SUMMARY OF Ph.D. DISSERTATION

School Graduate School of Science and Technology	Student Identification Number	SURNAME, First name KAWAGUCHI, Nobutaka

Title

Detection of Hit-list Worms based on Propagation Behavior

Abstract

This dissertation presents series of novel worm detection techniques based on worm's propagation behaviors.

Network worms have been one of the major threats against the computer networks. To reduce the damages caused by the worms, fast detection of their existence is essential. Most worms use address-scans to locate victim hosts. So, conventional approaches focus on the activities to detect the worms quickly. Recently, however, a new type worm named hit-list worm is appearing. Instead of address scan, this worms use address lists of vulnerable hosts to locate victims, and therefore it is difficult to detect the existence by conventional approaches.

The objective of this study is to realize the fast detection of hit-list worms that propagate in enterprise networks. Proposed approach focuses on the worm's propagation behavior that makes tree-like structures composed of hosts as nodes and connections as edges. Furthermore, this approach is extended to realize the scalable distributed worm detection.

This doctoral dissertation is organized as follows. Chapter.1 describes the background and objective of this study.

Chapter.2 shows the taxonomy of network worms and existing counter measures.

Chapter.3 proposes a worm detection method named ACTM (Anomaly Connection Tree Method). ACTM detects the worms by tracking tree structures composed by worm's infection connections. By taking the anomaly of each connection into consideration, ACTM can detect the worms quite faster than existing approaches.

Chapter.4 presents a distributed worm detection method based on ACTM. In this method, multiple IDS are deployed in the network. Then, each IDS monitors the network activity of its target host and cooperates to each other to detect hit-list worms in a distributed manner. This approach is scalable since each IDS doesn't require any global knowledge of the network.

Finally, in Chapter.5, the series of studies are summarized and future works are described.

Through the studies, the fast detection method of hit-list worms in a distributed manner is realized by focusing on the worm's propagation behaviors and making multiple IDS cooperate to each others. The result of each study shows the effeteness of proposed approach on both the detection performance and cost.