

Kriangkrai Limthong 2009: Wavelet-Based Detection of Source-Network Packet Flooding. Master of Engineering (Computer Engineering), Major Field: Computer Engineering, Department of Computer Engineering. Thesis Advisor: Associate Professor Pirawat Watanapongse, Ph.D. 94 pages.

In this thesis, we proposed wavelet-based flooding detection method at source of a computer network. We changed the data which received from the computer network to signal that have a relationship between number of packet and time interval. After that, we decomposed the original signal into high frequency part and low frequency part for each level. Moreover, we analyze each level of the composite parts in order to detect anomaly behavior in computer network. If it is not have an abnormality in computer network, we will combine the original signal with normal signal which store in database so as to use for next detection.

In this work, we studied on the standard protocols that using in computer network such as, ICMP, TCP SYN, TCP SYN/ACK and UDP. The interval time in this work is 1 second and we use Haar mother of wavelet to decomposed original signal. The data set, we collected from Kasetsart IT Square laboratory rooms between June and August 2008.

The results from this work indicated that we can use wavelet-based decomposition and analysis of high frequency part and low frequency part in order to detect anomaly at source of computer network. The main of parameters for accurate and precisely detection of source network packet flooding is level of decomposition that use for this detection method.

Student's signature

Thesis Advisor's signature

___ / ___ / ___