"Current system administrators are missing intrusion alerts hidden by large numbers of false positives. Rather than accumulation more data to identify true alerts, we propose an intrusion detection tool that effectively uses select data to provide a picture of "network health". Our hypothesis is that by utilizing the data available at both the node and cooperative network levels we can create a synoptic picture of the network providing indications of many intrusions or other network issues. Our major contribution is to provide a revolutionary way to analyze node and network data for patterns, dependence, and e?ects that indicate network issues. We collect node and network data, combine and manipulate it, and tease out information about the state
of the network. We present a method based on utilizing the number of packets sent, number of packets received, node reliability, route reliability, and entropy to develop a synoptic picture of the network health in the presence of a sinkhole and a HELLO Flood attacker. This method conserves network throughput and node energy by requiring no additional control messages to be sent between the nodes unless an attacker is suspected. We intend to show that, although the concept of an intrusion detection system is not revolutionary, the method in which we analyze
the data for clues about network intrusion and performance is highly innovative."