オニオンルーティングにおける経路制御の研究

Study on path control for onion routing

李　岩

Li　Yan

概 要

本文では代表的な匿名通信技術であるオニオンルーティングを対象に，中継ノードの選択制御，および経路の最適化，を目的とした経路制御手法を検討した．具体的には，エニーキャストと最短経路制御を用いた経路制御方式を提案した．ここで，エニーキャストは，マルチキャスト技術を用いて複数ホストのなかから最も近いホストを選択して通信する技術である．また，最短経路制御としてインターネットで広く適用されている OSPF (Open Shortest Path First) の経路制御の仕組みを利用する．次に，従来方式と比較しながら提案方式の性能を接続特性と伝送特性で評価した．接続特性の評価項目は接続可検出時間と接続不可検出時間である．伝送特性の評価項目は送受信ホスト間の伝送遅延時間である．中継ノードは，従来方式ではランダムに１つづつ選択されるのに対して，提案方式では同時に最適に選択されることから，全ての評価項目において提案方式の方が優れていることを明らかにした．

Abstract

The paper highlighted path control of the Onion Routing (OR) that is a typical anonymous communication scheme, and proposes a routing method of OR which enables both best choice of relay nodes and optimization of packet routing paths. To attain the aim, it employed anycast and OSPF (Open Shortest Path First) routing technology. Here, the anycast chooses the nearest host among the candidate hosts joining the onion routing, and the OSPF is widely applied in the Internet. Next, comparing with the conventional OR, the performance on the proposal was evaluated. The evaluation items were connection and transmission performances. The connection performance included connect-able and connect-unable detection times, and transmission performance was transmission delay between the sending and receiving hosts. While the conventional OR chooses the relay nodes randomly and one-by-one, the proposed OR does properly and simultaneously.　The paper demonstrated that the proposed OR is superior to the conventional OR in terms of the every performance.

found that the phishing URL becomes difficult to distinguish and tends to be mistaken for legitimate URL, comparing with the previous study results by McGrath et al. in 2008. We also found that 65% of the phishing pages are on falsified websites, and that in many cases phishers exploit the websites of the light users with inexpensive rental servers. So we proposed a server-side countermeasure using whitelist filtering, which can be easily introduced by website operator. By keeping the whitelist in advance to permit URL access and combining with the black list of the brand name of phishing target, the proposed countermeasure informs the risk to the user while preventing damage to the phishing. We experimented the countermeasure and verified its effectiveness and ease of deployment.