On the differences between Covert Channels and Interference

Loic Helouet, Aline Roumy

On the differences between Covert Channels and Interference

Loïc Hélouët and Aline Roumy

IRISA, INRIA, Rennes, France
loic.helouet@irisa.fr,aline.roumy@irisa.fr

Since the seminal paper by Goguen & Messeguer in 1982 [1], it is frequently written that cover channels are a specific case of interference. Let us recall the definition of both notions. We consider a system S, in which several agents are allowed to perform actions. In addition to the system, several security rules indicate which (sequences of) actions should remain unobservable (secret), which users are allowed to communicate (confinement), etc. An user u **interferes** with an user v in a system S if and only if what u does can affect what v can observe or do. Interference then characterizes information leaks, as through its observations, user v can learn what user u does.

The term **covert channel** was introduced by [3]. We say that there is a covert channel from an user u to another user v (which are not allowed to communicate otherwise) of a system S if and only if user u can transmit a message of arbitrary size to v through its use of S.

Though both definitions seem very close, there are some major differences. First of all, an interference can occur from an user u to an user v even when u is an honest agent of the system, while covert channels suppose an a priori agreement of a pair of dishonest agents to establish a communication. That is, if agent u can play several actions to signal a bit of information to v, it will choose the best strategy so that v receives this bit. Another difference is that **leaking once** some information is sufficient to be interferent. If user u plays an action a that is observed later on by agent v, then this situation is called an interference, even if this is the only leak in any run of artbitrary size. On the other side, covert channels suppose that any **message of arbitrary size** can be transferred from user u to user v. This supposes an iterated behavior, in which each iteration of channel's use allows to pass some bits of information from one user to another.

Even with these differences, it may seem that systems containing covert channels from u to v are necessarily interferent, in a way or another. We will however show that both notions are **orthogonal issues**, as interference occurs as soon as actions of u and observations of v "coincide" (which is not necessarily a covert channel), and as a covert flow exists as soon as u and v have a strategy to iterate information passing (which is not always an interference).

Information theoretic frameworks have been proposed by Millen [4] for interference, and recently for covert channel [2]. Interference is characterized by a non-null mutual information between u's actions and v's observations and covert flows as a non-null average maximal mutual information between u's actions and v's observations (i.e it is a channel capacity). We will show that even in these very generic frameworks, interference and covert flows remain orhtogonal issues.

Last, we will discuss how covert channels can be seen as games, where a pair of players u, v wins against the system if it succeeds in maximizing the average covert information from u to v in infinite runs. Finding the best possible strategy (i.e. the strategy that maximizes the flow of information) is still an open issue in the field of numerical communications.

Références

1. J.A. Goguen and J. Meseguer. Security policies and security models. In IEEE Computer Society Press, editor, *Proc of IEEE Symposium on Security and Privacy*, pages 11–20, April 1982.
2. L. Hélouët and A. Roumy. Covert channel detection using information theory. In *SECCO 2010, 8th international workshop on security issues in concurrency*, 2001.
3. B. Lampson. A note on the confinement problem. *Communication of the ACM*, 16(10) :613–615, 1973.
4. J. Millen. Covert channel capacity. In *IEEE Symposium on Security and Privacy*, pages 60–66, 1987.