Covert Communication: Past, Present and Future

Peng Jiang

School of Cyberspace Science and Technology,
Beijing Institute of Technology, Beijing, China.
pengjiang@bit.edu.cn

Abstract. Covert communication is defined as the exchange of information/data via a covert channel. It enables the covert information transmission against communication signal detection, such that no attackers can launch illegal behaviors without detecting the signal. Covert communication has been mandatory for the message transmission in many applications such as underwater acoustic and military communications.

In this talk, I will first review the traditional covert communication including the basic model and mechanisms. A core task in the covert communication is to design and deploy the covert channel which is usually built upon the network protocol. Such network-based covert channels have limitations on concealment, reliability and anti-traceability. Next, I will introduce present solutions for covert communication using blockchain, i.e., blockchain-based covert communication, which hides covert information into transactions and breaks through the above limitations. I will depict its system architecture and potential application scenarios, such as digital evidence preservation. Blockchain's inherent features, like low throughput, flooding propagation, openness and transparency, incur new challenges and impede the construction of blockchain-based covert channels. For the covert channel building, I will present three key technologies: information embedding, transaction filtering, and transaction obfuscation. To better evaluate blockchain-based covert channel, I will present metrics of concealment, bandwidth, transmission delay, robustness and transmission cost. Finally, I will point out the possible privacy issues with perspectives of blockchain users and communicating parties, and provide the potential countermeasures. I will also show technical challenges on the blockchain-based covert communication and offer corresponding research directions in aspects of communication modes, channel building techniques, efficiency, evaluation methods etc.