先端科学技術研究科　修士論文要旨

所属研究室 (主指導教員)	情報基盤システム学 (藤川　和利 (教授))		
学籍番号	2411156	提出日	令和 8年 1月 19日
学生氏名	関口　裕香		
論文題目	DoH通信を利用した敵対的攻撃に対する機械学習モデルの頑健性評価		

要旨

DNS over HTTPS (DoH) はプライバシー保護やセキュリティという観点において, サービスプロバイダーとユーザー間で急速に普及している. 一方で, DoH通信は他のHTTPS通信と区別が困難な特性を持つため, DGAマルウェアを始めとした悪性通信の隠蔽にその特性が悪用されることが懸念される. そのため, DoH通信を利用する悪性通信を検知する研究が重要となる. 先行研究は機械学習モデルを用いたDGAマルウェアによる悪性通信の検知のため, 通信の統計的特徴に着目している. しかし, 攻撃者が悪性通信の特徴量を良性通信に似せることで, 悪性通信を良性通信であると誤って判断させる敵対的攻撃を行う可能性がある. 本研究では, 機械学習モデルに敵対的攻撃を行うことを想定し, 機械学習モデルが悪性通信を正しく検知できるか (頑健性) を評価する. 具体的には先行研究で使用されたDoH通信の特徴量をHTTPS通信に似せるために、ドメイン長を操作してクエリサイズを動的に変動させ, 可変パディングと同様のサイズ分散を持たせた. また, それらの異なるクエリに対し, 送信間隔などの転送制御を用いることでデータセット作成を行った.