Army researchers earn patent for secure communications invention

13 August 2020

Researchers from the Army's corporate laboratory and Lehigh University receive a patent for inventing a practical method for Army wireless devices, such as radios, to covertly authenticate and communicate. Credit: (Jason Edwards)

Army researchers have been awarded a patent for inventing a practical method for Army wireless devices to covertly authenticate and communicate.

Authentication is one of the core pillars of wireless communications security, along with secrecy and privacy. The value of authentication in a military setting is readily apparent and mandatory.

Receivers verify that an incoming transmission did indeed come from an ally and not a malicious adversary, therefore maintaining the integrity of communications. This invention, in particular, greatly increases an adversary's difficulty in impersonating an ally.

The researchers, including Drs. Paul Yu and Brian Sadler from the U.S. Army Combat Capabilities Development Command's Army Research Laboratory and Prof. Rick Blum and Dr. Jake Perazzone from Lehigh University, have invented a method to perform two tasks simultaneously: verifying the authenticity of wireless communications and communicating secret information.

Typically one or the other is done, but not both.

"In our invention, we take advantage of our wireless authentication capability to enable the covert communication of additional information," Yu said. "There are many uses of this synergistic capability including the maintenance of strong security through the establishment of shared secrets as well as low-rate covert communications."

The invention utilizes a shared key to create a secret code book, which is used to achieve authentication and establish an additional secure communications channel, Yu said. An adversary, not knowing the key, is unable to create the code book and thus cannot reliably impersonate legitimate parties.

"A secret key is used to generate a low-rate secret code book that is used to provide both authentication of a primary message and side-channel communication of a secure secondary message," Sadler said. "The code word chosen from the secret code book is superimposed on the primary message waveform and is used as an identification tag so the receiver can securely and privately verify the identity of the source. The additional information is conveyed through the choice of a valid code word."

A previous physical layer authentication patent by the CCDC ARL inventors considers the use of only one valid tag for the sole purpose of authentication. This expanded new scheme allows for a set of valid tags constructed in a way that introduces more uncertainty for an adversary and allows a small secondary message to be sent securely, Yu said. The new patent allows for greater flexibility in implementing the scheme.

Among other purposes, Yu said, the additional secure secondary message can provide a way in which the key can be updated to protect against future attacks. This would directly address the need to periodically change the secret keys shared by legitimate parties.

Authentication in general also holds great importance in the commercial wireless communications sector.

"Key agreement is even harder in commercial settings where there are less obvious backchannels for sharing additional key information, so other computational methods are utilized," Yu said. "The secure secondary message can be used to help communicate new key information to fluidly evolve the key over time to maintain an adversary's confusion."

The patent, awarded Aug. 4, is based on work published in the Institute of Electrical and Electronics Engineers' Transactions on Information Forensics and Security, and extends an earlier patent.

The invention has been verified via detailed simulations. Earlier experiments using software-defined radios have shown that such a physical layer authentication scheme can be implemented successfully, as patented previously.

This research supports the Network Army Modernization Priority by establishing a method for efficient and future-proof secure wireless communications.

"My team is focused on developing technology that is well-suited to be put into the hands of the Soldier in the not-too-distant future," Yu said. "We are optimistic that by keeping an eye on future threats while exploring the art of the possible, we can help the future Army network be resilient and robust to the future threat environment."

More information:
www.ieee.org/membership-catalo … l?product=PER204-ELE

Provided by The Army Research Laboratory