SCIS 2022 2022 Symposium on
Cryptography and Information Security
Osaka, Japan & Online, Jan. 18 – 21, 2022
The Institute of Electronics,
Information and Communication Engineers

物理的サイバー攻撃検知手法の一検討 －ハードウェアトロイの検知－
A Study on Detection Method for Physical Cyber Attacks -Hardware Trojan Detection-

西田 奏太 * 清水 晶太 * 櫻澤 聡 * 伊澤 真人 *
Kanata Nishida Shota Shimizu Satoru Sakurazawa Masato Izawa

加藤 勇夫 *
Isao Kato

キーワード 伝送線路，ハードウェアトロイ，検知手法

あらまし

昨今，情報漏洩などの意図しない動作を引き起こすハードウェアトロイの脅威が報告されている．その対象はICチップに限らず，伝送線路に対するハードウェアトロイ挿入の可能性も指摘されている [1, 2]．このようなハードウェアトロイは，あらゆる機器に挿入される可能性があるため，低コストの検知手法が求められる．

ハードウェアトロイ挿入を検知する手法として，Time Domain Reflectometry (TDR)により，ハードウェアトロイ挿入に伴う特性インピーダンスの変化を検知する手法や，ネットワークアナライザを用いて計測したSパラメータから線路特性の変化を検知する方法が挙げられる．一方で，これらの手法では高価な専用回路や機器が必要となる．

本研究では，既存手法と同様に，ハードウェアトロイ挿入に伴い伝送線路の物理的特性が変化することを利用した検知手法を提案する．図1に提案手法の概要を示す．提案手法では，伝送線路にテスト信号として正弦波を印加する．ハードウェアトロイが挿入された場合，挿入点において反射信号が発生する．この反射信号とテスト信号の位相差を求めることで，挿入点までの距離を算出する．提案手法では，観測信号と，テスト信号あるいは定常時観測信号から反射信号を生成できるため，方向性結合器などの回路を必要とせず，安価に構成することが可能である．

評価実験では，インピーダンス整合された伝送線路での定常時観測信号を基準として，終端を開放した同軸ケーブルを接続した際の反射信号との位相差から，同軸ケーブルの長さを算出することで，提案手法の実現可能性の確認をしている．加えて，伝送線路へのハードウェアトロイ挿入として，オシロスコープのプローブを接続した際の位相差の変化を観測し，ハードウェアトロイの挿入を検知できる見込みを示している．

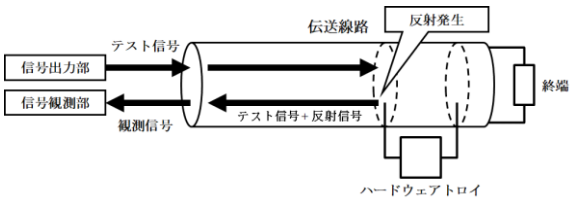

図1 提案手法の概要

今後の課題として，非整合線路への提案手法の適用や検知精度の向上に関する検討が挙げられる．

参考文献

[1] M. Kinugawa, D. Fujimoto, and Y. Hayashi, “Electromagnetic Information Extortion from Electronic Devices Using Interceptor and Its Countermeasure,” IACR Transactions on Cryptographic Hardware and Embedded Systems, vol.2019, issue 4, pp.62-90, 2019.

[2] 西鳥羽 陽，鍛治 秀伍，衣川 昌宏，藤本 大介，林 優一，“オンチップセンサを用いた線路上のハードウェアトロージャン検知に関する基礎検討,” 信学技報，vol.121，no.206，HWS2021-48，pp.38-42，2021.

* 住友電気工業株式会社，〒554-0024 大阪市此花区島屋 1-1-3,
Sumitomo Electric Industries, Ltd.,
1-1-3, Shimaya, Konohana-ku, Osaka, 554-0024, Japan