L-011

物理構成可視化方式に関する検討

Study on Method of Visualization for Physical Network Structure

越出和磨† 坂崎尚生†
Kazuma Koshide Hisao Sakazaki

1. はじめに

鉄道、水道、電力、ガスなどの社会インフラを支える制御システムは、ネットワークや装置への汎用技術の組込みや、情報システムとの接続の増加に伴い、情報システムと同様のセキュリティ対策が求められてきている。近年、制御システムを狙ったサイバー攻撃が主に海外で発生しており、今後、日本においても制御システムを狙ったサイバー攻撃が増加すると予想される。

制御システムのセキュリティ確保には、サイバー攻撃を未然に防ぐための事前対処と、サイバー攻撃発生後の迅速な対処である事後対処の両者を実施する必要があり、意思決定プロセスである OODA(Observe, Orient, Decide, Act)ループによる迅速なハンドリングが効果的である[6]。

近年では、外部のセキュリティ機関等にから脆弱性情報及び対策方法が広く配信されるようになり、Observe フェーズが比較的実施しやすくなってきているが、多くの制御システムでは、物理的な機器構成までは把握できておらず、例え制御システム内で脆弱性が発見されても目的機器が実際にどこに配置されているのかを特定することができない場合がある。

そこで、本稿では、OODA ループの対策実施の役割を担う Act フェーズにおいて、“制御システム内で発生したセキュリティインシデント等の対処位置の把握”を目的とし、稼働中の制御システムへの影響を抑えつつ、物理的なシステム構成を可視化する技術を提案する。

本論文の構成は次の通りである。2 章では、関連研究の紹介と従来技術の課題を説明する。3 章では、物理構成可視化手法を提案し、4 章にて提案手法における実験結果を報告する。

2. 関連研究

ネットワークトポロジー検出に関して多くの関連研究が存在する。Nowicki らは、スイッチにエージェントを配置し、エージェント間で通信を観察することで、トポロジを検出するアルゴリズムを提案している[1]。深見らは、主に通信キャリアが提供するネットワークサービスの保守を目的とし、ネットワーク構成を統一したスキーマで保持することにより、ネットワークの種別が追加されてもを構成把握が容易となる手法を提案している[2]。Flathagen らは、LLDP(Link Layer Discovery Protocol)を用いてスイッチ間のトポロジを検出する手法を提案している[3]。また、中村らは、ネットワーク内の送受信トラフィック量を比較することで、各 IF の接続関係を推定する方法を提案している[4]。また、高田らは、故障が発生した際に装置が発生する警報情報を用いて装置間のトポロジを検出する方法を提案している[5]。

しかしながら、既存方式の多くでは、必要なデータを取得する際の時刻に依存する場合が多く、タイムスタンプのズレが生じた場合、正しく物理構成を把握できない場合がある。また、一般的な時刻同期プロトコルである NTP(Network Time Protocol)で保障される精度は 1ms～100ms 程度であり、それよりも短い単位での時刻同期が必要な場合、適用が困難となる。

また、トラフィックデータや LLDP データ、MAC アドレステーブルデータ等、分析に必要な情報を取得できない装置も存在し、その様な仕様の装置を利用しているシステムでは、既存方式を適用することができない。

本研究では、上記状況に鑑み、以下の 2 点を特徴とする物理構成可視化手法を提案する。

(1) 装置間の時刻同期を必要としない。
(2) トラフィックデータや LLDP データ、MAC アドレステーブルデータ等、装置の仕様により取得可否が分かれるようなデータを用いない。

3. 物理構成可視化手法

一般的にネットワークは、レイヤ 1 及びレイヤ 2 の中継機器(リピータ HUB、スイッチング HUB 等)で構成された LAN 内のネットワークと、L3 の中継機器(ルーター等)を用いて構成される LAN 外のネットワークに分けることができる。LAN 外の中継機器間の接続関係は、traceroute や、L3 中継機器が所有する OSPF(Open Shortest Path First)のデータベースを用いて導出することができるが、LAN 内の接続関係を導出することは難しい。

制御システムでは、一つの建屋内に、プラント設備やコントローラ、情報機器が設置されており、大きな機器であるなら、物理的な位置を把握しやすいが、小規模な機器や端末の様な物の場合、建屋内の何処に存在しているのか、物理的な位置を把握することが困難な場合がある。また、一つの建屋を単位として LAN が構成されている場合、ある機器に脆弱性が発見されても、該当機器の設置場所が把握できず、物理的な対処が遅れる場合が生じる。

本研究では、上記状況に鑑み、制御システムにおける LAN 単位での物理構成可視化を提案する。尚、本研究は有線接続されたネットワークを対象とする。

3.1 提案手法のラフスケッチ

提案手法では、まず、LAN 内に存在する全ての中継機器(リピータ HUB、スイッチング HUB)に、ping 送受信を行う探査用の機器(以降、探査機と称する)を 1 台ずつ設置する。そして、各探査機を用いて、LAN 内の各構成機器及び自身以外の探査機に対して ping 送受信を行い、ping パケットを送信してから応答が返ってくるまでの時間である RTT(Round Trip Time)を計測する。

RTT は、物理的な距離(中継機器を挟むホップ数)に依存するので、RTT の時間差より、機器間の接続関係を分析し、LAN 内の物理的な機器構成を導出する。

†株式会社日立製作所 研究開発グループ
システムイノベーションセンタ
Hitachi, Ltd., Research & Development Group,
Center for Technology Innovation - Systems Engineering.

Copyright © 2021 by
The Institute of Electronics, Information and Communication Engineers and
Information Processing Society of Japan All rights reserved.

より具体的には、最小の RTT となる機器間に接続関係があるとし(図 1 参照)、全組合せ分の RTT を分析することによって全体のトポロジーを導出する。

また、中継機器に探査機を設置する際、探査機の物理的位置(例えば、建屋の何階のどの部屋)を記録し、その探査機と接続されている中継機器およびその中継機器に接続されている各構成機器を、探査機と同じ場所にあるものとして管理端末に表示する。もちろん中継機器から必要以上に長い LAN ケーブルで接続されている場合、実際の設置場所と異なることになるが、LAN ケーブルを辿ることにより、目的機器を見つけることができる。

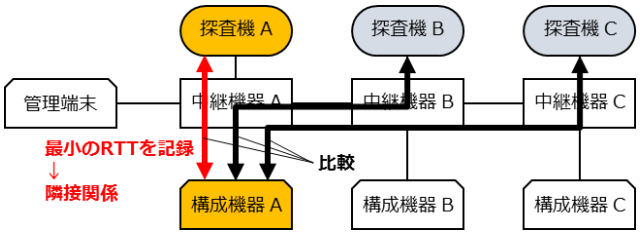


図 1　RTT 比較

尚、LAN 内の中継機器が全てスイッチング HUB であったならば、ping パケットの通過経路を分析することで機器構成を導出することも可能であるが、リピータ HUB が挟まると、リピータ HUB は、不要なポートにも ping パケットを複製し転送する為、機器構成によっては、通過経路から物理構成を導出することができなくなる。

それ故、本研究では、RTT に注目し、機器構成可視化を検討した。提案方式では、RTT の計測だけで分析する為、機器間の時刻同期が必要ない。また、中継機器の機能(MAC アドレステーブル参照の可否等)にも依存せず、ping 送受信のみで物理構成を導出することができる。

3.2 RTT による物理構成導出方法

提案方式は、全探査機を管理端末から遠隔操作し、機器間の全組合せの RTT を計測・分析して物理構成を導出する(図 1 参照)。尚、RTT は、物理的な経路(特に中継機器のホップ数)と、送信/応答端末の処理速度の影響を受ける。故に本稿では、送信端末αから応答端末βへの$\mathrm{RTT}_{\alpha\beta}$を簡易的に式(1)で表し、検討した。

$$\mathrm{RTT}_{\alpha\beta} = X_{send_\alpha} + X_{res_\beta} + 2\left(\sum_{r \in \mathrm{R}_{\alpha\beta}} T_r\right) + 2\left(\sum_{s \in \mathrm{S}_{\alpha\beta}} T_s\right) \quad \cdots (1)$$

X_{send_α} ：送信側の端末αの処理時間
X_{res_β} ：応答側の端末βの処理時間
$\mathrm{R}_{\alpha\beta}$ ：$\alpha\beta$間の経路上に存在する L1 中継機器の集合
$\mathrm{S}_{\alpha\beta}$ ：$\alpha\beta$間の経路上に存在する L2 中継機器の集合
T_r ：L1 中継機器rの経由に掛かる時間
T_s ：L2 中継機器sの経由に掛かる時間

式(1)でのX_{send}の値は、ping パケットの送信機器である探査機毎の処理能力(スペック)に依存する。そこで提案方式では、全探査機のスペックを統一した上で実施する。これによりX_{send}の機器毎の差異を抑える。また提案方式では、RTT データを分析する際、異なる探査機から同一の応答端末に対する RTT 同士を比較する。これによりX_{res}の機器毎の差異を抑える。即ち、比較する RTT データ同士では、式(1)におけるX_{send}及びX_{res}を定数と見なすことができる。以上から、RTT の大小関係は、経路上の各中継機器を往復する処理時間のみに依存すると仮定できる。そして、応答端末に直接接続されている中継機器は、どの探査機からの経路にも必ず存在する。例えば図 1 において、応答端末を構成機器 A とすると、中継機器 A は、探査機 A, B, C からのどの経路にも存在していることが分かる。即ち、RTT は、必ず中継機器 A を往復する時間以上になると言える。したがって、構成機器 A に直接接続されている(正確には、中継機器 A を介して接続されている)探査機 A からの RTT が最小となり、最小の RTT を見つけることにより、中継機器との接続関係を導出することができる。

この様に提案方式では、探査機とその探査機が接続されている中継機器を同一視し、同一応答端末に対する最小の RTT となる探査機(中継機器)を接続関係とすることで、LAN 内の物理構成を可視化する。

尚、測定において、RTT にはノイズが含まれるため、提案方式では、50 回計測した平均値を比較対象とした。

3.3 物理構成可視化アルゴリズムの詳細

具体的な手順を説明する。提案方式は、大きく a. 事前準備フェーズ、b. RTT 計測フェーズ、b. 分析フェーズ、d. 可視化フェーズの 4 つのフェーズから成る。

【a. 事前準備フェーズ】
a.1. 管理端末を対象の LAN に設置する。
a.2. 全中継機器に一つずつ探査機を接続する。探査機の物理的位置を記録する。
a.3. 管理端末、探査機、L2 中継機器であることを識別する為に、それらの機器の IP アドレスを記録する。
a.4. 管理端末から LAN 内に存在可能な IP アドレスに対して ARP 要求を送信し、ARP 応答した IP アドレスを記録する。その際、a.3 で記録した IP アドレス以外を可視化対象の構成機器とする。

【b. RTT 計測フェーズ】
b.1. 管理端末からの遠隔操作により、ある探査機から自身以外の全機器(IP アドレス)に対して、ping パケットを n＝50 回送信し、RTT を計測する。
b.2. 応答端末毎に RTT の平均値を計算し、管理端末に送信する。
b.3. RTT の計測・集計(b.1 及び b.2 の処理)を全探査機から実施する。尚、参考までに図 2 は、送信機器(192.168.0.9)から応答機器(192.168.0.1)への RTT データであり、50 回の平均が 0.579ms であることを示している。また、RTT 差異の顕著化を図るため、ここではパケットサイズを 1028byte に設定している。

【c. 分析フェーズ】
c.1. 応答端末毎に RTT 平均値を比較し、最小の RTT 平均値を記録した探査機(中継機器)を接続関係とする(図 1 参照)。

Copyright © 2021 by
The Institute of Electronics, Information and Communication Engineers and
Information Processing Society of Japan All rights reserved.

c.2. 接続関係のある機器同士を纏めてグルーピングする。

c.3. グループが複数存在する場合、あるグループに属する探査機群から別グループの探査機群に対して RTT 平均値を比較し、グループ間を跨りつつ RTT 平均値が最小となる探査機同士がグループ間をつなぐ接続関係とする。例えば、図 3 の様に 2 つのグループに分かれた場合、赤線矢印の RTT 平均値を比較し、最小値を示す探査機同士を、グループ間をつなぐ接続関係とする。尚、3 つ以上のグループに分かれた場合も同様にグループの組合せ分だけ RTT 平均値を比較し、最小値を示す探査機同士を、グループ間をつなぐ接続関係とすることで、最終的に一つに繋がった構成を導きだすことができる。

【d. 可視化フェーズ】

d.1. ある探査機と接続関係のある構成機器を線で結び、描写する。また、それら構成機器の物理的位置を、その探査機の物理的位置情報として表示する。

d.2. 探査機と HUB を同一視し、探査機同士の接続関係を線で結び描写する。

図 4 左側は、接続関係を描写した例である。立方体が HUB を表し、その HUB に接続している構成機器を線でつないでいる。また接続関係のある HUB 同士も線でつなぎ描写した例である。右側は、表として構成機器の物理的位置(フロア、詳細情報)を接続探査機の物理的位置情報として表示した例である。

```
192.168.0.9
PING 192.168.0.1 (192.168.0.1) 1000(1028) bytes of data
64 bytes from 192.168.0.1: icmp_seq=1 ttl=64 time=0.588 ms
64 bytes from 192.168.0.1: icmp_seq=2 ttl=64 time=0.593 ms
64 bytes from 192.168.0.1: icmp_seq=3 ttl=64 time=0.568 ms
64 bytes from 192.168.0.1: icmp_seq=4 ttl=64 time=0.573 ms
                    ⋮
64 bytes from 192.168.0.1: icmp_seq=49 ttl=64 time=0.553 ms
64 bytes from 192.168.0.1: icmp_seq=50 ttl=64 time=0.581 ms

--- 198.168.0.1 ping statistics ---
50 packets transmitted, 100 received, 0% packet loss, time 50000ms
rtt min/avg/max/mdev = 0.553/0.579/0.593/0.030 ms
```

図 2　RTT データ例

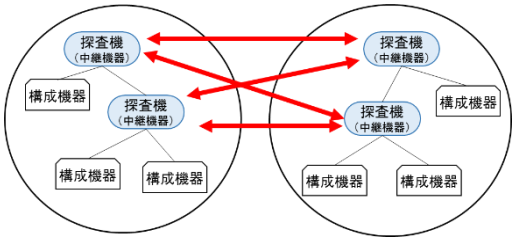
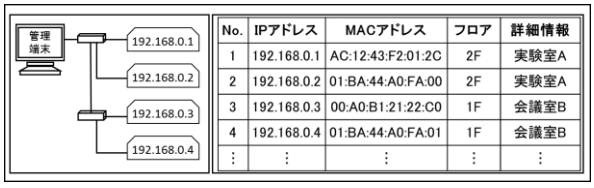


図 3　グループ間の接続関係導出



No.	IPアドレス	MACアドレス	フロア	詳細情報
1	192.168.0.1	AC:12:43:F2:01:2C	2F	実験室A
2	192.168.0.2	01:BA:44:A0:FA:00	2F	実験室A
3	192.168.0.3	00:A0:B1:21:22:C0	1F	会議室B
4	192.168.0.4	01:BA:44:A0:FA:01	1F	会議室B
⋮	⋮	⋮	⋮	⋮

図 4　可視化の例

4. 提案手法における実験結果

提案方式における物理構成可視化の実現性を検証すべく、実験環境を構築し、評価実験を行った。実験環境では、管理端末 1 台、スイッチング HUB3 台、リピータ HUB2 台、構成機器(可視化対象)5 台を図 5 の様に接続し、また、各 HUB には探査機をそれぞれ設置した。

尚、探査機は、全ての HUB に設置することを考慮し、安価で実装できるようにシングルボードコンピュータを用いることにした。実環境に提案手法を適用する際、探査機を必要台数分用意する必要があるが、これにより、比較的費用を抑えることができる。

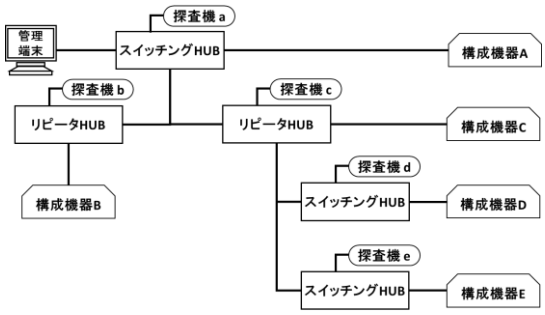


図 5　実験環境

表 1 は、送信側の探査機を列に、応答側の機器(構成機器及び探査機)を行にした、RTT 平均値の一覧表である。行毎に見て、水色部分(太字部分)が、ある応答端末に対する最小の RTT 平均値であり、列から、当該最小 RTT 平均値を計測した探査機を確認できる。即ち、水色部分(太字部分)の行(応答側の機器)及び列(探査機)が接続関係を示している。尚、応答側が探査機の場合(表 1 の下 5 行)、水色部分の接続関係同士だけを結ぶと、探査機 a,b,c のグループと探査機 d,e のグループに分離することが分かる。この場合、a,b,c グループに属する探査機と d,e グループに属する探査機間で、RTT 平均値を比較し、グループ間を跨りつつ RTT 平均値が最小となる探査機同士をグループ間をつなぐ接続関係とする。この例の場合、探査機 c と d がグループ間の接続関係を示している。図 6 は、構成機器 A に対して各探査機が 50 回計測した RTT、及びその平均値を示すグラフである。縦軸が RTT[ms]、横軸が回数[times]であり、計測された RTT がプロットされ、平均値(avg)が直線で示されている。グラフから、探査機 a が計測した RTT 平均値である a_avg が最小となることが分かる。

続いて、実際にプロトタイプシステムを用いて図 5 の環境を可視化した結果を図 7 及び図 8 に示す。尚、管理端末の接続箇所は自明であるため、可視化の対象外とした。図 7 は、探査機 a,b,c のグループと、探査機 d,e のグループに分断されたまま可視化した結果を示しており、3.3.c.3 で述べた手法によりグループ間を繋いだ、最終的な可視化結果が図 8 である。図 5 及び図 8 から分かるように、提案手法を用いて、物理構成可視化の実現性が確認できた。

Copyright © 2021 by
The Institute of Electronics, Information and Communication Engineers and
Information Processing Society of Japan All rights reserved.

表 1　評価実験結果一覧

送信 / 応答	a	b	c	d	e
A	**0.1943 (0.0209)**	0.4533 (0.0231)	0.2965 (0.0229)	0.3085 (0.0148)	0.3357 (0.0223)
B	0.4553 (0.0270)	**0.2877 (0.0218)**	0.5633 (0.0298)	0.5719 (0.0164)	0.5915 (0.0230)
C	0.4619 (0.0234)	0.7238 (0.0266)	**0.4554 (0.0265)**	0.4639 (0.0170)	0.4895 (0.0212)
D	0.3095 (0.0224)	0.5649 (0.0265)	0.3061 (0.0193)	**0.1953 (0.0262)**	0.2225 (0.0221)
E	0.3514 (0.0212)	0.6171 (0.0282)	0.3461 (0.0160)	0.2452 (0.0184)	**0.2174 (0.0213)**
a		0.4551 (0.0220)	**0.3004 (0.0200)**	0.3042 (0.0196)	0.3327 (0.0254)
b	**0.4467 (0.0237)**		0.5668 (0.0191)	0.5674 (0.0278)	0.5947 (0.0186)
c	**0.2975 (0.0194)**	0.5616 (0.0202)		0.3085 (0.0592)	0.3261 (0.0207)
d	0.3095 (0.0545)	0.5624 (0.0260)	0.3008 (0.0189)		**0.2185 (0.0206)**
e	0.3268 (0.0277)	0.5883 (0.0248)	0.3282 (0.0187)	**0.2189 (0.0232)**	

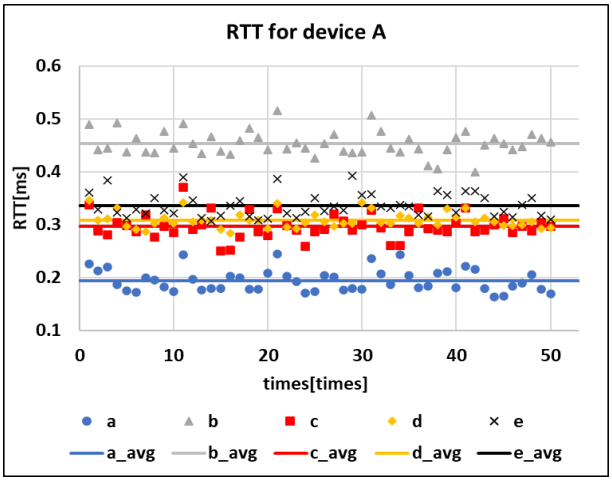


図 6　連結前の分離した構成の可視化結果

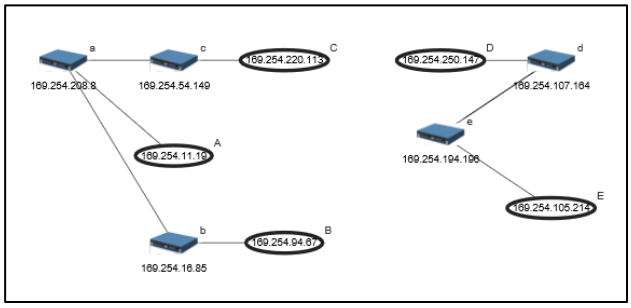


図 7　連結前の分離した構成の可視化結果

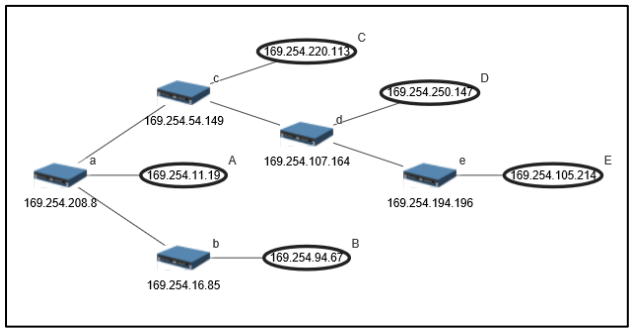


図 8　構成を連結した最終的な可視化結果

5. おわりに

本稿では、物理的なシステム構成を可視化する技術を提案した。具体的には、LAN 内に存在する全ての中継機器に、ping 送受信を行う探査機を 1 台ずつ設置し、探査機からの ping パケットの RTT を計測し、その最小値から接続関係を導き出す方法を提案した。提案方式では、RTT の計測だけで分析する為、機器間の時刻同期が必要ない。また、中継機器の機能(MAC アドレステーブル参照の可否等)にも依存せず、ping 送受信のみで物理構成を導出することができる。更に、実験環境を用いて提案方式の評価を行い、正しく物理構成が可視化できることを確認した。

尚、提案方式では、RTT の平均値を用いている。本実験では、n=50 回での平均値を用いているが、n が小さいとノイズによる影響が考えられ、また n が大きいと、その分、計測時間がかかる。それ故、最適な n の回数を求めることも重要と考え、今後の課題とする。また、提案方式では、全中継機器に探査機を 1 台ずつ設置しているが、大規模システムを想定した場合、それは現実的ではない。それ故、探査機の設置数を削減しつつ、物理構成を可視化できることが望ましい。今後の課題とする。

参考文献

[1] Krzysztof Nowicki, Aleksander Malinowski, “Topology Discovery of Hierarchical Ethernet LANs without SNMP support”, Annual Conference of the IEEE Industrial Electronics Society, IECON2015-Yokohama, November 9-12, pp5439-5443,(2015).

[2] 深見 公彦, 佐藤 正崇, 田山 健一, 堀内 慎吾,“複数ネットワーク構成の可視化方式に関する一検討”, 信学技報, ICM2017-80, pp.145-150, (2018).

[3] J.Flathagen, and O.I.Bentstuen, “Proxy-based Optimization of Topology Discovery in Software Defined Networks”, International Conference on Military Communications and Information Systems, Montenegro, May 2019, pp.1-5

[4] 中村 瑞人, 丹治 直幸, 高田 篤, 関 登志彦, 山越 恭子,“トラフィック情報を用いた構成管理技術における制度向上方法の検討”, 信学技報, ICM2019-16, pp.59-64, (2019).

[5] 高田 篤, 林 直輝, 中村 瑞人, 丹治 直幸, 関 登志彦, 山越 恭子,“警報を活用した通信事業者ネットワークにおけるトポロジ検出技術”, 信学技報, ICM2020-1, (2020).

[6] “総務省における情報セキュリティ政策の推進に関する提言”, 情報セキュリティ アドバイザリーボード, 平成 25 年 4 月 5 日, https://www.soumu.go.jp/main_content/000217000.pdf, (Accessed January 2021)

Copyright © 2021 by
The Institute of Electronics, Information and Communication Engineers and
Information Processing Society of Japan All rights reserved.