B.5.1 TRUMP Sender State Diagram

The TRUMP Sender operation goes through three stages. Connection establishment negotiates connection parameters and determines if the receiver is willing to accept connection. Data transmission either transmits a data packet if no acknowledgment packet can be received, or deals with the ack packet. Connection termination occurs on receiver errors, or if all data packets have been received sucessfully.

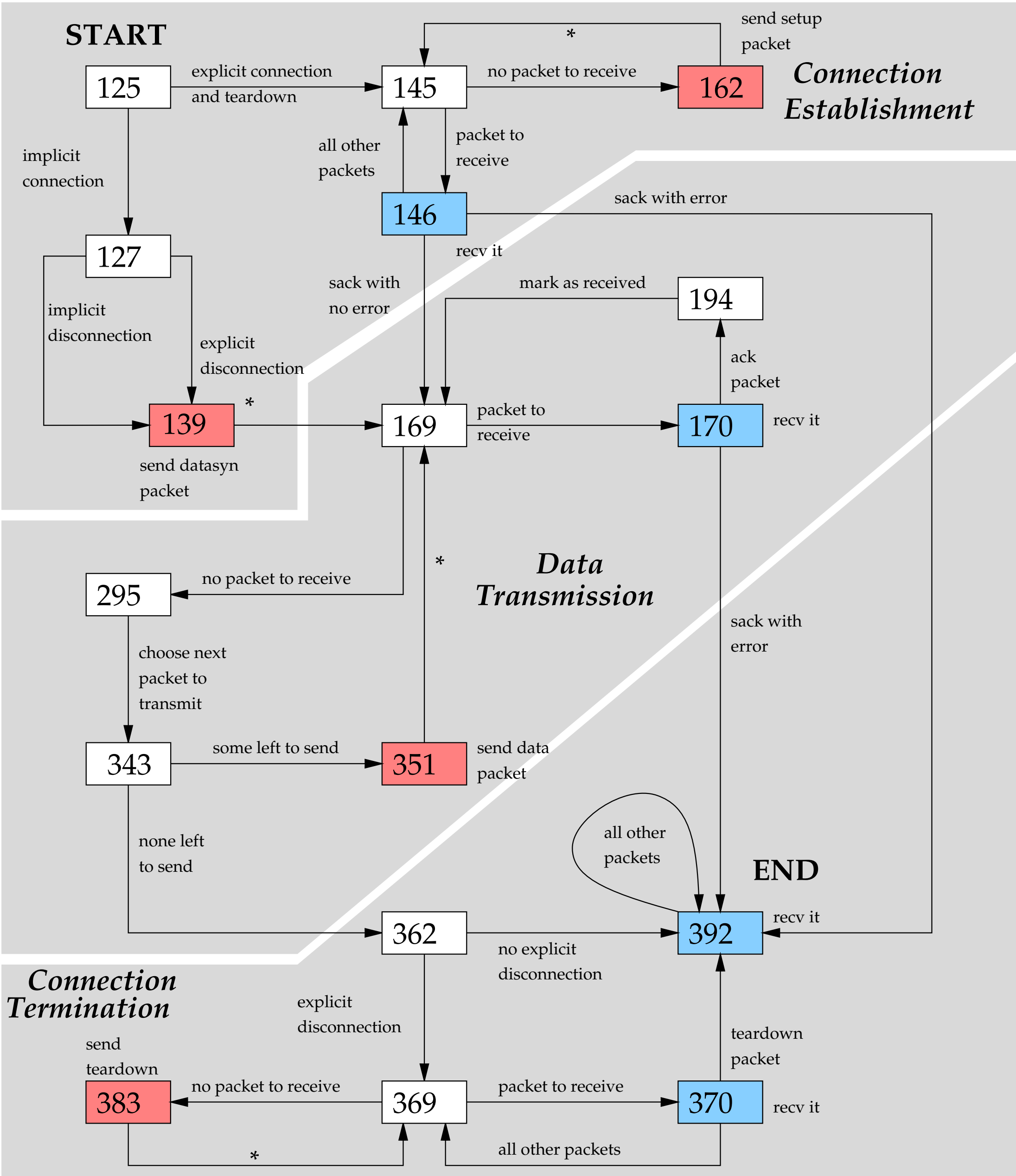

Figure 64: TRUMP Sender State Diagram

B.5.2 TRUMP Receiver State Diagram

The TRUMP Receiver operation also goes through three stages. Connection establishment negotiates connection parameters and determines if the receiver is willing to accept connection. Data reception is controlled by packets from the source (lines 456 and 464), and returns acknowledgment packets. Connection termination occurs when teardown packets are received, and returns teardown packets to the source. A fourth stage of operation, Abnormal Termination, is only used if the receiver wishes to abort the connection at any stage.

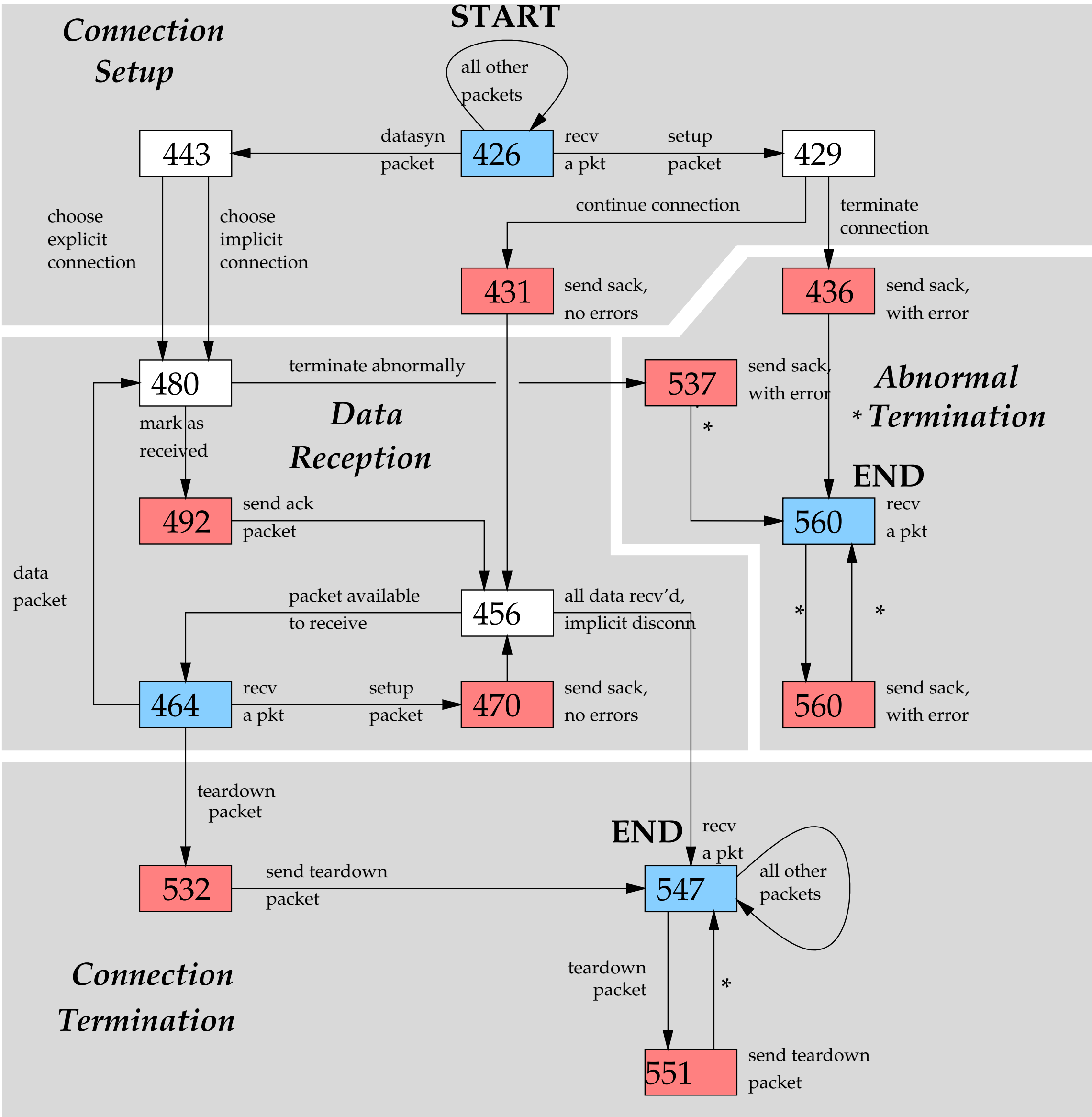

Figure 65: TRUMP Receiver State Diagram

B.6 Verification of TRUMP

A TRUMP protocol, with certain of the available features enabled, is correct if:

- both the Sender and Receiver finish in an 'end' state,
- there are no messages left to be received in any message channel,
- each process has passed through all of its 'progress' states, and
- all assertions have been shown to be true,

ment, the sender must immediately desist transmission of all packets. This arbitrary return of an 'error' acknowledgment increases the size of the state space to approximately 2.6 times that of the equivalent 'no features' protocol; the state size is unchanged. The supertrace method was used for all values of N, showing that TRUMP with arbitrary receiver errors is provably correct after covering $\geq$ 98% of states for N up to 250 data packets.

B.6.4 Implicit Connection Setup

Enabling implicit connection setups and teardown (with the latter selectable by both sender and receiver), the size of each state is approximately twice that with implicit connections disabled. The state space for implicit connections is also approximately 3.5 times that of the equivalent 'no features' protocol. The supertrace method was used for all values of N, showing that TRUMP with implicit connections is provably correct after covering $\geq$ 98% of states for N up to 250 data packets.

B.6.5 Packet Losses

Two of the selectable 'features' in the TRUMP implementation are the enabling of packet reordering on the two links between the sender and receiver, and the enabling of packet loss on these two links. These features do not affect the sender's or receiver's code, but they do affect the protocol's operation. Both options have a tremendous effect on the possible interleavings of the sender, receiver and link states, and so significantly affect the size of the total state space to be verified. With either enabled, TRUMP cannot be verified for large values of N.

The implementation of TRUMP in Promela imposes a limit on the number of packet reorderings and packet losses on a single link. This is set in the 'constants' file at 20 reorderings and 20 losses per link. Even with these small values, the state space is extremely large.

With only packet loss enabled, the state space to be explored is *at least* 330 times that of TRUMP with no packet loss, for equivalent values of N: for example, there are $2.8 * 10^7$ states for N =5 packets. The size of each state is unaffected. Figure 66 shows the range of N vs. packet loss values for which the TRUMP specification in Promela can be verified correct.

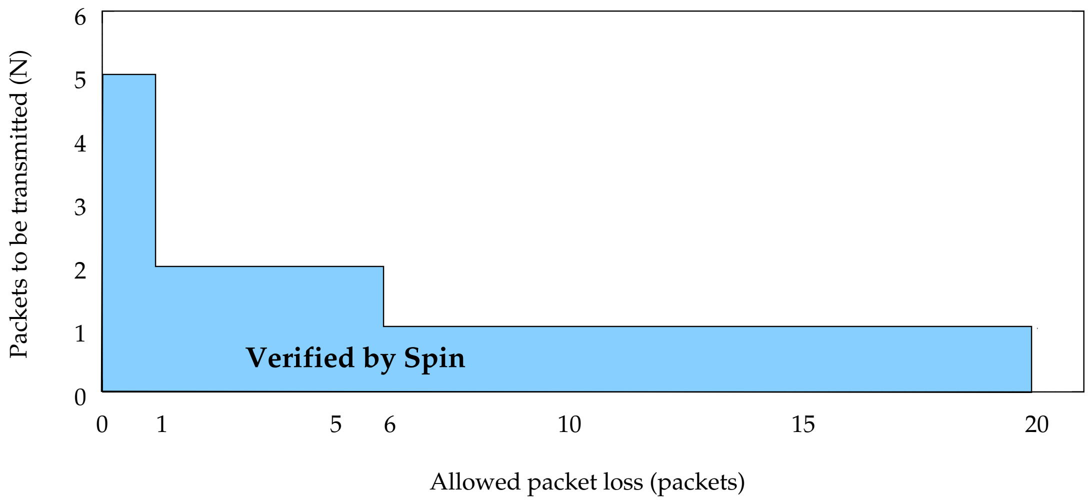

Figure 66: Verification of TRUMP during Packet Loss

B.6.6 Packet Reordering

With only packet reorderings enabled, the state space to be explored is again very much larger than that of TRUMP with no packet loss. The size of each state is unaffected. Figure 67 shows the range of N vs. packet loss values for which the TRUMP specification in Promela can be verified correct.

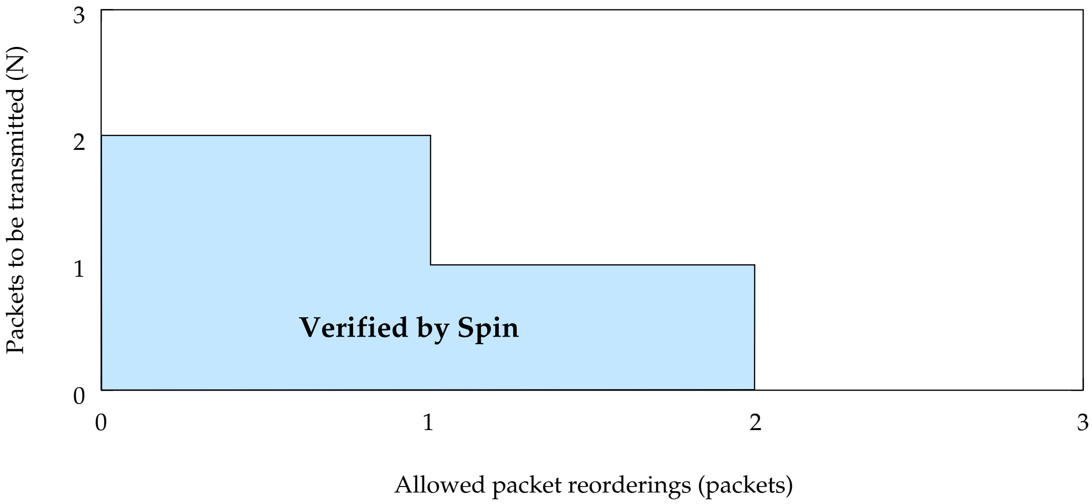

Figure 67: Verification of TRUMP during Packet Reordering

B.7 Summary

The correct operation of a complex transport protocol must be verified; otherwise, severe operational errors may come to light either after an implementation of the protocol, or after the implementation's deployment. In this appendix, we have reviewed the use of the Spin protocol verification tool to prove TRUMP correct where possible.

Due to CPU and memory constraints, Spin was unable to exhaustively prove TRUMP correct. The Promela implementation of the protocol was designed to allow certain TRUMP functionality to be enabled and disabled. With packet loss and packet reordering disabled, the TRUMP protocol was verified with the following features enabled, for up to 250 data packets per connection:

- No other features,
- Selective acknowledgments of size 8,
- Arbitrary receiver errors, and
- Implicit connection setup.

The complexity of the Promela implementation of TRUMP increases dramatically with packet losses or packet reordering enabled. With no features enabled, Spin was able to prove the correctness of the TRUMP protocol for a very small number of packet loss/data packet combinations, and similarly for a very small number of packet reordering/data packet combinations.

Although TRUMP has not been exhaustively verified, it appears to be a robust transport protocol, with no correctness flaws discovered.