New Drone Technology Enables Listening to Underwater Messages

Posted by Okachinepa 03/30/2025

Courtesy of SynEvol
Credit: Princeton University

Researchers at Princeton and MIT have created a technique to capture underwater communications from the sky, questioning deeply held assumptions about the safety of underwater transmissions.

The team developed a gadget that employs radar to intercept underwater acoustic signals, known as sonar, by interpreting the subtle vibrations generated by those signals on the water's surface. According to the researchers, the method could potentially provide a general estimate of where an underwater transmitter is situated.

In a paper delivered at ACM MobiCom on November 20, the team outlined the technology and suggested methods to protect against the novel form of eavesdropping it facilitates. They effectively showcased the system at Lake Carnegie, a petite artificial lake located in Princeton. Although employing this technique in the open sea poses significantly greater difficulties, the scientists think it could be feasible with considerable engineering progress.

The researchers stated that their goal is not only to warn individuals about the susceptibility of underwater communications, but also to outline strategies that can be implemented to stop eavesdropping.

"I hope that some of the countermeasure strategies we suggest will be adopted by those who create acoustic transmitters for underwater communication," stated Yasaman Ghasempour, assistant professor of electrical and computer engineering and the lead investigator of the study.

Sending messages between underwater and aerial devices was deemed technically impossible until MIT researchers created a system for this in 2018. However, the MIT method depended on collaboration between the air and sea teams — exchanging data rates, frequencies, and other crucial technical information beforehand. At that moment, it was uncertain if this method could effectively capture private messages from uncooperative underwater transmitters.

Working alongside the MIT team, Ghasempour and her colleagues at Princeton investigated the security ramifications of the technology and created a method to interpret similar types of messages without needing to understand any of those technical particulars.

The researchers stated that intercepting underwater communications from the air presents numerous security threats. They claimed that an opponent could exploit the technology to capture sensitive data sent by climate monitoring sensors, oil and gas platforms, and submarines.

“This research demonstrates that sensitive data can be exposed in previously unexamined manners,” stated Poorya Mollahosseini, a Princeton graduate student and co-lead author of the paper alongside Sayed Saad Afzal, a graduate student at MIT.

The researchers stated that the security of underwater communications depends greatly on the fact that sound traveling underwater cannot penetrate the surface. Information-bearing signals are sent underwater as sound waves. Due to the significant difference in densities between air and water, the surface of the water serves as a barrier to sound. When sound waves in water contact the surface, they primarily reflect off it.

In 2018, the MIT team discovered that the effect of sound waves on the surface of the water creates a type of fingerprint of minuscule vibrations that match the underwater signal. The group utilized a drone-mounted radar to sense surface vibrations and implemented algorithms to identify the pattern, interpret the signal, and retrieve the message.

“Communicating from underwater to air is one of the most challenging enduring issues in our domain,” stated Fadel Adib, associate professor of media arts and sciences at MIT and co-author of the recent paper. "It was thrilling – and unexpected – to witness our technique succeed in interpreting underwater communications from the minuscule vibrations they produced at the surface."

However, for the method to be effective, the MIT team’s system needed prior knowledge of specific physical parameters, like the transmission frequency and modulation type.

Expanding on this advancement, the Princeton team employed a comparable approach to identify surface vibrations, but created new algorithms that leverage the contrasts between radar and sonar to reveal those physical parameters. This enabled the researchers to interpret the message independently of the underwater transmitter's assistance.

The researchers employed a low-cost commercial drone and radar to evaluate their approach in a swimming pool. The scientists placed a speaker in the water and, while swimmers created disturbances, operated a drone above the surface. The drone constantly emitted short radar pings toward the water. When the radar signals reflected off the water’s surface, they displayed the pattern of vibrations from the sound waves for the system to identify and interpret.

The researchers additionally employed a boom-mounted radar for experiments in a practical setting at Carnegie Lake in Princeton. They discovered that the system was capable of identifying the unknown parameters and interpreting messages from the speaker, despite disruptions from wind and waves. In reality, it might identify the modulation type, a crucial parameter, with an accuracy of 97.58%.

"We aimed to demonstrate that this could be accomplished using standard, basic tools," Ghasempour stated. "Consider what one might achieve with a more advanced radar."

They discovered that the design factors of an underwater communication link significantly influence its vulnerability to these types of attacks. Certain forms of modulation, for instance, are simpler to understand than others. The article offers suggestions for creating transmitters that are less susceptible to eavesdropping. Ghasempour expressed her desire to continue providing additional recommendations for methods to safeguard against such attacks.