

Cryptography ePrint Archive: Report 2011/714

Position-Verification in Multi-Channel Models

Huajun Zhang and Zongyang Zhang and Zhenfu Cao

Abstract: We propose an collusion-attack-resistant position-verification protocol in a new model called multi-channel model. In the multi-channel model, there are lots of communication channels. When a player picks a random channel and sends a short message over it, the message might slip by an adversary with high probability if the adversary does not know the channel beforehand. This idea is motivated from the spread spectrum communication techniques. We adopt it to solve the position-verification task. Adding different constraints into the multi-channel model, we make three sub-models: receiving-constrained multi-channel model, sending-constrained multi-channel model and cover-constrained multi-channel model. Our position-verification protocol is secure under all of these sub-models with appropriate parameters.

Category / Keywords: cryptographic protocols / Multi-channel model, Position-verification

Date: received 1 Jan 2012

Contact author: zhanghuajun.cn@gmail.com

Available formats: [PDF](#) | [BibTeX Citation](#)

Note: Welcome any discussion on this topic.

Version: 20120102:203150 ([All versions of this report](#))

Discussion forum: [Show discussion](#) | [Start new discussion](#)

[[Cryptography ePrint archive](#)]