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 *
Kanata Nishida Shota Shimizu Satoru Sakurazawa

伊澤 真人 * 加藤 勇夫 *
Masato Izawa Isao Kato

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おり，その検知が重要になっている．本研究ではハードウェアトロイ挿入に伴い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．具体的には，線路にテスト信号の正弦波を印加して，その反射信号との位相差からハードウェアトロイ挿入とその挿入位置を検知する．原理確認として同軸ケーブルを例に，終端整合した線路の定常時観測信号を基準に用いて，終端開放した線路を接続した際に発生する反射信号との位相差から線路長を算出する実験を行い，提案手法の実現可能性を確認した．さらに，線路に対する模擬ハードウェアトロイ挿入として，線路にオシロスコープのパッシブプローブを接続した際の位相差変化の観測実験を行い，提案手法によるハードウェアトロイ挿入の検知可能性を確認した．

キーワード 伝送線路，ハードウェアトロイ，検知手法

1. はじめに

Society 5.0の実現に向けて，重要インフラや産業基盤を支える制御システムの重要性が増している．一方で，外部ネットワークとの接続などの高度化に伴い，制御システムに対する脅威が顕在化している[1]-[3]．このような状況において，サイバー空間（仮想空間）とフィジカル空間（現実空間）が高度に融合するSociety 5.0では，サイバー空間でのセキュリティだけでなく，フィジカル空間でのセキュリティも考慮する必要がある．フィジカル空間での脅威として，不正機器の接続や伝送線路の切断（以降，線路と呼ぶ）などが挙げられる[4].

特に，不正機器接続による攻撃手法として，ハードウェアトロイ挿入が考えられる. ハードウェアトロイとは，ICチップなどに挿入され, 情報漏洩などの意図しない動作を引き起こす不正な回路[5]-[9]であるが，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[10, 11]. ハードウェアトロイによる線路からの情報漏洩は，秘密情報の流出に留まらず，IIoT（Industrial Internet of Things）をはじめとする制御機器の不正制御などのより高度な攻撃に悪用される恐れがある．そのため，線路に挿入されたハードウェアトロイの検知が重要となる.

本研究では，ハードウェアトロイ挿入に伴い線路の物理的特性が変化することに着目した検知手法を提案する. ハードウェアトロイが挿入された場合，挿入点の電気特性の変化によりインピーダンスが不整合の状態になるため，交流信号の反射が発生する．提案手法では，線路にテスト信号として正弦波を印加し，テスト信号と反射信号の位相差の変化を観測することで，ハードウェアトロイ挿入を検知する.

以下，第2章では，提案手法について具体的に説明する．第3章では，提案手法の原理確認として，提案手法により線路を測距する実験を行った結果，提案手法の実現可能性を確認したことを示す．第4章では，ハードウェアトロイを模擬して線路へ接続したオシロスコープのパッシブプローブを，提案手法により検知する実験を行

*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

った結果，提案手法によるハードウェアトロイ挿入の検知が可能な見込みを得たことを示す．最後に第 5 章で，まとめと今後の課題を述べる．

2. 正弦波の位相差情報を用いた検知手法

本章では，提案手法である正弦波の位相差情報を用いた検知手法について，概要と具体的な検知処理・手順をそれぞれ 2.1 節と 2.2 節で述べる．

2.1 概要

提案手法の概要について図 1 を用いて説明する．図 1 は，線路の特性インピーダンスに等しい終端抵抗が接続されている場合（整合終端された場合）における，定常時とハードウェアトロイ挿入時の差異を示している．検知用デバイスの信号出力部・信号観測部が対象の線路に接続されているとする．インピーダンス整合されている線路に信号出力部よりテスト信号を印加した場合，反射は発生しない．一方で，ハードウェアトロイが挿入されている場合，線路の特性変化によって反射が発生し，信号観測部ではテスト信号と反射信号が重畳した信号が観測される．テスト信号は既知であるため，観測信号からテスト信号を除去し，反射信号を取り出すことができる．そして，信号解析によりテスト信号と反射信号の位相差を算出する．定常時からの位相差変化により，ハードウェアトロイ挿入を検知することができる．

類似の技術として，Time Domain Reflectometry (TDR)が挙げられる．TDR では反射信号の過渡応答を観測することから，広帯域信号を扱うため，アナログ信号処理部の平坦性が求められる．一方，提案手法は反射信号である交流信号の定常応答を観測することから，狭帯域の信号を使用すればよいという利点がある．

2.2 検知処理・手順

具体的な検知処理内容と手順について説明する．図 1 と同様に，線路は整合終端されているとする．ハードウェアトロイが挿入された場合，テスト信号と反射信号間には位相差 φ が生じる．テスト信号 $y_t(t)$が振幅 A_1，周波数 f，角速度ωの余弦波

$$y_t(t) = A_1 \cos(2\pi f t) = A_1 \cos(\omega t) \tag{1}$$

で表されるとき，反射信号 $y_r(t)$は振幅を A_2 とすると，

$$y_r(t) = A_2 \cos(\omega t + \varphi) \tag{2}$$

で表される．まず，信号観測部で観測される信号 $y_o(t)$は，テスト信号と反射信号が重畳した信号であるため，差分を取ることで反射信号

$$y_r(t) = y_o(t) - y_t(t) = A_2 \cos(\omega t + \varphi) \tag{3}$$

を取り出すことができる．ここで，虚数単位を j とすると，ヒルベルト変換などによってテスト信号と反射信号それぞれの複素解析信号

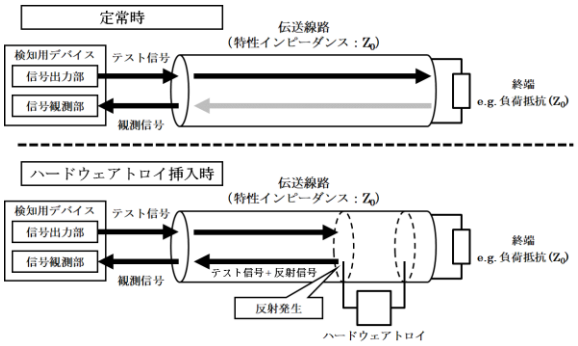

図 1　伝送線路の定常時とトロイ挿入時の差異

$$Y_t(t) = A_1 \cos(\omega t) + j\, A_1 \sin(\omega t) = A_1 e^{j(\omega t)} \tag{4}$$

$$\begin{aligned} Y_r(t) &= A_2 \cos(\omega t + \varphi) + j\, A_2 \sin(\omega t + \varphi) \\ &= A_2 e^{j(\omega t + \varphi)} \end{aligned} \tag{5}$$

を得ることができる．次に，両解析信号の偏角を求めることで，テスト信号と反射信号の位相

$$\theta_{Y_t(t)} = \omega t = Phase\big(y_t(t)\big) \tag{6}$$

$$\theta_{Y_r(t)} = \omega t + \varphi = Phase\big(y_r(t)\big) \tag{7}$$

および位相差

$$\varphi = \theta_{Y_r(t)} - \theta_{Y_t(t)} \tag{8}$$

を算出できる．定常時からの位相差変化を観測することで，ハードウェアトロイ挿入により生じる反射の検知が可能となる．また，光速を c，線路の比誘電率を ε_r とすると，以下の式により，

$$l = \frac{1}{2} \times \frac{\varphi}{2\pi} \times \frac{c}{f\sqrt{\varepsilon_r}} \tag{9}$$

算出した位相差から，反射発生点までの距離を得ることができる．

3. 原理確認実験

本章では，提案手法の原理確認のため行った，提案手法により線路を測距する実験について，実験概要と実験結果，考察をそれぞれ 3.1 節と 3.2 節で述べる．

3.1 実験概要

第 2 章で述べたように，テスト信号と反射信号の位相差を求めることで，反射発生点までの距離を算出できる．本実験ではその原理確認として，初めに整合終端された線路を基準としてテスト信号の印加とその観測を行った（図 3 基準）．次に，終端開放した同軸ケーブルを新たに接続し，観測信号（テスト信号+反射信号）から終端（反射発生点）までの距離を算出した（図 3 ケーブル長測距）．同軸ケーブルの長さに対応した位相差が生じるため，ケーブル長が算出される．

本実験で使用した機材に関して，検知用デバイスを表 1，線路を表 2 に示す．また，実験環境を図 2 に示す．原理確認であり，外部環境の影響を軽減するため，同軸

ケーブル（JIS 1.5D-2V）を使用した．同軸ケーブルの絶縁体はポリエチレンであり，距離算出式（9）の比誘電率 ε_r は 2.3 とした．テスト信号の印加と観測には検知用デバイス上の Digital Analog Converter (DAC)と Analog Digital Converter (ADC)を用いた．DAC と ADC にはそれぞれ 0.2 m の SMA 同軸ケーブルを接続し，各種コネクタによって計測対象である BNC 同軸ケーブルを接続した．ここで，分岐コネクタ-SMA 同軸ケーブル-ADC 間がスタブとなり，反射が発生してしまうため，貫通抵抗器を介して接続した．

実験内容を図 3 に示す．1.06 m と 3.06 m の同軸ケーブルそれぞれに対して，1~10 MHz の正弦波を含んだテスト信号により測距を行った．具体的な手順を以下に示す．

1. 分岐コネクタに終端抵抗を接続し．整合終端した状態で DAC からテスト信号を 1,000 回印加し，ADC で信号を観測した．距離算出では，ここでの観測信号をテスト信号として扱う．
2. 分岐コネクタに計測対象である BNC 同軸ケーブルを接続し．終端を開放した状態でテスト信号を 1,000 回印加し，信号を観測した．
3. 手順 1.と 2.で取得した各観測信号から直流成分を除去した後，2.での観測信号から 1.での観測信号(テスト信号)を減算し，反射信号を算出した．
4. 1,000 個のテスト信号，反射信号をそれぞれ 10 個毎に平均化し，正弦波部を取り出した（図 4）．
5. 4.で抽出したテスト信号と反射信号の正弦波部に対してヒルベルト変換と位相の算出および位相アンラップを行った．
6. テスト信号と反射信号の位相差から距離を算出し，100 個の距離系列データそれぞれに対して前方移動平均を求めた．移動平均のタップ数は，各周波数の 1 波長分とした．

3.2 実験結果

距離算出結果について，算出値の平均とばらつきを表 3 に示す．ばらつきは，標準偏差をσとしたときの 3σを表している．結果として，計測対象の同軸ケーブル長を真値とすると，0.1 ~ 0.3 m 程度，正確度について誤差が生じた．原因の一つは，使用した同軸ケーブルの各周波数での実測のインピーダンスが設計値（50 Ω）から外れていたことが考えられる．そこで，Vector Network Analyzer (VNA) (E5061B)により同軸ケーブルの特性インピーダンスを計測した（図 5）．図 5 に示す同軸ケーブルの周波数特性から，本実験で使用した周波数帯では同軸ケーブルの特性インピーダンスが設計値（50 Ω）から変動し，ケーブル長に応じた位相差を計測できなかった可能性がある．

また，比較対象として，E5061B の Fault Location

表 1　検知用デバイス

ボード	Eclypse Z7* *Zynq-7000 APSoC (XC7Z020-1CLG484C) (667 MHz dual-core Cortex-A9 processor)
DAC	Zmod DAC 1411* *サンプルレート：100 Mega samples per second *分解能：14-bit *出力インピーダンス：50 Ω
ADC	Zmod ADC 1400* *サンプルレート：100 Mega samples per second *分解能：14-bit *入力インピーダンス：1 MΩ

表 2　線路（原理確認）

BNC 同軸ケーブル （計測対象）	JIS 1.5D-2V* *特性インピーダンス：50±2Ω 静電容量：約 100 nF/km
SMA 同軸ケーブル （接続用）	JIS 1.5D-2V* *特性インピーダンス：50±2Ω 静電容量：約 100 nF/km
貫通抵抗器	4391-50* *特性インピーダンス：50 Ω
終端抵抗	BNC-TD* *特性インピーダンス：50 Ω

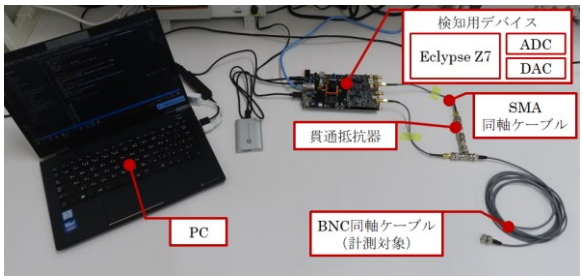

図 2　実験環境（原理確認）

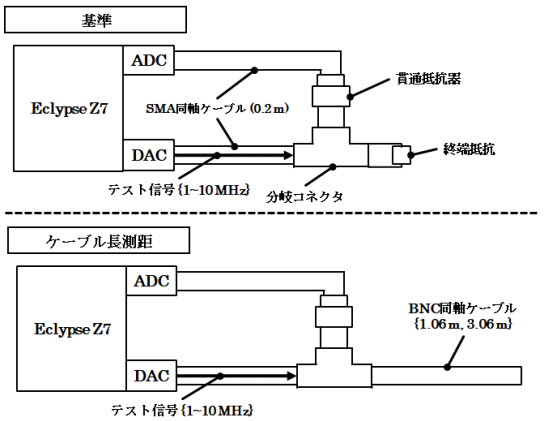

図 3　実験内容（原理確認）

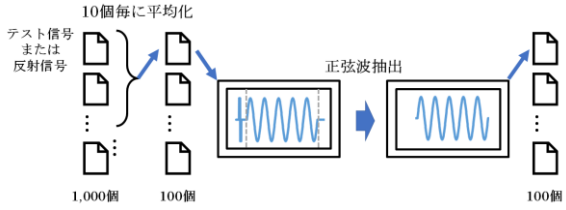

図 4　信号平均化および正弦波抽出処理

表 3　ケーブル長計測実験結果

印加周波数 [MHz]		1	2	3	4	5	6	7	8	9	10
平均値 [m]	1 m	1.148	1.158	1.169	1.183	1.210	1.244	1.271	1.278	1.293	1.297
	3 m	3.242	3.260	3.276	3.287	3.305	3.332	3.340	3.311	3.300	3.285
ばらつき (3σ) [m]	1 m	0.058	0.041	0.033	0.029	0.025	0.025	0.022	0.024	0.019	0.020
	3 m	0.057	0.041	0.031	0.029	0.024	0.023	0.020	0.020	0.017	0.018

Analysis [12]を用いたケーブル長計測結果を表 4 に示す．比誘電率を 2.3 として速度係数を設定し，1 MHz, 10 MHz で計測した．表 4 に示す結果には計測のために接続している各種コネクタ分の長さ（0.1m 程度）も含まれており，実際の結果としては，ケーブル実長に近い値となっていた．加えて，VNA での計測結果に同軸ケーブルの特性インピーダンスによる影響はあまり見られなかった．VNA での計測では校正により測定系が持つ誤差要因を排除しているのに対して，本実験系では計測対象までの測定系の影響を排除できていない．したがって，提案手法の誤差については，同軸ケーブルの特性インピーダンスの変動だけではなく，DAC と分岐コネクタ間，ADC と分岐コネクタ間および分岐コネクタを経由した ADC から DAC までの間の経路上にある何らかの誤差要因が影響していると思われる．

精度については，例として，10 MHz による 1m 同軸ケーブルの測距値の出現頻度を図 6 に示す．図 6 より算出値が正規分布に従うと仮定して，平均値±3σの範囲に約 99.7%の算出値が含まれており，例えば 10 MHz のテスト信号を印加した場合，おおよそ 0.02 m 程度のばらつきで距離を算出できることを表している．

終端を開放した同軸ケーブル接続時の位相差変化の検知は，等価回路の容量成分が支配的になることから，実質的に線路の容量変化を検知しているものとして捉えることができる．表 3 に示すばらつきの 2 倍（±3σ）の値を本実験結果の分解能と仮定すると，計測対象とした同軸ケーブルの静電容量は約 100 nF/km であるため，容量換算すると約 4 pF（10 MHz の場合）の容量変化の検知が可能であると考えられる．そこで，10 pF 程度の容量を持つオシロスコープのパッシブプローブを対象として，提案手法による接続検知実験を行い，ハードウェアトロイ挿入の検知可能性を確認することとした．

4.　挿入検知可能性確認実験

本章では，ハードウェアトロイ挿入の検知可能性を確認するため行った，線路へ接続したオシロスコープのパッシブプローブを，提案手法により検知する実験について，概要と実験結果，考察をそれぞれ 4.1 節と 4.2 節で述べる．

4.1　実験概要

文献[11]で提案されているようなハードウェアトロイの挿入は，線路へのコンデンサと抵抗の挿入とみなすことができる．そこで本実験では，オシロスコープのパッシブプローブを接続することでハードウェアトロイの挿入を模擬し，プローブ接続時の位相差変化を観測することで，検知可能性を確認した．図 7 にプローブ接続前後の線路の等価回路を示す．プローブ装着前の等価回路は，単位長あたりの抵抗，インダクタンス，漏れコンダクタンス，静電容量をそれぞれ R_c, L_c, G_c, C_c とすると，図

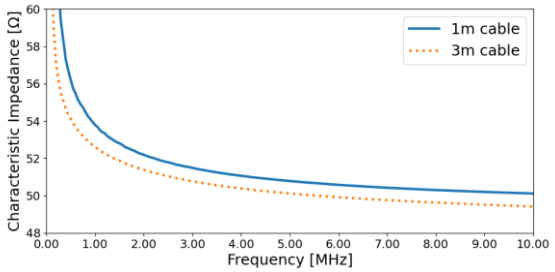

図 5　同軸ケーブルの特性インピーダンス（実測値）

表 4　VNA によるケーブル長計測結果

計測対象 [m]	周波数 [MHz]	結果 [m]
1	1	1.171
	10	1.181
3	1	3.253
	10	3.243

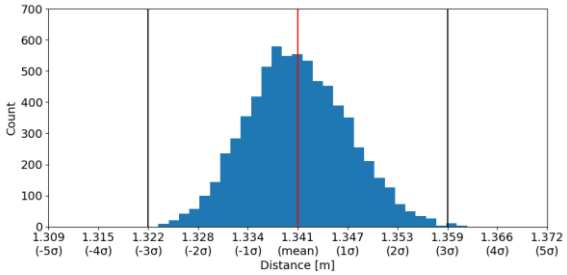

図 6　算出値の分布（10 MHz, 1m 同軸ケーブル）

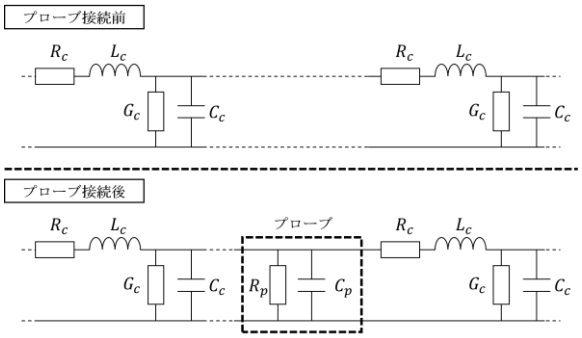

図 7　プローブ接続前後の線路の等価回路

7 上部のように表される．一方で，プローブを装着した場合，プローブ先端の入力抵抗 R_p，入力容量 C_p が線路に付加される．ここで，単位長あたりの抵抗，インダクタンス，漏れコンダクタンス，静電容量がそれぞれ R, L, G, C の線路の特性インピーダンス Z_0 は，

$$Z_0 = \sqrt{\frac{R + j\omega L}{G + j\omega C}} \tag{10}$$

で表され，理想的な無損失線路の場合，

$$Z_0 = \sqrt{\frac{L}{C}} \tag{11}$$

となる．プローブ接続に伴い線路の静電容量が変化すると，インピーダンス不整合点が生じるため，反射が発生する．したがって，プローブ接続前後での位相差変化からプローブの検知が可能となる．

本実験では，プローブの検知可能性の確認として，線路に接続した基板にプローブを接続し，接続前後での位相差変化を観測した．本実験で使用した機材を表 5 と図 8 に示す．表 5 で記載していない機材に関しては，第 3 章での原理確認実験と共通している．また，実験環境と実験内容をそれぞれ図 9 と図 10 に示す．分岐コネクタに校正キットの Load を接続したときの観測信号を基準として，プローブ接続時／非接続時の位相差の違いを確認した．印加する周波数は 1, 5, 10, 20 MHz とした．また，プローブの検知可能性の確認のため，終端は校正キットの Open を接続し，容量成分の変化を検知しやすい終端開放の状態で実験を行った．以下に具体的な手順を示す．

1. 分岐コネクタに校正キットの Load を接続した状態で DAC からテスト信号を 1,000 回印加し，ADC で信号を観測した．
2. 分岐コネクタに SMA 同軸ケーブルとプローブ接続用基板および校正キットを接続し，プローブ接続／非接続それぞれの条件でテスト信号を 1,000 回印加して観測信号を得た．
3. 各観測信号から直流成分を除去した後，2.で取得した各観測信号の位相と 1.で取得した各観測信号の位相を求め，位相アンラップの後，位相差を算出した．
4. 算出した位相差を印加周波数に応じた 1 波長分の点数毎に平均化し，正弦波 1 波長分に対する位相差を求めた．

4.2 実験結果

プローブ接続による位相差の変化を図 11 に示す．プローブ有無それぞれについて，算出した位相差の出現頻度を示している．周波数が高くなるにつれて，プローブ

表 5 実験機材（検知可能性確認）

オシロスコープ	EXR204A
プローブ	N2873A* *入力抵抗：10 MΩ 入力容量：9.5 pF
校正キット	85033E

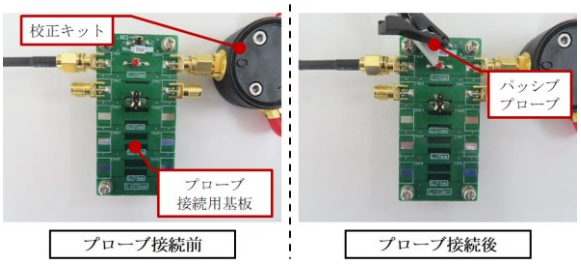

図 8 プローブ接続用基板

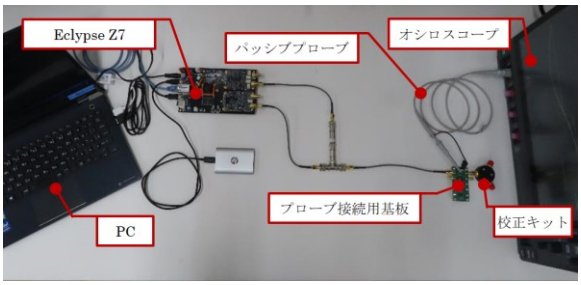

図 9 実験環境（検知可能性確認）

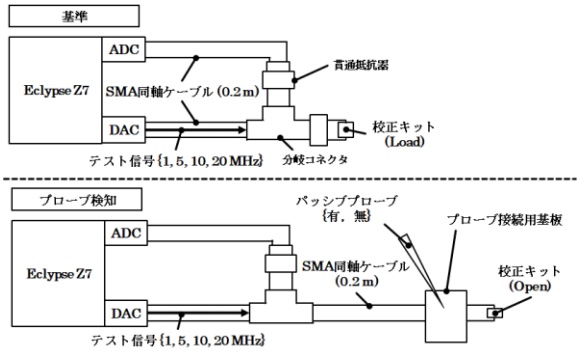

図 10 実験内容（検知可能性確認）

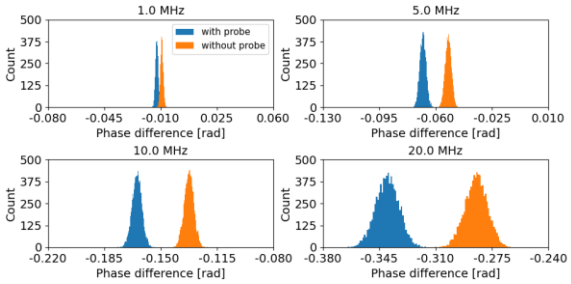

図 11 プローブ接続による位相差変化（終端開放）

接続時の分布と非接続時の分布が分離していくことが確認できた．周波数を高くすると，容量成分の影響を受けやすくなり，プローブ接続による容量挿入を捉えやすくなったと考えられる．一方で，分布の幅も広がった．これは，DAC と ADC のサンプルレートが 100 MS/s であ

るため，正弦波 1 波長を少ない点数で表すことになり，位相の分解能が低くなることが影響したと考えられる．

以上の結果より，提案手法は線路が終端開放されている場合，9.5 pF（プローブの入力容量）程度の容量が挿入されたことを検知可能であると考えられ，ハードウェアトロイ挿入の検知可能性があると考えられる．なお，本実験ではプローブ接続用基板を介して検知対象のプローブを接続したが，ハードウェアトロイ挿入では線路の外部導体の切断が必要であるため，今後はその影響についても検討する必要がある．

5. まとめ

本研究では，印加したテスト信号とその反射信号の位相差から線路へのハードウェアトロイ挿入を検知する手法を提案した．評価実験では，観測した位相差から線路長の算出を行い，容量換算して 5 pF 程度の分解能を持つ見込みがあることを確認した．また，線路にハードウェアトロイ挿入を模擬したオシロスコープのパッシブプローブ（9.5 pF）を接続し，提案手法による検知を行った．実験結果より，プローブ挿入検知が可能であることを示した．

今後は，検知精度の向上や整合線路および非整合線路への本提案手法の適用について検討する予定である．

参考文献

[1] 独立行政法人 情報処理推進機構（IPA），“制御システムのセキュリティリスク分析ガイド補足資料:「制御システム関連のサイバーインシデント事例」シリーズ，”
https://www.ipa.go.jp/security/controlsystem/incident.html, (Accessed: 2021-12-28).

[2] Federal Office for Information Security, “Industrial Control System Security Top 10 Threats and Countermeasures 2019,” BSI-CS 005E, version 1.30, 2019.
https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/BSI-CS/BSI-CS_005E.pdf?__blob=publicationFile&v=1,
(Accessed: 2021-12-28).

[3] 宮地利雄，“制御システムに対するセキュリティ脅威の動向，” 計測と制御, vol.58, no.12, pp.912–915, 2019.

[4] 独立行政法人 情報処理推進機構（IPA），“制御システムのセキュリティリスク分析ガイド 第 2 版，” 2020.
https://www.ipa.go.jp/files/000080712.pdf,
(Accessed: 2021-12-28).

[5] S. Adee, “The Hunt For The Kill Switch,” IEEE Spectrum, vol.45, issue 5, pp.34–39, 2008.

[6] R. S. Chakraborty, S. Narasimhan, and S. Bhunia, “Hardware Trojan: Threats and emerging solutions,” 2009 IEEE International High Level Design Validation and Test Workshop, pp.166–171, 2009.

[7] M. Tehranipoor and F. Koushanfar, “A Survey of Hardware Trojan Taxonomy and Detection,” IEEE Design & Test of Computers, vol.27, issue 1, pp.10–25, 2010.

[8] S. Bhunia, M. S. Hsiao, M. Banga, and S. Narasimhan, “Hardware Trojan Attacks: Threat Analysis and Countermeasures,” Proceedings of the IEEE, vol.102, issue 8, pp.1229–1247, 2014.

[9] J. Francq and F. Frick, “Introduction to hardware Trojan detection methods,” 2015 Design, Automation & Test in Europe Conference & Exhibition (DATE), pp.770–775, 2015.

[10] S. Wakabayashi, S. Maruyama, T. Mori, S. Goto, M. Kinugawa, and Y. Hayashi, “A Feasibility Study of Radio-frequency Retroreflector Attack,” 12th USENIX Workshop on Offensive Technologies, 2018.

[11] 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.

[12] Keysight Technologies,
https://ena.support.keysight.com/e5061b/manuals/webhelp/eng/measurement_with_options/option_010_time_domain_fault_location_analysis/fault_location_analysis/fault_location_analysis.htm,
(Accessed: 2021-12-28).