Vol.2016-IOT-32 No.18
2016/3/3

時間付きマルコフモデルを用いた障害検知手法の提案

近藤 喜芳† 立花 篤男† 下園 幸一‡ 長谷川 輝之† 阿野 茂浩† 山之上 卓††

概要：通信事業者が安定した通信サービスを提供するためには，ネットワーク装置の障害を迅速に検知し，適切な復旧対応を実施することが重要である．一般的に，ネットワーク装置障害はイベントログに含まれているアラート情報により直接的に検知されるが，より検知感度の高い手法として，イベントログ時系列パターンに着目し，発生数の少ないパターンを検知する方法も研究されている．これまで，マルコフモデルを用いてイベントログ時系列を学習し，状態遷移確率の低い時系列パターンを検知する手法が提案されているが，これらの手法は，各状態遷移の時間的な特徴を考慮していない．このため，平常時と同一の状態遷移を短時間に繰り返すような障害に対応できない課題がある．そこで，筆者らは時間付きマルコフモデルを用いて，状態遷移の時間的な特徴も考慮した障害検知手法を提案する．本稿では，提案手法の概要を述べると共に，キャンパスネットワークに設置されたネットワーク装置のイベントログを用いた評価結果について述べる．

A Proposal of Anomaly Detection Method based on Timed Markov Model

KIYOSHI KONDO† ATSUO TACHIBANA† KOICHI SHIMOZONO‡
TERUYUKI HASEGAWA† SHIGEHIRO ANO† TAKASHI YAMANOUE††

Abstract- It is important for network operators to promptly detect failure incidents and then take appropriate actions to mitigate them. Network failure incidents are often detected by directly discovering alert information included in the event logs of network devices and servers. However, in some cases, no event logs indicate alert information that is helpful to identify the failure. To address this problem, in this paper, we propose an anomaly detection method which considers temporal characteristics of state transition by using Timed Markov Model. The proposed method is evaluated with actual network logs of a campus network, and is shown to have high detectability.

1. はじめに

近年，ネットワーク(NW)を利用した IT システムは我々の生活に不可欠なものとなっており，NW 装置の障害によりシステムに不具合が発生した場合には，生活に重大な支障が生じる可能性がある．NW 装置の障害時間を短縮して障害による影響を抑制するためには，NW 管理者が NW 装置障害を迅速に検知し，適切な復旧作業を実施することが重要である．一般的に，NW 装置障害は NW 装置が発報するイベントログに含まれるアラート情報により直接的に検知される場合が多いが，障害発生時において，必ずしもイベントログにアラート情報が含まれているとは限らない．

これに対し，これまで，アラート情報を含まないイベントログの発生系列に着目し，発生数の少ない時系列パターンを障害の候補として検知する手法が検討されている(e.g., [1][2][3])．しかしながら，これらの手法の多くはイベントの発生順序に着目しており，イベントの発生間隔については十分に考慮していない．このため，NW装置において多数の(アラートでない)イベントが短時間に繰り返し発生するような障害[4]が発生した場合であっても，イベント発生順序が平常時と同様である限りにおいては，障害として検知できない課題がある．

そこで筆者らは，NW 装置のイベント発生を監視対象の状態遷移と捉え，時間付きマルコフモデル[5]に基づいて，発生頻度の低い(稀な)状態遷移系列をより高い感度で検知する手法を検討している[6]．ここで，時間付きマルコフモデルとは，ある状態から次の状態に遷移する遷移確率が，遷移元状態における滞在時間に応じて変化する状態遷移モデルである．

以下，本稿では，提案手法の概要を説明すると共に，キャンパス NW に設置された NW 装置のイベントログ(装置ログ)用いて提案手法の有効性を評価した結果について述べる．

2. 関連研究

前述の通り，イベントログの発生系列に着目して発生数の少ないパターンを検知する手法はこれまでにも提案されている(e.g., [1][2][3])．例えば，文献[1]は，NW装置で発生したイベントログ時系列から，平常時におけるイベント発生(順序)パターンを抽出した後，評価対象のイベントログ時系列が抽出されたイベント発生パターン集合に合致する

† (株)KDDI 研究所
KDDI R&D Laboratories Inc.
‡ 鹿児島大学
Kagoshima University
†† 福山大学
Fukuyama University

ⓒ2016 Information Processing Society of Japan

かどうかを調査することで，正常/異常の判定を実行する．しかし，この手法は，イベントの発生間隔を考慮していないため，イベント発生間隔が特異な障害が発生したとしても，評価対象のイベントログ時系列が抽出パターンと一致する場合は，障害として検出できない課題がある．

また，文献[2][3]は，ネットワークトラヒック情報やシステムログの分析に基づき，異常な状態遷移をサイバー攻撃として検知する手法を提案している．監視対象システムの状態遷移をマルコフモデルで表現した上で，遷移確率があらかじめ設定した閾値未満の状態遷移系列を検出した場合は，当該系列を異常として検知する．しかし，一般的なマルコフモデルでは，各状態遷移の発生間隔は考慮されないため，文献[1]と同様に，遷移元状態での滞在時間が特異な障害であっても，同一の状態遷移系列の中において検知できない場合がある．

一方，実際のNW装置の運用においては，短時間にイベント発生を繰り返す障害が存在することが知られている[4]．本研究では，従来手法に対して，イベントの発生間隔(各状態での滞在時間)も考慮した手法を提案し，上述のようなイベント時系列の検出に対応する．

3. 提案手法

3.1 用語

以降，本論文の用語は，本節の定義に従う．

- イベント：NW 装置で発生した事象
- イベントログ：イベントが発生した際に NW 装置より発報されるメッセージ
- イベントログ時系列：同一の NW 装置で発生したイベントログを発生した順番に並べた系列
- 状態遷移：NW 装置の状態が変化すること，または 2 つの連続するイベントログより得られる NW 装置の状態変化
- 状態遷移系列：2 つ以上の連続する状態遷移より得られる複数の状態遷移の系列

3.2 概要

障害時の状態遷移系列は正常時と比べて発生数が少ないと考えられるため，これを検知することで，単一のイベントのみでは判断が困難な障害を検知できると考えられる．提案手法の概要を図 1 に示す．

① まず，監視対象の NW 装置から平常時のイベントログ時系列を取得し，これを学習データとして，NW 装置の状態遷移を時間付きマルコフモデルで表現する．

② 次に，時間付きマルコフモデルを用いて学習データから作成した各状態遷移系列についてその発生数の多さを表す評価値を算出し，評価値の分布から閾値を決定する．

③ 最後に，障害検知を実施する期間中に取得したイベントログ時系列を評価データとして，評価データから作成した各状態遷移系列について同様に評価値を計算する．評価値が閾値未満となる稀な状態遷移系列を障害の候補として抽出する．実際のネットワーク運用においては，イベントが発生する度に，当該監視対象において直近に発生したイベントと組み合わせてイベントログ時系列を作成し，評価データを作成する．

3.3 NW 装置ログを用いた学習

以下，監視対象は NW スイッチのポートを仮定して説明する．NW 装置ログから監視対象毎にイベントログ時系列 $E_N = (e_1, \ldots, e_N)$を学習データとして取得し，図 2 に示すような時間付きマルコフモデルで状態遷移を表現する．時間付きマルコフモデルとは，状態遷移確率が時間に依存するマルコフモデルであり，ある状態から次の状態に遷移するまでの遷移元状態での滞在時間に応じて遷移確率が変化する状態遷移モデルである．ポートの状態遷移を時間付きマルコフモデルで表現する手順は以下の通りである．

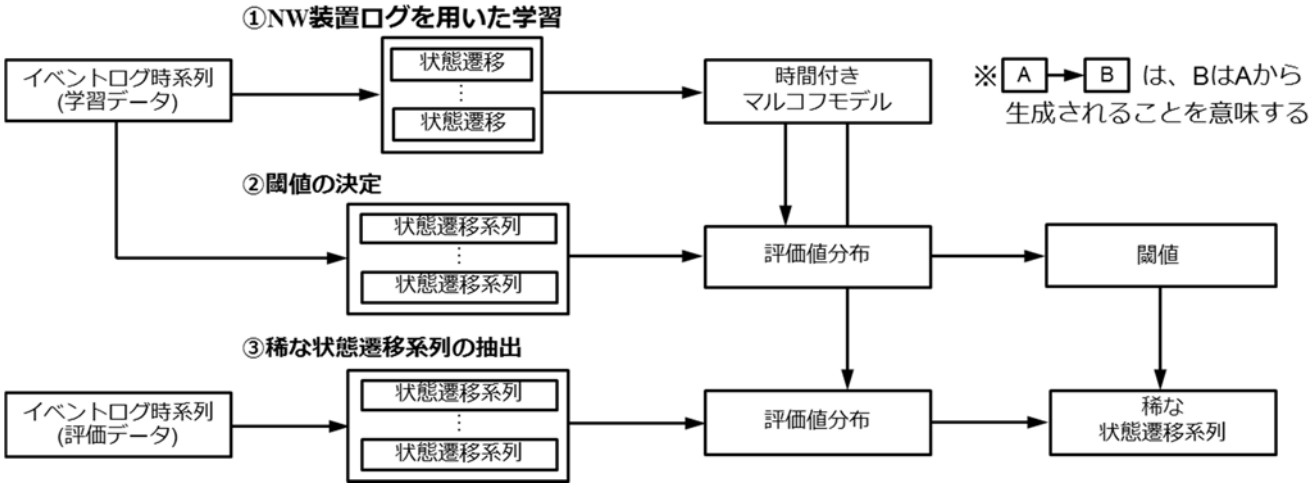

図 1 提案手法の処理フロー

ⓒ2016 Information Processing Society of Japan

・ポートが取り得る全状態の集合を$Y = \{y_1, \ldots, y_S\}$と表し，その各要素をモデルの状態として定義する．
・n番目に観測されたイベントログを$e_n = (t_n, x_n)$と表す．t_nはe_nの発生時刻，$x_n \in Y$はe_n発生後のポート状態である．
・E_Nより任意の連続する 2 つのイベントログ$e_h, e_{h+1}(h = 1,2, \ldots, N-1)$を抽出すると 1 つの状態遷移$x_h \rightarrow x_{h+1}$を表すことができる．この時，遷移元状態に滞在していた時間は$t_{h+1} - t_h$である．全ポートのE_Nより全ての状態遷移を抽出し，$y_i \rightarrow y_j\ (i, j = 1,2, \ldots, S)$について以下を算出して時間付きマルコフモデルを表現する．
  ・$g_{y_i y_j}$：状態がy_iの場合にy_jに遷移にする確率
  ・$f_{y_i y_j}(T_i)$：$y_i \rightarrow y_j$の遷移におけるy_iでの滞在時間$T_i = t_j - t_i$の分布を示す確率密度関数

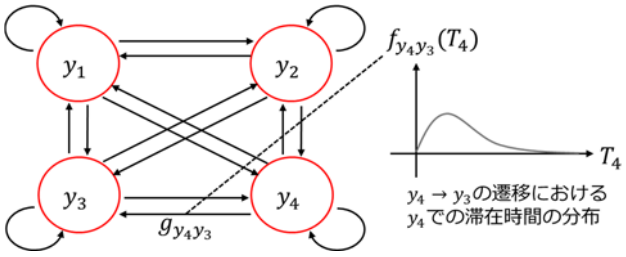

図 2 時間付きマルコフモデル(S=4)

3.4 閾値の決定

3.3 で作成した時間付きマルコフモデルから，稀な状態遷移系列の抽出に用いる閾値を計算する．E_Nから監視対象毎に連続する長さKのイベントログ時系列$P_{v,K} = (e_v, \ldots, e_{v+K-1})$をスライディングウィンドウ方式で切り出し，各イベントログ時系列について(式 1)より評価値$R(P_{v,K})$を算出する．この評価値は高いほど発生数の多い状態遷移系列であるとみなす．算出した評価値の分布を作成し，下位z%(z：任意の値)に位置する評価値を閾値とする．ここで，$p(x_v)$はポートの全状態の中でx_vが初期状態である確率，$F_{x_l x_{l+1}}(t_{l+1} - t_l)$は$x_l \rightarrow x_{l+1}$の遷移関数であり(式 2)に示す累積確率を用いる．

$$R(P_{v,K}) = p(x_v) \prod_{l=v}^{v+K-2} F_{x_l x_{l+1}}(t_{l+1} - t_l) \qquad \text{(式 1)}$$

$$F_{y_i y_j}(T_i) = g_{y_i y_{j_i}} \int_0^{T_i} f_{y_i y_j}(u) du \qquad \text{(式 2)}$$

ここで本稿では，装置が故障して状態が不安定な場合，状態間を頻繁に(短い時間間隔で)遷移する事象が発生する可能性が高いと考え，状態間の遷移間隔が短いほど評価値が小さくなるように累積分布を用いることとした．

3.5 稀な状態遷移系列の抽出

障害検知を実施する期間内に取得した監視対象のイベントログ時系列$E_M = (e_1, \ldots, e_M)$から監視対象毎に連続する長さKのイベントログ時系列$P_{w,K} = (e_w, \ldots, e_{w+K-1})$をスライディングウィンドウ方式で切り出す．$P_{w,K}$を 3.3 で作成した時間付きマルコフモデルに当てはめ，(式 1)より評価値$R(P_{w,K})$を求める．算出した$R(P_{w,K})$が 3.4 で決定した閾値未満である場合，稀な状態遷移系列として抽出する．

(式1)・(式2)より，提案手法は，①状態間の遷移の発生数が少ない状態遷移，②遷移元状態での滞在時間が短い状態遷移，を含む系列を稀な状態遷移系列として抽出しやすいと言える．従って，NW装置の障害により，平常時では遷移する回数が少ない状態への状態遷移や，平常時よりも頻繁に(短い時間間隔で)遷移する事象が発生した場合に，稀な状態遷移系列として抽出できる．

4. 評価試験

鹿児島大学学術情報基盤センターの NW 装置(監視対象ポート数は 671 ポート)のイベントログ(2015/03/29～10/24)を分析対象とし，学習データ$E_N(N = 140{,}752)$と評価データ$E_M(M = 132{,}508)$に分割した．E_Nから$S = 4$の時間付きマルコフモデルを作成し，提案手法の評価試験を行った．以下に試験結果の概要を説明する．

(1) 実験的に，試験のパラメータとして$K = 3$，閾値を学習時の評価値分布の下位2%(z=2)と設定した結果，131,829件の状態遷移系列の内，5,351件を稀な状態遷移系列として抽出した．抽出した系列は以下の特徴を持つ2種類の状態遷移系列であった．
  ① 遷移確率が非常に低い状態遷移を含む状態遷移系列．例えば，図2中の状態遷移:$y_1 \rightarrow y_3 \rightarrow y_2$において，状態遷移確率$g_{y_3y_2}$は0.013であり，表1に示す他の状態遷移確率$g_{y_iy_j}$よりも1/10以下と低い．このような場合，評価値$R$は非常に小さな値になる．
  ② 遷移確率は低くないが，遷移元状態での滞在時間が平常時よりも短い状態遷移を含む状態遷移系列．例えば，図2中の状態遷移：$y_4 \rightarrow y_3 \rightarrow y_1$において，$y_4$での滞在時間$T_4$が2秒の場合，図3の累積分布に基づいて計算される$F_{y_iy_j}(T_i)$の値が0.1以下と低い．このような場合においても，評価値Rは非常に小さな値になる．

表1 状態間の遷移確率(抜粋)

$y_i \rightarrow y_j$	$g_{y_iy_j}$
$y_1 \rightarrow y_3$	0.999
$y_3 \rightarrow y_2$	0.013
$y_4 \rightarrow y_3$	0.999
$y_3 \rightarrow y_1$	0.353

ⓒ2016 Information Processing Society of Japan

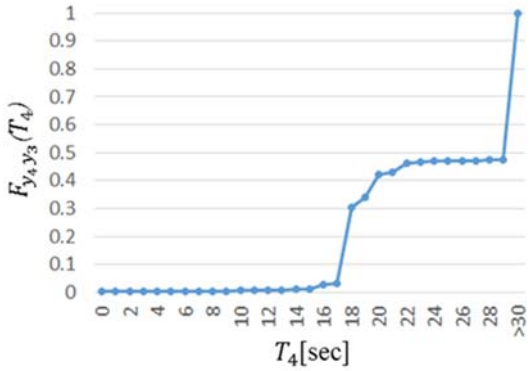

図3 滞在時間の累積分布(抜粋)

(2) 上記で抽出した稀な状態遷移系列を，7 件のユーザからの障害報告と照合した．本評価試験では，障害発生からユーザからの報告までに日数を要することを考慮し，図 4 に示すように，報告日時から過去 1 週間以内に稀な状態遷移系列が検知されている場合は，障害検知に成功したと見なした．

照合の結果, 評価データに対応する期間内(119日間)のユーザからの障害報告7件ついて，全て障害検知に成功していた．ここで，7件中の6件では②の系列，残りの1件は①の系列であった．なお，監視対象671ポート全体では，1週間の期間内に少なくとも1件以上の稀な状態遷移系列が検知される確率は$0.374(1-\{(1-(5351/(671*119*24*60*60)))^{(7*24*60*60)}\})$と試算されるため，7件全てが偶発的に成功と判定された可能性は十分に低いと考えられる(約$0.1[\%] \fallingdotseq 0.374^7$).

今回のパラメータで提案手法を用いてNW運用を実施する場合，NW管理者が確認すべき稀な状態遷移系列は約45[件/日]となる．一方で，抽出結果にはユーザより報告されていない障害に紐づく状態遷移系列が含まれると考えられるため，さらなる検証は今後の課題である．

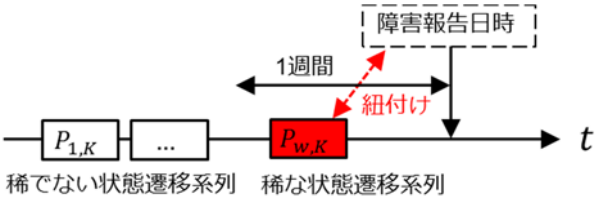

図 4 検知した稀な状態遷移系列と障害報告の紐付け方法

(3) また，時間付きマルコフモデルの代わりにマルコフモデルを用いて同様の評価試験を行った．その結果，時間付きマルコフモデルの代わりにマルコフモデルを用いた場合，ユーザからの障害報告と紐付いたのは3件のみであり，全て①の系列であった．この結果，遷移元状態での滞在時間を考慮する提案手法の有効性が確認できた．

5. まとめ

本稿では，NW 装置ログに記録されたイベントログ時系列から稀な状態遷移系列を抽出する手法を提案した．提案手法では，時間付きマルコフモデルを応用し，遷移元状態での滞在時間が短い状態遷移系列に低い評価値を設定して稀な状態遷移を抽出した．キャンパス NW の装置ログを用いて提案手法の評価試験を行い，抽出した稀な状態遷移系列にユーザから報告された障害が含まれることを確認した．より大規模な評価実験や様々なNW装置への適用性の検討が今後の課題である．

参考文献

[1] 外川 他, ”ログの出力パターンに基づく大規模システム向けログ分析手法の開発と評価”, 信学技報, vol. 114, no. 389, ICM2014-34, pp. 13-18, 2015 年 1 月.
[2] N. Ye, Y. Zhang and C.M. Borror (2004), Robustness of the Markov-Chain Model for Cyber-AttaCk Detection, IEEE Irunsactions on Reliability, 53(1), pp. 116-123.
[3] 荒木 他:通信のクラスタ間遷移に基づくサイバー攻撃検知手法，コンピュータセキュリティシンポジウム 2015 論文集, vol.2015 , No.3 , pp. 1066 – 1072, 2015.
[4] NTT Communications, ICT 用語辞典, Route Flapping; http://www.ntt.com/business/techsupport/dictionary/word/0581.html
[5] Jan.Lunze; Diagnosis of Quantized Systems Based on a Timed Discrete-Event Model, IEEE Trans. Syst. Man. Cybern., vol.30, no.3, pp.322-335, (2000).
[6] 近藤 他, "時間付きマルコフモデルを用いたシステム異常検知に関する一検討”, IEICE ソサイエティ大会講演論文集 2015 年_通信(2), no. B-16-9, pp. 334, Aug. 2015.

ⓒ2016 Information Processing Society of Japan