通信制御系に対するモデルベース縮退運転システム

佐々木 翼† 澤田 賢治† 新 誠一† 細川 嵩‡
†電気通信大学情報理工学研究科
‡技術研究組合制御システムセキュリティセンター

あらまし 近年，工場や発電所といったプラントの制御システムにおいて制御機器のネットワーク化が進行しており，生産性の向上が実現されている．一方で，制御システムに対するサイバー攻撃の危険性が指摘されている．制御システムにおいて異常が発生した場合の事後対策として，正確な異常検出と安全側への制御（縮退運転）が必要となる．しかし，中間者攻撃による情報改ざんを想定したときデータ通信ネットワーク上のパケットを用いた縮退運転は安全とは限らない．そこで本稿では，パケットを用いない縮退運転の実現のために有限状態機械を用いたモデルベース縮退運転を提案する．
キーワード モデルベース縮退運転，中間者攻撃，双線形オブザーバ

A Model Based Fallback System for Communication Control System

Tsubasa Sasaki† Kenji Sawada† Seiichi Shin† Shu Hosokawa‡
†The University of Electro-Communications, Graduate School of Informatics and Engineering
‡Control System Security Center

Abstract Recently, a networking of controllers is developing on a control system for a factory or a power plant. The networking helps to increase a productivity. On the other hand, with the networking, there are new threads of cyber-attacks against control systems. For control systems, an exact anomaly detection and a control to the safe side (the fallback operation) are needed as subsequent countermeasures when anomaly happens. However, the fallback operation with packet on data communication network is not always safe when manipulation of information on data communication network is supposed. This paper proposes a model based fallback operation via Finite State Machine to implement the fallback operation without packet.

Keywords Model based fallback, MITM, Bilinear observer

1. 問題設定

近年，制御システムでは制御機器のネットワーク化が進められおり，生産性の向上が実現されている[1]．その一方で，制御システムにおけるマルウェアや不正アクセスといったサイバーセキュリティのリスクが高まっている．2010 年には，イランの核施設の破壊を目的とした Stuxnet とよばれるマルウェアが報告されている．その後，Stuxnet と類似したマルウェアである Duqu と Flame がそれぞれ 2011 年，2012 年に報告されている[2]．さらに，2014 年には制御システムを標的としたトロイの木馬型不正プログラム Havex が報告されている[3]．

こうした状況において，制御システムのサイバー攻撃対策が迅速に進んでいる．現状は情報システムセキュリティの技術転用であり，システム管理レベルでの事前防止策や攻撃検出に関する研究が主である[4-5]．一方で，制御システムのセキュリティレベルは情報システムのそれに比べて未だ堅牢ではない．堅牢ではない理由はいくつかある．そのうちの 1 つは，Table 1 に示すような情報システムと制御システムのセキュリティの視点の違いである．このような違いがあるため，情報システムセキュリティ技術を制御システムに転用するのみでは不十分であり堅牢になりえない．

制御システムに対するサイバー攻撃の目的にはシステムの破壊や停止も含まれることを考慮すると，攻撃を前提とした事後対応（インシデント対応[6]）も重要である．例えば，FA (Factory Automation) システムにおいてサイバー攻撃が発生し，システムが停止すると多大な被害が想定される．その 1 つの例に，2005 年 8 月に不正プログラム「WORM_ZOTOB」によって発生した独ダイムラー社の米国 13 工場の操業停止事件がある．各工場の製造ラインが止まり，50 分間作業ができない状態になった．部品サプライヤへの感染も疑われ，およそ 1400 万ドル（当時の為替で約 11 億円）の損害をもたらした[7]．このような被害を避けるためには，

Table 1 Security focus in IT vs. industrial control systems[6]

セキュリティ項目	情報システム	制御システム
ウイルス対策 モバイルコード	一般的 広く使用	効果的な配備は 一般的でない/不可能
サポート技術の 寿命	2-3 年 多様なベンダ	最大 20 年 単一ベンダ
外部委託	一般的	運用は外部委託されることもあるがサービス提供者は多くない
パッチの適用	広く利用	まれ，非計画的 ベンダ固有
変更管理	定期的 計画的	厳格に管理され 複雑
時間に厳しい処理	一般に遅延を許容	遅延は許されない
可用性	一般に遅延を許容	24 時間 365 日 (連続稼働)
セキュリティ意識	民間，公共部門 ともに中程度	物理的セキュリティ 以外は貧弱
セキュリティテスト 監査	優れたセキュリティ プログラムに含まれる	停電に備えた テストを時折実施
物理セキュリティ	安全 (サーバ室など)	遠隔/無人 安全

システムがサイバー攻撃を受けても運転が継続できる枠組みが必要である．

また，制御システムに対するサイバー攻撃は経済的な影響を及ぼすだけでなく安全をも脅かす．制御システムの安全を確保するための規格として，機能安全規格がある．機能安全規格に則った機器を使用することで，制御システムの安全を確保できる．しかし，現在の機能安全規格にはサイバー攻撃による影響が考慮されていない．例えば，機能安全規格に則ったプラント異常対応策として，安全計装システムがある．安全計装システムはデータ通信ネットワークに接続され，異常の検出ならびに安全側への制御を行う．これは，サイバー攻撃を除いたシステム故障・異常に対してプラントの高安全性と高稼働率性を維持するものである．データ通信ネットワーク上の情報を用いる以上，中間者攻撃 (MITM: Man In The Middle attack)[8]のような情報改竄に対して安全とは限らない．したがって，現状の機能安全規格に則った安全計装システムは安全とはいえない．制御システムの安全を確保するためにも，サイバー攻撃に対応した異常検出技術と安全側への制御技術が必要である．

本稿では，通信制御系に対する中間者攻撃の事後対応策として縮退運転システムを提案する．本稿における縮退運転とは，機能を制限しながら中間者攻撃に対して防御に徹することで制御システムの稼働継続を実現させる運転である．縮退運転システムは，中間者攻撃の検出と縮退運転への切り替えを行う．特に，本稿では制御システムのモデル情報に基づき縮退運転システムを構築する．ここでモデルとは，制御ロジックの遷移プロセスを予測・推定するための単純化された数理モデルのことである．正常時の遷移プロセスをモデル化できれば（正常モデル），正常モデルから逸脱した状態を異常として検出できる．このようなモデルベースの縮退運転により，中間者攻撃後の稼働継続を実現する．

本稿では，FA システムの不良品判別器を模擬したプラントに対して縮退運転システムを構成する．ここで，中間者攻撃用の縮退運転システムを実現するため，既存の安全計装コントローラには無い要素技術を 2 つ提案する．1 つ目は，データ通信ネットワーク上のパケットを用いない中間者攻撃検出である．これにより，縮退運転システムをネットワーク化制御器側にではなく，制御対象側に設置する．この技術の利点は，中間者攻撃による情報改竄の影響を受けることのない異常検出が可能となる点である．具体的には，制御ロジックの遷移プロセスを有限状態機械（FSM: Finite State Machine）でモデル化し，中間者攻撃検出のためのオブザーバを構成する．本稿でのオブザーバとは制御工学の状態推定理論に基づくものであり，センサ情報とモデルから推定対象の内部状態を観測する方法である[9]．本縮退運転システムでは，アナログ電圧としてプラントから直接取得されたセンサ情報とオブザーバを用いて中間者攻撃による異常を検出する．2 つ目の要素技術は縮退運転中にプラントとネットワーク化制御器を隔離する仕組みである．この技術により，縮退運転中に中間者攻撃によるプラントへの悪影響を避けることが可能となる．具体的には，縮退運転切り替え時にプラントとデータ通信ネットワークを自動的に遮断する．

本稿では，以上 2 つの要素技術を実装しモデルベース縮退運転システムの提案と Arduino[10]を用いた実機実験を行う．

表記：実数のn次元ベクトルを$\mathbb{R}^n$と表記する．整数のn次元ベクトルを$\mathbb{Z}^n$と表記する．また，$n \times n$の実行列を$\mathbb{R}^{n\times n}$，$n \times n$の整数行列を$\mathbb{Z}^{n\times n}$と表す．$\boldsymbol{D}^{\mathrm{T}}$は行列$\boldsymbol{D}$の転置を表す．$\{0,1\}^n$は，要素が 0 または 1 の$n$次元ベクトルを表す．

2. 問題設定

はじめに，本稿で想定する通信制御系の構成を Fig. 1 に示す．ネットワーク機器間の接続には，産業用イーサネット通信規格の一つである Modbus/TCP を用いる．リモート I/O は制御用パケットをアナログ電圧（電流）に変換しアクチュエータを駆動させる．また，模擬プラントから出力されたセンサ情報はリモート I/O により Modbus/TCP パケットに変換され，通信路を介してネットワーク化制御器へ送られる．

次に，実機実験に用いる模擬プラントの外観を Fig. 2 に，概略図を Fig. 3 に示す．このプラントの機能は，

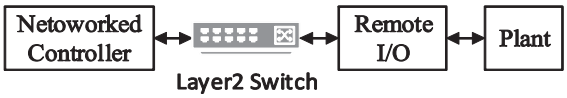

Fig. 1 Subject of this study

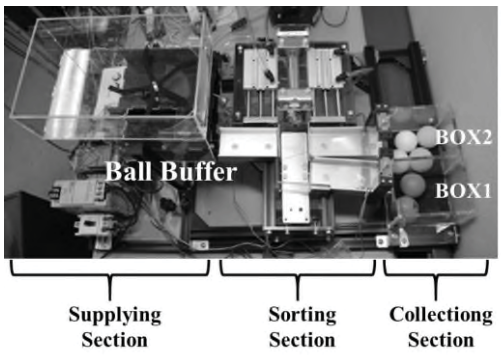

Fig. 2Appearance of the simulated plant

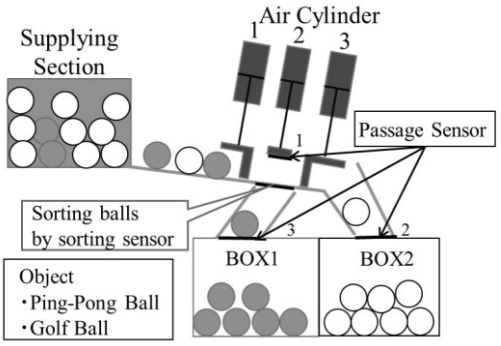

Fig. 3 Behavior of simulated plant

重量の異なる 2 つのボールを仕分けるというものである．実機実験では，軽いボールとして卓球ボールを，重いボールとしてゴルフボールを使用する．本稿では，このプラントを FA システムにおける不良品判別器と想定する．ここでは，軽いボールを良品，重いボールを不良品として考える．すなわち，本稿で用いるシステムは FA システムのサブシステムを想定したものである．

最後に，ボールの仕分けを行うための制御ロジックを Fig. 4 に示す．本稿で用いる模擬プラントは，3 つのエアシリンダ，1 つの仕分け用センサおよび 3 つの通過検出センサを備えている．模擬プラントは，ゴルフボールを不良品として BOX1 へ，卓球ボールを良品として BOX2 へ仕分ける．

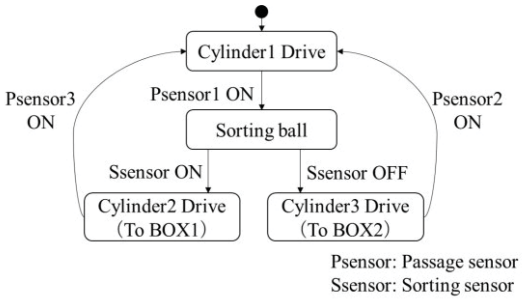

Fig. 4 Control Logic for Normal Operation

3. サイバー攻撃

本稿では，サイバー攻撃として中間者攻撃を想定する．中間者攻撃は攻撃者が通信を行う二者間に割り込み，情報の傍受および改ざんを行うという攻撃手法である．実機実験では，MATLAB/Simulink の Instrument Control Toolbox を用いて TCP パケット（制御用信号）改ざんを模擬する．

本稿の目的は，中間者攻撃発生後のプラント稼働継続である．そこで，模擬プラントを対象とした中間者攻撃に対する脆弱性解析を行う．一般に脆弱性とは「コンピュータの OS やソフトウェアにおいて，プログラムの不具合や設計上のミスが原因となって発生した情報セキュリティ上の欠陥」のことを指す（総務省[11]）．一方，本稿が扱う脆弱性とは情報セキュリティ上の欠陥ではなくプラントの物理セキュリティの欠陥のことを意味する．本稿では，このような意味での脆弱性について解析を行う．

実機実験で用いる模擬プラントはゴルフボールが卓球ボールとして誤認識されると，ゴルフボールが仕分け部分で詰まるという機能を持っている．この機能はセンサエラーが発生したとき，次の制御周期でセンサ情報を再確認できるようにするためのものである．この機能により，不良品が良品に混入しなくなる．一方で，センサエラーが解消されず上流工程からゴルフボールが供給され続けると，ボールバッファ部分の許容量を超過し玉詰まりによる稼働停止が発生する．本稿では，この仕組みを脆弱性と捉える．プラントの稼働停止を目的とした攻撃者は，この脆弱性をねらって中間者攻撃を行うものと想定する．さらに本稿では，センサ自体の故障は考えずセンサエラーは中間者攻撃によってのみ発生させられるものとする．

4. 縮退運転システム

本稿で提案する通信制御系に対する縮退運転システムの構成を Fig. 5 に示す．先行研究[12]では，ネットワーク化制御系に対する中間者攻撃の事後対応策としてペトリネットと線形オブザーバを用いたモデルベース縮退運転（Model Based Fallback System）が提案されている．これに対して本稿では，Fig. 4 の制御ロジックを有限状態機械（FSM）と捉え，これを双線形状態方程式で表現し双線形オブザーバの構成を行う．オブザーバの構成後，オブザーバの推定誤差から切り替え型リアプノフ関数を決定し中間者攻撃による異常を検出する．

Fig. 4 で与えられた制御ロジックを双線形状態方程式で表現すると

$$\begin{cases} \boldsymbol{x}(k+1) = \sum_{i=1}^{r} u_i(k)\boldsymbol{A}_i\boldsymbol{x}(k) \\ \boldsymbol{y}(k) = \sum_{i=1}^{r} u_i(k)\boldsymbol{C}_i\boldsymbol{x}(k) \end{cases} \quad (1)$$

となる．ここで，$\boldsymbol{x} \in \mathbb{Z}^n$は状態量，$\boldsymbol{u}_i(k) \in \{0,1\}^r$は入力，$\boldsymbol{y} \in \mathbb{Z}^n$はセンサなどにより観測可能な状態量である$(i \in 1,2,\cdots,r)$．また，$\boldsymbol{A}_i, \boldsymbol{C}_i$は実数係数行列である．(1)式は以下の制約式を満たす．

$$\sum_{i=1}^{n} \boldsymbol{x}_i(k) = 1, \quad (2)$$

$$\sum_{i=1}^{r} \boldsymbol{u}_i(k) = 1. \quad (3)$$

文献[13]ではブール半環により FSM を(1)式で表現できることを示している[13]．一方，本稿ではブール半環は用いず，FSM の状態遷移を制約条件(2)と(3)を有する離散事象システム(1)として表現する．離散時間システムにおいてはサンプリング時間が経過すると$\boldsymbol{k} \rightarrow \boldsymbol{k}+1$となる一方，離散事象システムでは状態が遷移してはじめて$\boldsymbol{k} \rightarrow \mathrm{k}+1$となることに注意する必要がある．(1)式について双線形オブザーバを構成すると

$$\begin{cases} \tilde{\boldsymbol{x}}(k+1) = \sum_{i=1}^{r} u_i(k)\boldsymbol{A}_i\tilde{\boldsymbol{x}}(k) - \sum_{i=1}^{r} u_i(k)\,\boldsymbol{K}_i\boldsymbol{e}_y(k) \\ \tilde{\boldsymbol{y}}(k) = \sum_{i=1}^{r} u_i(k)\boldsymbol{C}_i\tilde{\boldsymbol{x}}(k) \end{cases} \quad (4)$$

となる．ここで，$\tilde{\boldsymbol{x}} \in \mathbb{Z}^n$は推定状態量，$\tilde{\boldsymbol{y}} \in \mathbb{Z}^n$はオブザーバからの出力，$\boldsymbol{e}_y(k) \coloneqq \tilde{\boldsymbol{y}}(k) - \boldsymbol{y}(k)$，$\boldsymbol{K}_i \in \mathbb{Z}^{n\times n}$は整数型オブザーバゲインである．先行研究[12]のペトリネットによるモデリングは，プラントの動作を離散事

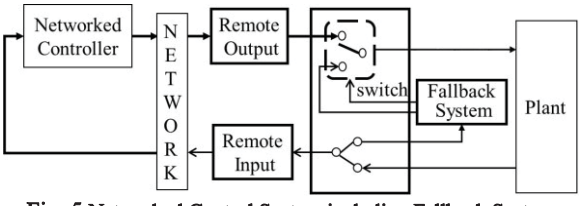

Fig. 5 Networked Control System including Fallback System

象システムの観点から観察する必要がある．一方，本稿のモデリングは制御ロジックが FSM で設計されていればそのまま使用することが出来る．これが，FSM をモデリング手法としたときの利点である

ここで，状態の推定誤差を

$$\boldsymbol{e}(k) = \tilde{\boldsymbol{x}}(k) - \boldsymbol{x}(k) \quad (5)$$

と定義する．(1), (4), (5)式より状態の推定誤差に関する状態方程式は

$$\boldsymbol{e}(k+1) = \sum_{i=1}^{r} u_i(k)\tilde{\boldsymbol{A}}_i\boldsymbol{e}(k) \quad (6)$$

と求められる．ただし，$\tilde{\boldsymbol{A}}_i = \boldsymbol{A}_i - \boldsymbol{K}_i\boldsymbol{C}_i$である．すなわち，(6)式が安定になるようなオブザーバゲイン$\boldsymbol{K}_i$が存在するならば，(4)式によって$\lim_{k\to\infty} \boldsymbol{e}(k) = 0$が達成されることになる．

本稿では(6)式の安定条件を考えるために，u_iを切り替え信号とみなし(6)式を切り替え型システムとして捉える．このとき，(6)式の安定性は切り替え型リアプノフ関数[15]を導入することで評価できるようになる．切り替え型リアプノフ関数として二次形式

$$V(k, e(k)) = \boldsymbol{e}(k)^{\mathrm{T}}\left(\sum_{i=1}^{r} u_i(k)\boldsymbol{Q}_i\right)\boldsymbol{e}(k) \quad (7)$$

を考える．ただし，$\boldsymbol{Q}_i \in \mathbb{R}^{n\times n}$は正定行列である．このとき，(6)式の安定条件は$\boldsymbol{e}(k)$の状態軌道に対して

$$V(k+1, e(k+1)) - V(k, e(k)) < 0. \quad (8)$$

が成り立つことである．

Table 2 入力の場合分け（$i, j \in 1,2,\cdots,r$）

ステップ数	パターン 1	パターン 2
k	$u_i(k) = 1$	$u_i(k) = 1$
$k+1$	$u_i(k+1) = 1$	$u_j(k+1) = 1$

(7)式では Table 2 のようにkステップと$k+1$ステップの前後で入力が同じ場合と異なる場合が存在する．この場合分けを考慮した上で(6), (7)式を(8)式に代入すると，(8)式の成立は以下の行列不等式

$$\tilde{\boldsymbol{A}}_i^T\boldsymbol{Q}_j\tilde{\boldsymbol{A}}_i - \boldsymbol{Q}_i < 0 \quad i, j \in 1,2,\cdots,r \quad (9)$$

の成立と等価となる．すなわち，(9)式を満たすような正定行列$\boldsymbol{Q}_i$ が存在するならば，(6)式は安定となる．$\boldsymbol{Q}_i$を変数とした(9)式は線形行列不等式（LMI: Linear Matrix Inequality）と呼ばれるもので有り，内点法によって効率的に変数を求めることができる[14].

したがって，(9)式を満たすオブザーバゲイン$\boldsymbol{K}_i$により双線形オブザーバ(4)を構成できる．一方で，$\boldsymbol{K}_i$を変数とすると，(9)式は$\boldsymbol{Q}_i$と$\boldsymbol{K}_i$を変数とする双線形行列不等式（BMI: Bilinear Matrix Inequality）となり，求解が容易でない．そこで，文献[15]で提案されている手法を用いる．詳細を省くと，$i \in 1,2,\cdots,r$に対して(9)式を満たす正定行列$\boldsymbol{Q}_i$と行列$\boldsymbol{K}_i$が存在することは，

$$\begin{bmatrix} -\boldsymbol{Q}_j^T + \boldsymbol{G}_i^T + \boldsymbol{G}_i & \boldsymbol{G}_i\boldsymbol{A}_i - \boldsymbol{L}_i\boldsymbol{C}_i \\ (\boldsymbol{G}_i\boldsymbol{A}_i - \boldsymbol{L}_i\boldsymbol{C}_i)^T & \boldsymbol{Q}_i \end{bmatrix} > 0 \quad (10)$$

$$i, j \in 1,2,\cdots,r$$

を満たす正定行列$\boldsymbol{Q}_i$と行列$\boldsymbol{L}_i \in \mathbb{R}^{n\times n}$，$\boldsymbol{G}_i \in \mathbb{R}^{n\times n}$ が存在することと等価である．また，$\boldsymbol{L}_i$は以下のように与えられる．

$$\boldsymbol{L}_i = \boldsymbol{G}_i\boldsymbol{K}_i \quad (11)$$

(10)式は変数行列に対して線形であるため，オブザーバゲイン$\boldsymbol{K}_i = \boldsymbol{G}_i^{-1}\boldsymbol{L}_i$は LMI を解くことで求められる．

つぎに切り替え型リアプノフ関数による異常検出を考える．一般に，正定行列$\boldsymbol{P}$に対して

$$\lambda_{min}(\boldsymbol{P})\boldsymbol{x}(k)^T\boldsymbol{x}(k) \le \boldsymbol{x}(k)^T\boldsymbol{P}\boldsymbol{x}(k) \quad (12)$$

が成り立つ．ここで，$\lambda_{min}(\boldsymbol{P})$は$\boldsymbol{P}$の最小固有値を意味する．(7), (8), (12)式より

$$\lambda_{min}\left(\boldsymbol{Q}_i - \boldsymbol{A}_i^T\boldsymbol{Q}_j\boldsymbol{A}_i\right)\boldsymbol{e}(k)^{\mathrm{T}}\boldsymbol{e}(k) \le -\left(V(k+1, e(k+1)) - V(k, e(k))\right) \quad (13)$$

となる．すなわち正常時の推定誤差の変化率は以下のようになる．

$$V(k+1) - V(k) \le -\lambda_{min}\left(\boldsymbol{Q}_i - \boldsymbol{A}_i^T\boldsymbol{Q}_j\boldsymbol{A}_i\right)\|\boldsymbol{e}(k)\|_2^2 \quad (14)$$

だだし，$\|\boldsymbol{e}(k)\|_2$は推定誤差$\boldsymbol{e}(k)$に対するユークリッドノルムである．(14)式が満たされないとき，中間者攻撃による異常が発生したものとして検出する．

次に，通常運転から縮退運転への切り替えについて Fig. 6 に示す．Fig. 6 に示すように，(14)式を満たさず異常を検出すると自動的に縮退運転へと切り替える．縮退運転ではボールの仕分けは行わずボールを片方のボックスに流すことに専念する．このような運転制御を行うことでセンサエラーに依存しない稼働が可能となる．これは，”プラント稼働停止と比較して良品（卓球ボール）が不良品（ゴルフボール）BOX に流されるほうがリスクは小さい”というリスク分析に基づいたものである．

5. 実機実験

本章では，これまでに述べてきた手法を Arduino に実装し実機実験を行う．Fig.4 の制御ロジックを双線形状態方程式で表現すると

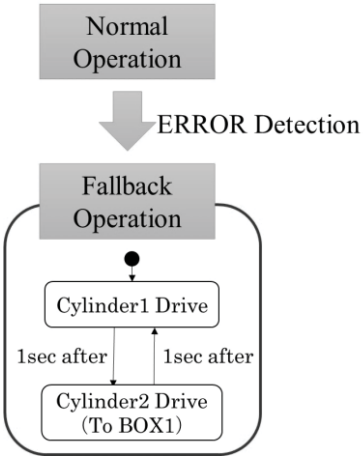

Fig. 6 Operation mode switching

$$\begin{cases} \boldsymbol{x}(k+1) = \sum_{i=1}^{5} u_i(k)\boldsymbol{A}_i\boldsymbol{x}(k) \\ \boldsymbol{y}(k) = \sum_{i=1}^{5} u_i(k)\boldsymbol{C}_i\boldsymbol{x}(k) \end{cases} \quad (15)$$

となる．ここで，$\boldsymbol{x}(k) \in \mathbb{Z}^4$, $\boldsymbol{u}(k) \in \mathbb{Z}^4$ $\boldsymbol{y}(k) \in \mathbb{Z}^4$は以下のように与えられる．

$$\boldsymbol{x}(k) = \begin{bmatrix} x_1(k) \\ x_2(k) \\ x_3(k) \\ x_4(k) \end{bmatrix}, \boldsymbol{u}(k) = \begin{bmatrix} u_1(k) \\ u_2(k) \\ u_3(k) \\ u_4(k) \end{bmatrix}, \boldsymbol{y}(k) = \begin{bmatrix} y_1(k) \\ y_2(k) \\ y_3(k) \\ y_4(k) \end{bmatrix}.$$

(15)式は以下の制約式を満たす．

$$\sum_{i=1}^{5} \boldsymbol{x}_i(k) = 1, \quad (16)$$

$$\sum_{i=1}^{5} \boldsymbol{u}_i(k) = 1. \quad (17)$$

ここで，Fig. 4 と(15)式の対応づけを Fig. 7 に示す．また，Fig. 7 に示した FSM と(15)式におけるx_iの関係性を Table 3 に示す．(16)式より，FSM の制御ロジックがある状態x_iにあるとき，$x_i = 1$となりその他の状態量の値は 0 となる．例えば，Fig. 7 において制御ロジックが Cylinder1 Drive という状態にあるときには

$$\boldsymbol{x}(k) = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}, \boldsymbol{y}(k) = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}$$

となる．また，センサ情報の状態と入力u_iの関係性を Table 4 に示す．(17)式より，ある入力u_iが印加されたときにはその他の入力は印加されない．例えば，Fig. 7 に Psensor1 が ON になるという入力 $(u_1 = 1)$ が印加されたとき，

$$\boldsymbol{u}(k) = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}$$

となる．また，$\boldsymbol{A}_i$, $\boldsymbol{C}_i$は以下のように与えられる．

$$\boldsymbol{A}_1 = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}, \boldsymbol{A}_2 = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix},$$

$$\boldsymbol{A}_3 = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}, \boldsymbol{A}_4 = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix},$$

$$\boldsymbol{A}_5 = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

$$\boldsymbol{C}_1 = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}, \boldsymbol{C}_2 = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix},$$

$$\boldsymbol{C}_3 = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}, \boldsymbol{C}_4 = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

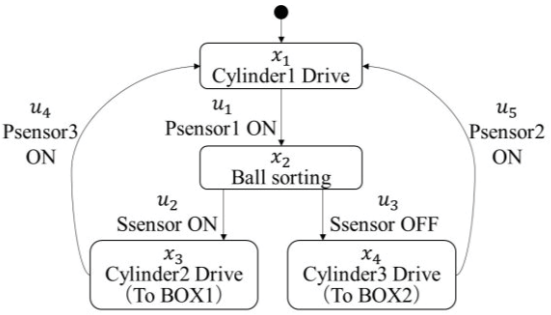

Fig. 7 FSM for MITM detection

Table 3 States definitions in state eq.

State in Fig. 4	Notation in state eq.
Cylinder1 Drive	$x_1 = 1$
Ball sorting	$x_2 = 1$
Cylinder2 Drive	$x_3 = 1$
Cylinder3 Drive	$x_4 = 1$

Table 4 Input definitions for state eq.

Sensor name and status	Notation in state eq.
Psensor1 ON	$u_1 = 1$
Ssensor ON	$u_2 = 1$
Ssensor OFF	$u_3 = 1$
Psensor2 ON	$u_4 = 1$
Psensor3 ON	$u_5 = 1$

Table 5 Ball input sequence

Input sequence	1	2	3	4	5	6	7
Ball	P	G	P	G	P	G	P

$$\boldsymbol{C}_5 = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}.$$

(15)式に対してオブザーバを構成すると，

$$\begin{cases} \tilde{\boldsymbol{x}}(k+1) = \sum_{i=1}^{5} u_i(k)\boldsymbol{A}_i\boldsymbol{x}(k) - \sum_{i=1}^{5} u_i(k)\boldsymbol{K}_i\boldsymbol{e}_y(\\ \tilde{\boldsymbol{y}}(k) = \sum_{i=1}^{5} u_i(k)\boldsymbol{C}_i\tilde{\boldsymbol{x}}(k) \end{cases} \quad (18)$$

となる．オブザーバゲイン$\boldsymbol{K}_i$は(10)式を計算することで求められる．本稿では，(10)式の計算のために YALMIP（パーサ）と SeDuMi（ソルバ）を用いた．計算の結果，$\lambda_{min}(\boldsymbol{Q}_i - \boldsymbol{A}_i^T\boldsymbol{Q}_j\boldsymbol{A}_i)$は以下のように得られた．

$$\lambda_{min}(\boldsymbol{Q}_i - \boldsymbol{A}_i^T\boldsymbol{Q}_j\boldsymbol{A}_i) = 1$$

このとき，(14)式は

$$V(k+1) - V(k) \leq -\|\boldsymbol{e}(k)\|_2^2 \quad (19)$$

となる．ここで，

$$V(k+1) = \sum_{i=1}^{r} u_i(k+1)\boldsymbol{e}^{\mathrm{T}}(k+1)\boldsymbol{Q}_i\,\boldsymbol{e}(k+1) \quad (20)$$

であるが未来の入力$u_i(k+1)$，未来の誤差$\boldsymbol{e}(k+1)$は計測データから得られないので実機実験では以下の式を用いて異常を検出する．

$$V(k) - V(k-1) \leq -\|e(k-1)\|_2^2. \qquad (21)$$

次に，これまで述べてきた中間者攻撃検出手法を実装した縮退運転システムを用いた実機実験を行う．実験環境は 2 章で述べたとおりである．本実験において模擬プラントに投入されたボールの系列を Table 5 に示す．ここで，P は卓球ボール，G はゴルフボールを意味する．本実験は，以下のように行う．

(i) 中間者攻撃を発生させずにボールの仕分けを行わせる．

(ii) 模擬プラント稼働中($k = 8$)に中間者攻撃を発生させる．

実験(i)における(21)式のプロットを Fig. 8 に，推定状態量の遷移を Fig. 10 に示す．また，実験(ii)における(21)式のプロットを Fig. 9 に推定状態量の遷移を Fig. 11 に示す．Fig. 10, Fig. 11 では，$D = 1\ (= 0)$となったとき中間者攻撃が検出された（検出されていない）ことを意味し，$F = 1\ (= 0)$のとき縮退運転を行っている（行っていない）ことを意味する．さらに，kはステップ数，tは実時間で単位は秒である．

Fig. 8 より，実験(i)では全てのステップで$V(k) - V(k-1) = -\|e(k-1)\|_2^2 = 0$ という結果が得られた．この結果は，(21)式の範囲を逸脱していない．したがって，中間者攻撃による異常は検出されなかったということになる．一方で，Fig. 9 より実験(ii)では$k = 11$から(21)式の範囲を逸脱していることが確認できる．ここで，中間者攻撃による異常が検出されていることがわかる．これは，Fig. 11 でも確認出来る．推定状態量の遷移は$k = 9, 10, 11$で$\hat{x}_1 \rightarrow \hat{x}_2 \rightarrow \hat{x}_1$となっておりBOX1，BOX2 いずれにもボールが送られていない．これは，玉詰まりが発生していることを意味する．その後，$k = 11$における(21)式の逸脱後自動的に縮退運転へと切り替えられ玉詰まりが解消されていることがわかる．このとき推定状態量の遷移は$k = 11, 12, 13$で$\hat{x}_1 \rightarrow \hat{x}_2 \rightarrow \hat{x}_3$となっておりボールは BOX1 へ送られていることがわかる．以降，ボールの種類に関わらず推定状態量の遷移は$\hat{x}_1 \rightarrow \hat{x}_2 \rightarrow \hat{x}_3$となりボールは常に BOX1 へ送られていることが確認出来る．

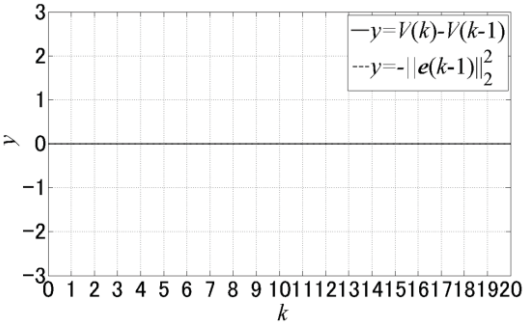

Fig. 8 Varination of Error without MITM

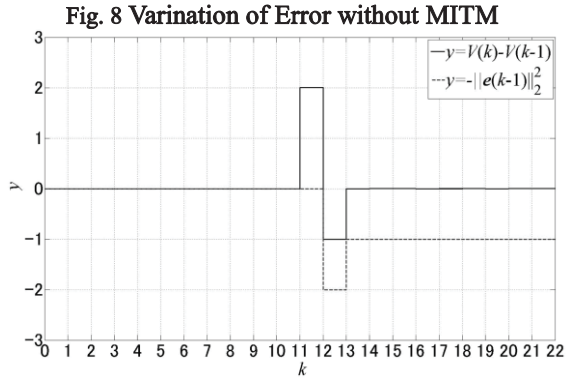

Fig. 9 Varination of Error with MITM

6. おわりに

本稿では，有限状態機械を用いたモデルベース縮退運転を実現した．一方，縮退運転から通常運転への復帰は未だ実現されていない．今後は，縮退運転から通常運転への復帰方法を考える．たとえば，復帰に必要な機能とその実装方法である．

また，異なるモデリング手法を用いた縮退運転システムについて比較を行う．比較の対象として，中間者攻撃検出速度，コードの容量，MATLAB/Simulink で必要となる Toolbox の数などが挙げられる．

[参考文献]

[1] 内藤 辰彦, 渡辺 紀：産業用イーサネット入門, CQ 出版社 (2009)

[2] S. Zhioua: The Middle East under Malware Attack Dissectiong Cyber Weapons, International Conference on Distributed Computing Systems Workshops (2013)

[3] http://www.trendmicro.com/vinfo/us/threat-encyclopedia/web-attack/139/havex-targets-industrial-control-systems

[4] M. Krotofil, A. A. Càrenas, B. Manning , J. Larsen,: CPS:Driving Cyber-Physical Systems to Unsafe Operating Conditions by Timing DoS Attacks on Sensor Signals, ACSAC'14 Proceedings of the 30th Annual Computer Security Applications Conference pp. 146-155 (2014)

[5] 柚木 祥慈, 大倉 敬規：制御システムの動作モードに基づいたネットワーク振舞異常検知方式, 電気学会論文誌 C（電子・情報・システム部門誌）, Vol.134, No.10, pp.1492-1497 (2014)

[6] 米国アイダホ国立研究所：制御システムのサイバーセキュリティ多層防御戦略（一般社団法人 JPCERT コーディネーションセンター訳）(2006)

[7] http://itpro.nikkeibp.co.jp/article/COLUMN/20120605/400489/

[8] http://canon-its.jp/eset/malware_info/term/a/005.html

[9] http://techon.nikkeibp.co.jp/article/WORD/20060419/116350/?rt=nocnt

[10] http://www.arduino.cc/

[11] http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/basic/risk/11.html

[12] K. Sawada, T. Sasaki, S. Shin, and S. Hosokawa, “A Fallback Control Study of Networked Control Systems for Cybersecurity,” 10th Asian Control Conference (ASCC’15), pp.88-94 (2015).

[13] 猪飼 武夫, 益本 晶幸, 福永 邦雄, 有限オートマトンの可到達性, 可観測性および最小実現, 電子情報通信学会技術研究報告. COMP, コンピュテーション, Vol. 95, No. 374, pp. 45-54 (1995)

[14] 蛯原 義雄：LMI によるシステム制御, 森北出版株式会社 (2012)

[15] J. Daafouz, P. Riedinger ,and C. Iung, “Stability analysis and control synthesis for switched systems: a switched Lyapunov function approach, ” Trans. Automatic Control,vol. 47, no. 11, pp. 1883-1887 (2002)

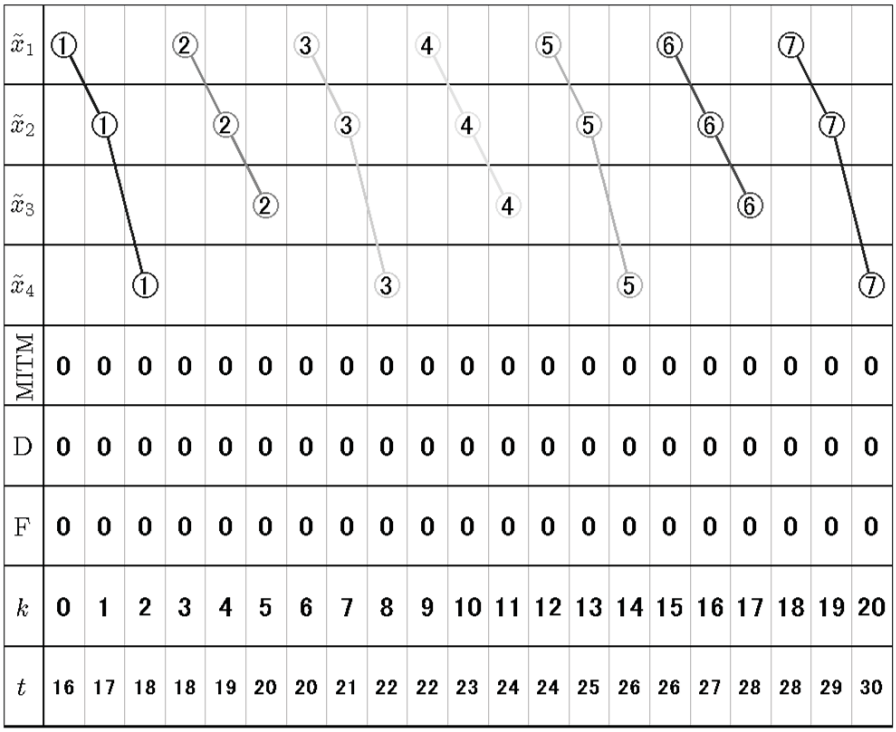

Fig. 10 State transition of the simulated plant without MITM

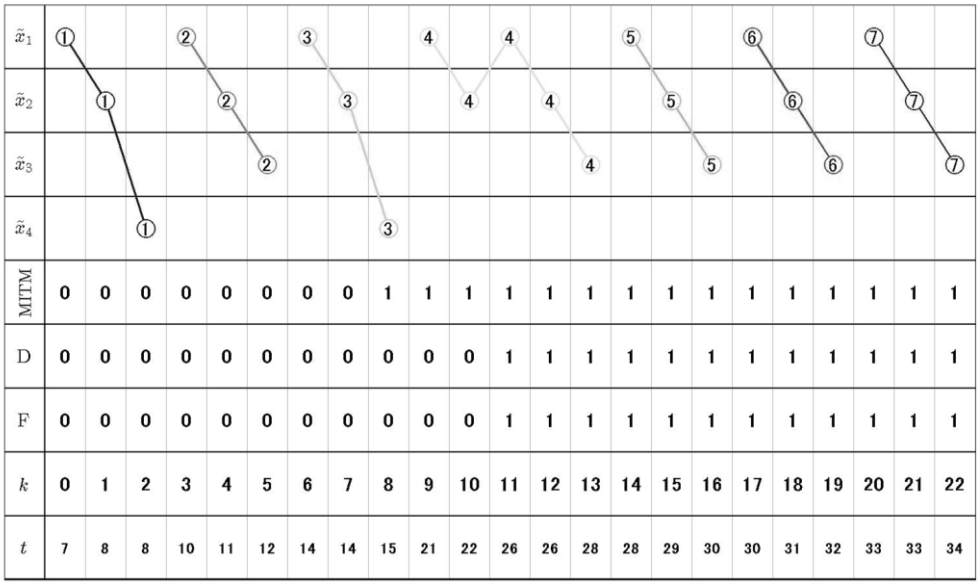

Fig. 11 State transition of the simulated plant with MITM