely on *cryptographic functions* because of:

- **Low computational power** -> priority on *power efficiency*
- **Limited bandwidth** -> minimize *overhead*

The *underwater acoustic channel* tends to be **unstable**

### GOAL

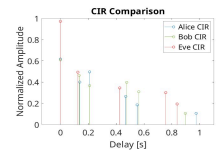
We propose a new method of **physical layer authentication** that exploits channel crafting



### CHANNEL PROPERTIES

The proposed authentication method relies on two properties of the physical acoustic channel:

- **Quasi-reciprocity** of the channel
- **Spatial and temporal de-correlation**



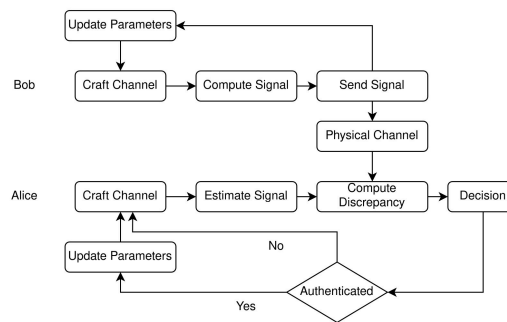
## PROPOSED METHOD

### TOKEN GENERATION

Extracts the most relevant **CIR contributions Average** with previously measured CIR  
Token generated by extracting and merging all the obtained **CIR statistics**

### CHANNEL CRAFTING

Starting from the token **generate** all the *delay* and *amplitude* values of the artificial channel  
The values depend also on the **message number** to avoid replay attacks



### CHANNEL MISMATCH

Metric that measures how **different** two channels are  
It creates bell-shaped curves around each CIR contribution and then multiplies them and sums the results

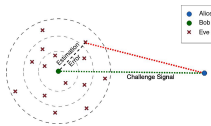
### DECISION

If the mismatch of the extracted CIR and the expected one is below a certain **threshold** the message is authenticated  
The threshold is computed by taking into account the mismatch of **previously authenticated messages**

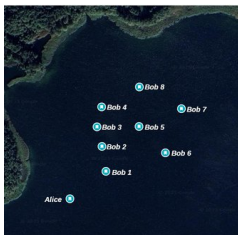
## RESULTS

### SCENARIO

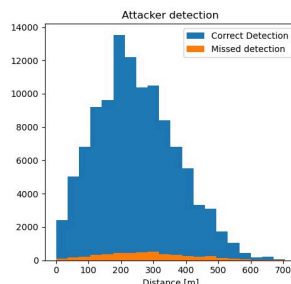
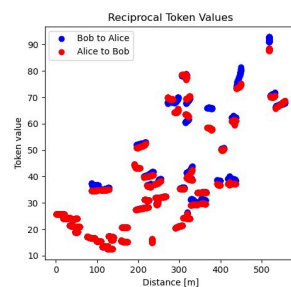
Different attackers (*Eve*) at increasing distances from *Bob*



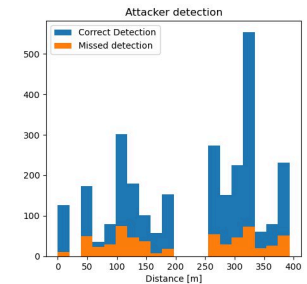
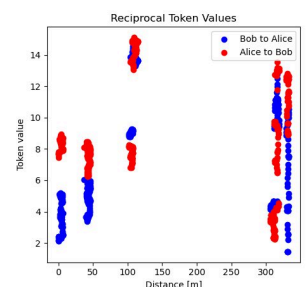
Real world data obtained at **Werbellinsee** near Berlin



### SIMULATIONS VS LAKE TEST



**Token values** computed from **both sides** of the communication (Bob and Alice)



Distribution of the **correct** and **missed detection** of an attacker.

The **authentication ratio** of *Bob* is **97%** in the simulations and **85%** in the lake test