

安全技术

基于CGA技术的移动IPv6绑定更新安全机制

曹 昉, 杜学绘, 钱雁斌

(解放军信息工程大学电子技术学院, 郑州 450004)

收稿日期 修回日期 网络版发布日期 2008-3-12 接受日期

摘要 为解决移动IPv6路由优化过程当中绑定更新消息的安全问题, 结合返回路径可达协议和CAM协议的优点, 提出一种基于加密生成地址(CGA)技术的绑定更新安全机制。该机制在没有部署PKI的环境下, 利用CGA技术实现了跨信任域的2个节点基于地址的身份认证, 可有效防止攻击者伪造、篡改绑定更新消息, 解决路由优化过程中存在的反射式攻击问题。

关键词 [路由优化](#) [绑定更新](#) [移动IPv6](#) [返回路径可达](#) [加密生成地址](#)

分类号 [TP393.08](#)

DOI:

通讯作者:

作者个人主页: [曹 昉](#); [杜学绘](#); [钱雁斌](#)

扩展功能

本文信息

- ▶ [Supporting info](#)
- ▶ [PDF](#) (90KB)
- ▶ [\[HTML全文\]](#) (0KB)
- ▶ [参考文献\[PDF\]](#)
- ▶ [参考文献](#)

服务与反馈

- ▶ [把本文推荐给朋友](#)
- ▶ [加入我的书架](#)
- ▶ [加入引用管理器](#)
- ▶ [引用本文](#)
- ▶ [Email Alert](#)
- ▶ [文章反馈](#)
- ▶ [浏览反馈信息](#)

相关信息

- ▶ [本刊中 包含“路由优化”的 相关文章](#)
- ▶ 本文作者相关文章
 - [曹 昉, 杜学绘, 钱雁斌](#)