# Active Network Defense
# - An Analysis Based on the Configuration and Tests of a Virtual Honeypot System

Yanyan Li, Keyu Jiang
Fort Hays State University

**Abstract**

With the popularity of Internet attacks, new network defense technologies are gradually coming out. This paper explores a new technology named “Honeypot”, which has big difference with the traditional network defense methods, like firewalls or IDS. The traditional methods only protect those known vulnerabilities and block the corresponding attacks. However, honeypot technology initiatively lures the attackers, and track the attacking process, purpose and other relevant information from hacking. After the deep analysis to those information, some unknown system vulnerability may be exposed. Moreover, it can also protect the normal operations of the core equipment from being targeted and affected.

This paper describes the process of building a virtual honeypot system, and then illustrates the invasion test conducted in the research. The test result shows that the virtual honeypot system can be detected by the external environment and also can effectively record the invasion process. This paper discusses the principle on deploying a honeypot and functionality honeypot can provides. Finally, this paper proposes that the honeypot system can be used to study botnet and some more complex network hacking.

*Keywords*: honeypot, attack, network defense, virtual system, invasion, botnet