

## Detecting Service Violation in Internet and Mobile Ad Hoc Networks

Bharat Bhargava  
CERIAS Security Center and  
Department of Computer Sciences  
Purdue University  
bb@cs.purdue.edu

Networks are vulnerable to attacks from users and malicious hosts.

For internet we present monitoring schemes based on low cost probes that use only edge to edge measurements. These schemes are scalable in large network domains. Stripes and overlay-based schemes are used to infer delay and loss at egress routers and detect congestions and misbehaved flows due to Service Level Agreement (SLA) violations. Experimental study measures overheads, delays, loss ratio, accuracy, and convergence time. Research results provide guidelines that allow in integrating schemes that can deal with intrusions and preserve QoS. Filters at ingress routers are used to block violating flows.

In ad hoc networks malicious attackers can prevent the integrity of the route establishment. The research challenge is to identify and isolate the attackers. The malicious hosts may be included in suspicious lists or blacklists depending upon trust and global information. Experimental studies measure effectiveness, accuracy, overhead and throughput of a Reverse Labeling Restriction (RLR)

Wormhole attacks, authentication, and privacy research will be briefly presented. This talk is based on joint work with A. Habib, Y. Lu, and W. Wang.

More information is available at [www.cs.purdue.edu/people/bb](http://www.cs.purdue.edu/people/bb).