**ETSJ004 - MODELING AND AUTOMATED CONTAINMENT OF WORMS**

**Abstract** — Self-propagating codes, called worms, such as Code Red, Nimda, and Slammer, have drawn significant attention due to their enormously adverse impact on the Internet. Thus, there is great interest in the research community in modeling the spread of worms and in providing adequate defense mechanisms against them. In this paper, we present a (stochastic) branching process model for characterizing the propagation of Internet worms. The model is developed for uniform scanning worms and then extended to preference scanning worms. This model leads to the development of an automatic worm containment strategy that prevents the spread of a worm beyond its early stage. Specifically, for uniform scanning worms, we are able to determine whether the worm spread will eventually stop. We then extend our results to contain uniform scanning worms. Our automatic worm containment schemes effectively contain both uniform scanning worms and local preference scanning worms, and it is validated through simulations and real trace data to be non-intrusive.