IPv6邻居发现协议的形式化验证

叶新铭, 郝松侠

叶新铭1, 郝松侠2

1(内蒙古大学 计算机学院,内蒙古 呼和浩特 010021)

2(中国科学院 软件中心,北京 100080)

作者简介: 叶新铭(1943－),男,内蒙古海拉尔人,教授,博士生导师,主要研究领域为网络协议形式验证与测试;郝松侠(1978－),女,硕士生,主要研究领域为网络协议形式验证与测试.

联系人: 叶新铭 Phn: +86-471-4992931, E-mail: xmy@imu.edu.cn, http://imu.edu.cn

Abstract

This paper presents the formal verification of properties of neighbor discovery protocol of IPv6 protocol suite using model checking. The protocol is modeled in MSC, whose use is popular in designing and documenting communication protocols. Linear temporal logic is adopted to specify properties of the protocol. The main result of this paper is an automatic method to extract properties from the MSC linearization directly.

摘要

采用模型检查技术,对IPv6的邻居发现协议的属性进行了形式化验证.该协议的模型由目前广泛用于设计和描述通信协议的MSC(message sequence charts)来描述,并通过线性时序逻辑说明该协议的属性.还提出了由MSC模型的线性化自动抽取协议属性的方法.

References:

[1] ITU-T.ITU-T Recommendation Z.120, Message Sequence Chart (MSC), 1999.

[2] Pratt V. Modeling concurrency with partial orders. Int'l Journal of Parallel Programming, 1986,15(1):33-71.

[3] Peled D. Specification and verification of message sequence charts. In: Bolognesi T, Latella D, eds. Proc. of the Formal Methods for Distributed System Development. Pisa: Kluwer Academic Publishers, 2000. 139-154.

[4] Alur R, Peled D, Penczek W. Model-Checking of causality properties. In: Proc. of the Proc. of the 10th Annual IEEE Symp. on Logic in Computer Science. San Diego: IEEE Computer Society Press, 1995. 90-100.

[5] Muscholl A, Peled D, Su Z. Deciding properties for message sequence charts. In: Nivat M, ed. Proc. of the FoSSaCS 1998, LNCS 1378. Berlin: Springer-Verlag, 1998. 226-242.

[6] Alur R, Yannakakis M. Model checking of message sequence charts. In: Baeten JCM, Mauw S, eds. Proc. of the CONCUR'99, Concurrency Theory. LNCS 1664, Berlin: Springer-Verlag, 1999. 114-129.

[7] Narten T, Nordmark E, Simpson W. Neighbor discovery for IP version 6 (IPv6). RFC 2461, 1998.

[8] Kindler E. Safety and liveness properties: A survey. EATCS-BuUetin, 1994,53:268-272.

[9] Deussen PH, Tobies S. Formal test purposes and the validity of test cases. In: Peled DA, Vardi MY, eds. Proc. of the FORTE 2002. LNCS 2529, Berlin: Springer-Verlag, 2002. 114-129.

[10] Holzmann HJ. The model checker spin. IEEE Trans. on Software Engineering, 1997,23(5):279-295.