Objective of Present Work

Broad outlines of the work:

Specifying the operational behaviour of Network protocols

The first step in the process of describing a protocol’s normal behavior, shown in Fig.1, is to understand its operational context. This can be done during the conception of a new protocol or retrospectively for one that is currently specified. A number of techniques could be used to understand a protocol’s operational context – for example, combinations of modeling, simulation, or observation on test beds or operational networks could be used. The ideal approach is to observe a protocol on an operational network with real usage patterns. However, this may not be possible for technical or organizational reasons.

Fig. 1. The processes involved in specifying the operational behavior of Network protocols

It will be important that a protocol is observed from a number of different viewpoints. A meaningful viewpoint is a point of observation where different protocol operation can be seen if the view is changed. As mentioned in the ARP example earlier, a network’s gateway router under normal conditions generates significantly more request traffic than a standard host, which leads to problems with the dropping mechanism. Here, the viewpoint is the device type and the set of views is the different devices. Other viewpoints could include the time of day, the
topological location of a device, or the underlying link type. An important consideration for this research is to understand what the meaningful viewpoints are. Having gained an understanding of the operational context of a protocol, the next step is to describe it. We envisage that a base specification of a protocol’s behaviour may in the first instance be defined by standardization bodies, for example. The base specification will define the relevant viewpoints and associated views. It will also define the features that make up a view (such as message rate or relevant protocol message fields) that can be used to identify normal behaviour. The base specification may define expected values for features, or describe functions that can be used to determine values. For example, a function could be specified that yields a normal ARP request rate for a network based upon its size. The relationship between viewpoints, views, and features are demonstrated in Fig. 2, with an example for the ARP protocol. It should be possible to tailor a base specification. Organizations may, based upon policies, wish to define local values for different features, or change the set of viewpoints and views in a way that is relevant to their local context. Furthermore, equipment vendors may wish to extend or adjust

Fig. 2. An example set of viewpoints, views, and features for the ARP