doi:10.1631/FITEE.1601548

题目：一种基于加密哈希的端口地址跳变通信自同步机制

概要：端口地址跳变（Port address hopping, PAH）通信是一种有用的网络动目标防御（Moving target defense, MTD）机制，它受无线通信领域的跳频通信思想启发发展而来。跳变同步是 PAH 通信的一个关键和难点问题，已有机制通常为通信会话提供周期为数秒或数分钟的跳变，且容易受到传输延时、流量拥塞、数据包丢包、乱序和重传等网络事件的影响。为了应对这些问题，在本文中我们提出了一种新的自同步机制，叫做基于加密哈希的自同步（Keyed-hashing based self-synchronization, KHSS）。本文方法基于 HMAC（Hash message authentication code）机制生成消息认证码（MAC），MAC 被进一步用作端口地址编码和解码的同步信息，为端口地址跳变系统提供了一个数据包一次的跳变和隐秘的消息认证功能，使得通过不可靠通信媒介连接的客户端和服务器能够在持续变换它们的通信标识的同时执行消息认证，而且这一过程不需要传输任何同步和认证信息。理论分析、仿真和实验结果表明本文提出的方法能有效防御中间人（man-in-the-middle, MITM）攻击和网络扫描，在安全性和跳变效率方面也明显优于已有方法。

关键词：同步；端口地址跳变；动目标防御；网络安全