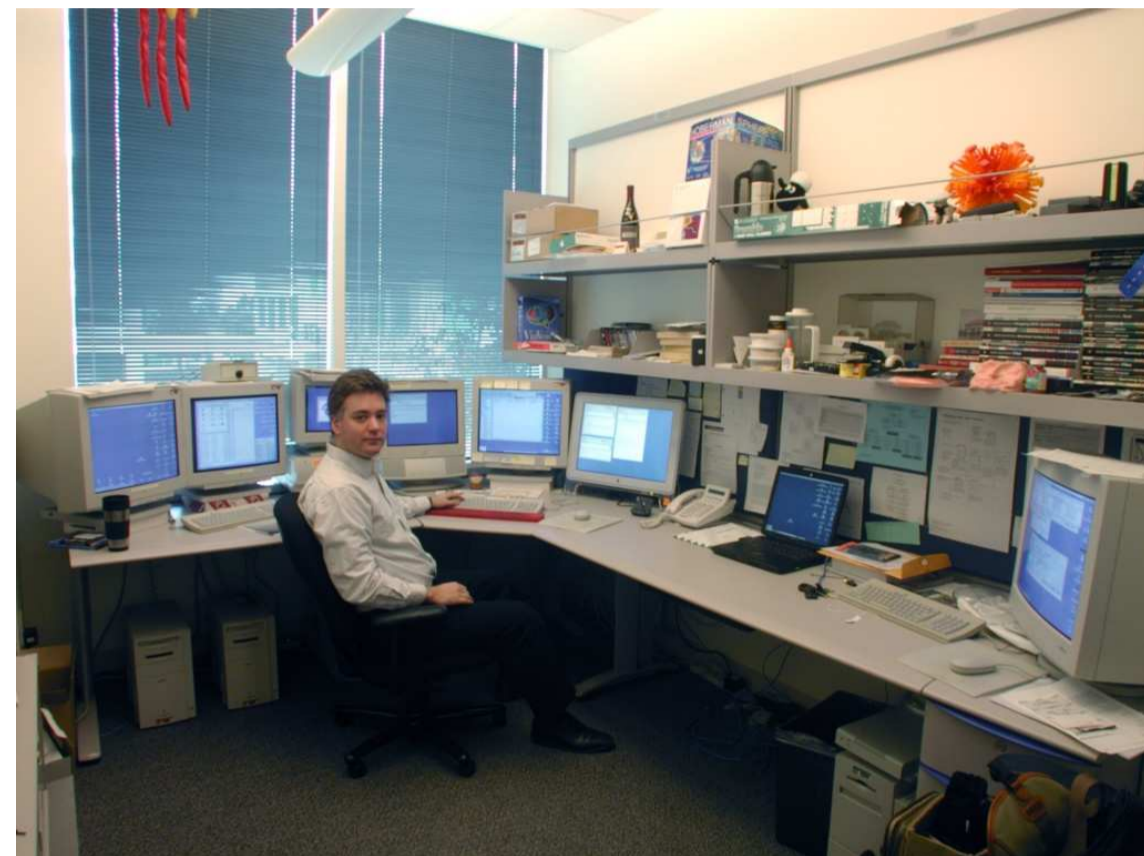


Formal Specification and Analysis of Zeroconf

Background

Zeroconf is a protocol for dynamic configuration of IPv4 link-local addresses, invented by Stuart Cheshire from Apple research and described by the IETF in RFC 3927.



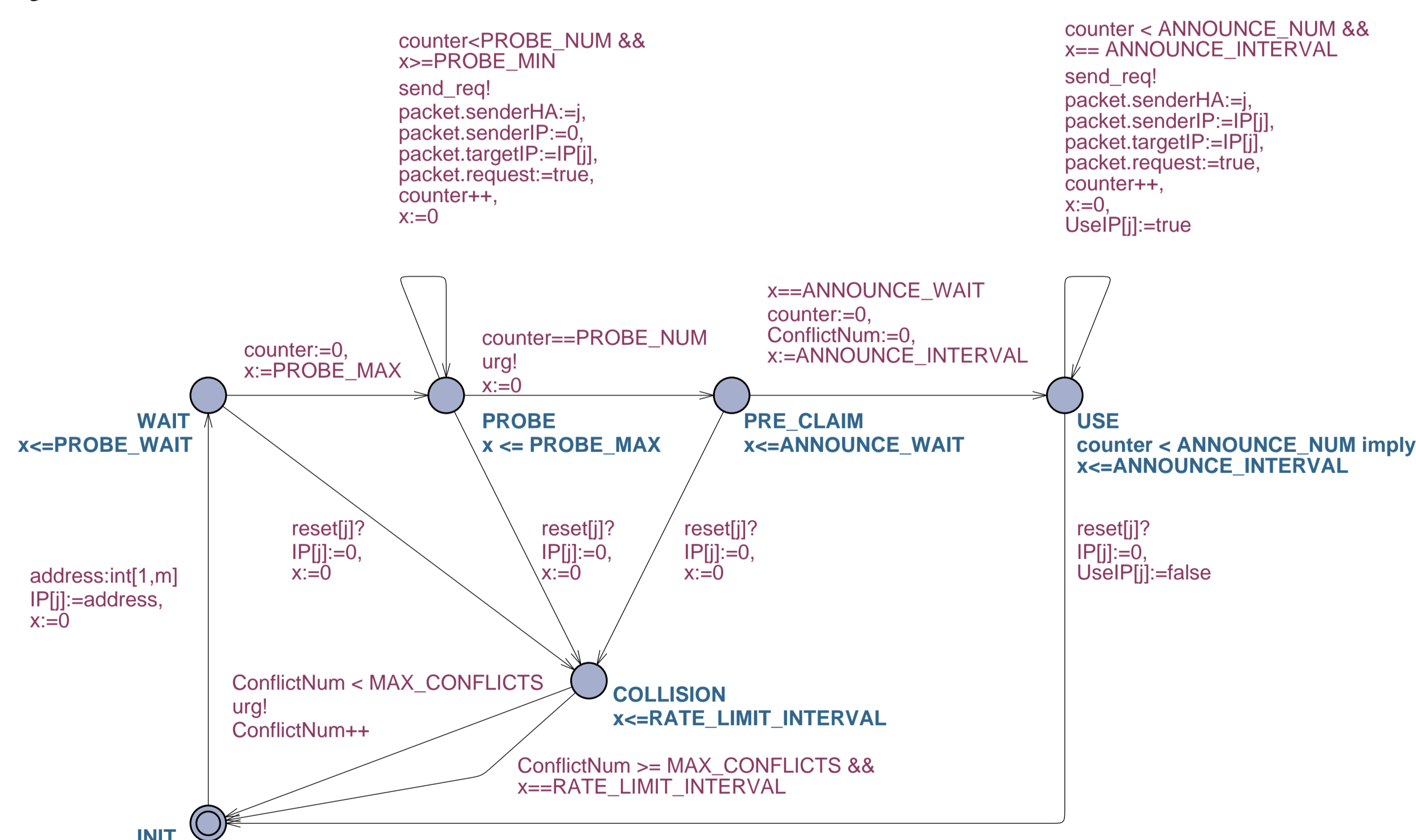
Zeroconf provides a plug-and-play network in which new hosts automatically configure an IPv4 address, without external configuration servers, like DNS.

It is surprising that protocol standards that are of such immense importance to our society are typically written in informal language, with frequent ambiguities, omissions and inconsistencies. They also fail to state what properties are expected of a network running the protocol, and what it means for an implementation to conform to a standard.

Objectives

Our goal has been to construct a model that

1. is easy to understand by engineers,
2. comes as close as possible to the RFC, and
3. may serve as a basis for formal verification.

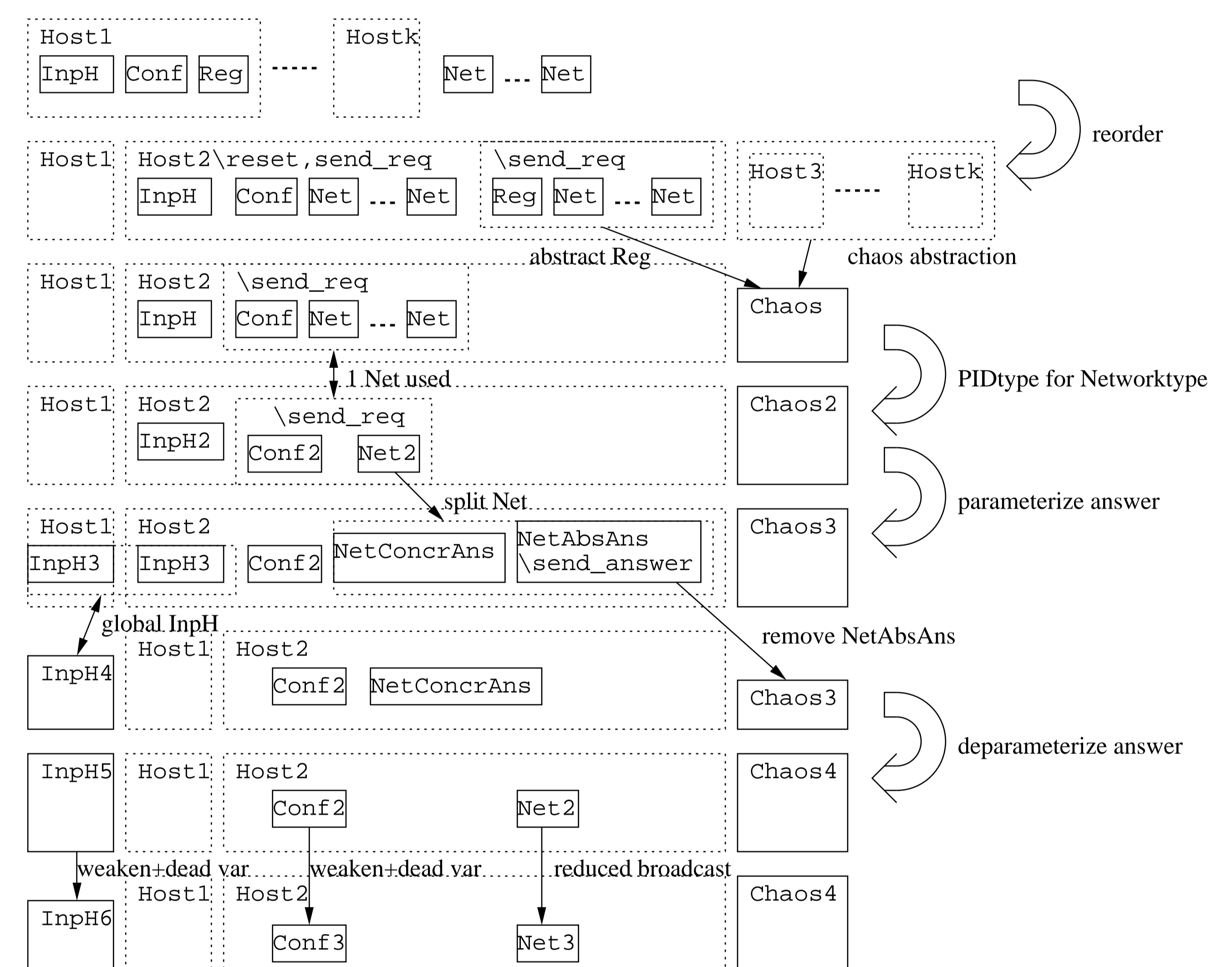


Results

We gave a **formal model** of (a critical part of) Zeroconf that is easy to understand, faithful to the RFC, and with an extensive discussion of the relationship between the model and the RFC.

Our efforts revealed **five errors and ambiguities** in the RFC that no one else spotted before.

We gave **two proofs of mutual exclusion** for Zeroconf (for an arbitrary number of hosts and IP addresses): a manual, operational proof, and a proof that combines model checking with the application of a new compositional abstraction relation. For model checking we used **Uppaal**, and the abstractions have been checked either by hand or by using **Uppaal-Tiga**.



More Information

- <http://www.ita.cs.ru.nl/publications/papers/fvaan/zeroconf/>
- Frits Vaandrager, f.vaandrager@cs.ru.nl
- Jasper Berendsen, j.berendsen@cs.ru.nl

