サイバー攻撃に頑強な制御通信システムの開発

研究代表者　　若　生　将　史　　神戸大学大学院システム情報学研究科　講師

1 はじめに

コンピュータやネットワーク技術の発展に伴い，現代社会においてサイバーフィジカルシステムが数多く見られるようになってきた．サイバー要素とフィジカル要素を組み合わせることによって，構成上様々な自由度が得られるものの，サイバー要素を通じてフィジカル要素に破壊工作が仕掛けられる深刻なリスクも生じるようになった．例えば，近年自動車[1]やドローン[2]などがサイバー攻撃にさらされうることが指摘されている．また，インフラ設備もサイバー攻撃の被害に遭っている．２０００年３月にオーストラリアの下水処理設備を，２０００年６月にイランの核燃料施設のウラン濃縮用遠心分離機を標的として，サイバー攻撃が実施された[3,4]．２０１４年にドイツの製鉄設備がサイバー攻撃を受け，制御不可能になったことが報告されている[5]．

以前の制御システムは独自のプロトコルを採用し，情報システムから独立していた．しかし，生産性の向上や開発コストの削減のために，近年は汎用的なプロトコルを用いてネットワークに接続されるようになった．これらの事情により，これまでは情報システムのみを対象としていたサイバー攻撃のリスクが制御通信システムに範囲を広げている．制御通信システムがサイバー攻撃の対象になると，操業停止やライフラインの破壊など深刻な被害を受け，人命が失われる可能性さえある．そのため，世界各国で制御通信システムに対するセキュリティの強化が緊急の課題になっている．

情報システムと異なり，制御通信システムは２４時間３６５日フル稼働することが要求されるため，セキュリティアップデートがリリースされたとしても即座に適用することができない．また制御システムの責任部署である設備管理部門は，安全性や生産効率性が重要視されるために，情報システム部門に比べてサイバーセキュリティに対する意識レベルが低く，持ち込んだ USB メモリやメール中のマルウェアによって不正侵入を許してしまうことが多い．このような背景のために，本質的にサイバー攻撃の被害を受けやすい制御通信システムでは，サイバー攻撃を受けた際に，いかに早くそれを検出できるか，そして正常な運転へ移行する間でも安全性を担保して稼働できるかが重要になる．この点は，機密情報の漏洩防止がその主目的である情報システムのセキュリティ・プライバシーと大きく異なっている．また，情報システムで利用される暗号化などのセキュリティ技術はリアルタイムでの応答性が悪く，操作スピードが要求される制御通信システムでは実現できないことも多い．

本稿では,離散事象システムを制御対象とし,サイバー攻撃に頑強なスーパーバイザ制御について述べる．離散事象システムとは，離散の状態空間と事象駆動の遷移構造をもつ動的システムのことである．このようなモデルは化学プラント[6]，電力網[7]，生産システム[8]などのサイバーフィジカルシステムを記述する際に広く用いられている．本稿の目的は，以下の問に答えることである：攻撃者が観測データの一部を改ざんできるときに，どのように離散事象システムを制御すればよいのか？

図１は本稿で考える閉ループシステムを示している．この閉ループシステムのおいて，プラントで生成された観測文字列が悪意ある攻撃によって別の文字列に改ざんされる，という状況を考える．この攻撃は，文字を付け加えたり，除去したり，取り換えることによって，元の文字列を改ざんするとする．さらに，非決定的に文字列を改ざんする，つまり，同じ文字列であっても，異なる文字列に改ざんすることが可能であるとする．さらに，一般に，制御系であるスーパーバイザを設計する段階では，どのように攻撃者が文字列を改ざんするかわからないため，考えうるすべての攻撃を考慮しなければならない．本稿で考える問題は，このようなサイバー攻撃のもとでも制御仕様を達成するスーパーバイザが存在するかどうかをいかに決定するかという問題である．これは，センサに対するサイバー攻撃のもとでの線形時不変システムの状態推定問題[9–11]の，離散事象システムにおける問題とみなすことができる．

離散事象システムのスーパーバイザ制御において，モデルの不確かさやプラントの故障を取り扱う研究は広く行われてきている[12–17]．これらの研究もサイバー攻撃に対する対応策として利用できるものの，不確かさや故障とサイバー攻撃の間には大きな違いが存在する．実際，不確かさや故障は悪意をもって連動することはないものの，サイバー攻撃では，攻撃者の目的を達成するように臨機応変に攻撃が行われる可能性がある．例えば，ステルス攻撃は，制御サイドによって検出されることなく情報を改ざんし，システムの破壊・停止や性能悪化を引き起こすことを目的としている[18, 19]．そのため，サイバー攻撃の下でのスーパーバイザ制御のための新しい枠組みが必要になる．

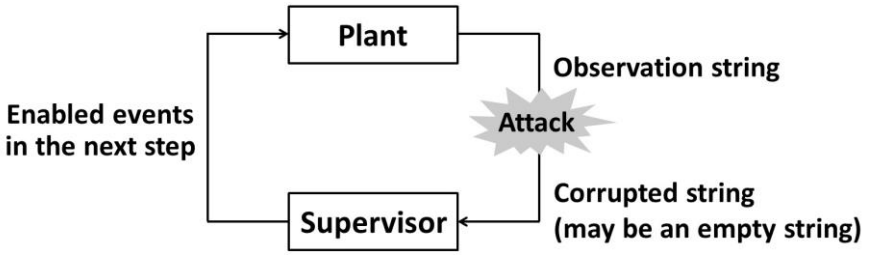

図１：閉ループシステム

これまでに離散事象システムにおいていくつかのセキュリティ技術が考案されてきた．そのうちの一つが opacity と呼ばれるものである．離散事象システムが opacity をもつとは，外部の攻撃者にとってシステムの秘匿情報が不確かであることをいう．詳細は文献[20–23]を参照していただきたい．また離散事象システムの枠組みで侵入検知の研究も行われている[24–27]．これらのセキュリティ技術はシステムの秘匿性や完全性を保証できるが．依然としてサイバー攻撃に対して頑強なスーパーバイザ制御の研究は行われていない．

サイバー攻撃を受ける可能性があるプラントは非決定的な観測を持つ離散事象システムとしてモデル化することが可能である．そのような離散事象システムに対するスーパーバイザ制御は文献[28, 29]で研究されてきた．これらの先行研究と本研究の問題設定の違いは，サイバー攻撃によって変更された文字列，つまり非決定的な観測関数が不確かであるという点である．いいかえると，攻撃A_iのもとでのプラントをモデル化することで得られる離散事象システムをG_{A_i}とすると，本稿で考える問題は，取りうるモデルの集合が$\{G_{A_1}, \dots, G_{A_n}\}$であるような不確かな離散事象システムを対象とするロバストなスーパーバイザ制御問題とみなすことができる．ここで，$\{G_{A_1}, \dots, G_{A_n}\}$の各々の要素は潜在的なサイバー攻撃のタイプを表している．

本稿では，まずサイバー攻撃を数学的に定義した後，サイバー攻撃のもとでの可観測性の概念を新しく導入する．これは従来の（サイバー攻撃を考慮しない）可観測性[30, 31]の自然な拡張になっている．そしてサイバー攻撃の下でも所望の制御仕様を達成するスーパーバイザが存在するための必要十分条件が，その仕様が可制御でかつサイバー攻撃の下で可観測であるということを示す．さらに，文字の付加・除去を行う任意のサイバー攻撃を考えた際に，新しい可観測性が従来の可観測性に帰着できることを示す．

2 記法と定義

以下の記法と定義は離散事象システムの文献[33, 34]における一般的なものである．

有限の事象集合Σに対して，Σ^*を空列εを含む，Σの要素からなる有限長のすべての事象の集合とする．言語$L \subset \Sigma^*$に対して，Lの要素のすべての接頭語からなる集合を$\overline{L}$で表す．そしてLが$L = \overline{L}$をみたすとき，（接頭語について）閉じているという．

事象集合Σが$\Sigma = \Sigma_c \cup \Sigma_u$のように２種類の集合に分割されているとする．ここで，Σ_cは可制御な事象の集合であり，Σ_uは不可制御な事象の集合である．言語$L \subset \Sigma^*$に対して，閉じている言語$K \subset L$が可制御であるとは，

$$K\Sigma_u \cap L \subset K$$

が成り立つことをいう．

事象が生成した際に観測される文字からなる集合をΔとする．そして，Σの属する各事象にΔの要素あるいは空列εを割り当てる写像をPとする．この観測写像は定義域をΣからΣ^*へと帰納的に拡張することができる：

$$P(\varepsilon) = \varepsilon, \qquad P(ws) = P(w)P(s), \qquad \forall w \in \Sigma^*, s \in \Sigma.$$

閉じている言語$K \subset L$がLに関して可観測であるとは，

$$\ker P \subset \mathrm{act}(K, L)$$

であることをいう．ここで，$\ker P$はΣ^*上の同値関係を表し，

$$\ker P \coloneqq \{(w, w') \in \Sigma^* \times \Sigma^* : P(w) = P(w')\}$$

で定義される．また$\mathrm{act}(K, L)$はΣ^*上の二項関係を表し，組(w, w')が$(w, w') \in \mathrm{act}(K, L)$をみたすとは，

$$w, w' \in K$$

が成り立つときに，

$$ws \in K, w's \in L \setminus K$$

あるいは

$$w's \in K, ws \in L \setminus K$$

をみたす$s \in \Sigma$が存在しないことをいう．もし，背景となるLが明らかなときは，省略して表す．

次にオートマトン$G = (X, \Sigma, z, x_0)$を考える．ここでXは状態の集合，Σは空でない事象集合，zは$X \times \Sigma \to X$の遷移写像，$x_0 \in X$は初期状態とする．そして，$z(x, s)!$を$z(x, s)$が定義されていることを示す記号とする．遷移写像zは写像$X \times \Sigma^* \to X$へと以下のようにして拡張することができる：

- すべての$x \in X$に対して，$z(x, \varepsilon) \coloneqq x$
- すべての$x \in X$，$w \in \Sigma^*$，$s \in \Sigma$に対して

$$z(x, ws) = \begin{cases} z(z(x, w), s), & z(x, w)! \text{ and } z(z(x, w), s)! \\ \text{undefined}, & \text{otherwise} \end{cases}$$

また，オートマトンGによって生成される言語を$L(G)$とする．すなわち，

$$L(G) = \{w \in \Sigma^* : z(x_0, w)!\}$$

である．

3 サイバー攻撃を考慮した離散事象システムのスーパーバイザ制御

本節では，まず 3.1 節で観測される文字に対するサイバー攻撃と，そのようなサイバー攻撃の下での可観測性に関する新しい概念を提案する．次に 3.2 節で本稿の主結果，すなわち，サイバー攻撃の存在下で所望の制御仕様をみたすためのスーパーバイザが存在するための必要十分条件を述べる．3.3 節ではサイバー攻撃として文字の付加・除去に焦点を当てる．そして，このサイバー攻撃のもとでの可観測性が，従来の（サイバー攻撃を受けていないシステムの）可観測性に帰着させることができることを述べる．

3-1 サイバー攻撃の下での可観測性

本稿では，離散事象システムに対するサイバー攻撃を，プラントによって生成される観測文字列$w \in \Delta^*$を別の文字列$y \in \Delta^*$に改ざんすることとして定義する．この改ざんされた文字列yは，元の文字列wにある文字を追加したり，あるいは除去・取り換えることによって得られるものとする．もっとも単純な攻撃は，Δ^*からΔ^*の関数$y = A(w)$として定義される．しかし，本稿では，より一般的なサイバー攻撃として，攻撃者が非決定的に元の同じ文字列$w \in \Delta^*$を別の文字列$y_1 \in \Delta^*$，$y_2 \in \Delta^*$に改ざんできると仮定する．これにより，スーパーバイザの制御仕様をみたすことは一層難しくなる．まとめると，本稿では，サイバー攻撃を集合値関数として定義する．つまり$A\colon \Delta^* \to 2^{\Delta^*}$であり，元の観測文字列$w \in \Delta^*$を，改ざん後の文字列$y$全体からなる集合集合$A(w) \subset \Delta^*$に移す関数である．このとき，スーパーバイザは集合$A(w)$のうち 1 つの文字列だけを受け取る．また，各々の$w \in \Delta^*$を集合$\{w\}$にうつす攻撃写像A_{id}はサイバー攻撃を一切行わない写像とみなすことができる．

スーパーバイザを設計する際にどのセンサが攻撃されるか明らかでないため，攻撃写像は一般には不確かであるといえる．そのため，本稿では実行されうるサイバー攻撃からなる集合$\Omega = \{A_1, \dots A_n\}$を考え，以下の状況でのスーパーバイザ制御問題を対象とする．：サイバー攻撃の集合Ωは既知であり，そのうちの 1 つのサイバー攻撃が実行されるとする．いいかえると，攻撃者は集合Ωのサイバー攻撃を適宜切り替えることはできないとする．しかし，スーパーバイザを設計するときにはどの攻撃が実際に実行されるかわからないため，集合Ωのすべての攻撃に関してロバストなスーパーバイザを設計することが目的である．

例１：図２のオートマトンGによって生成される言語を$L(G)$とする．そして，図３のオートマトンG_Kによって生成される仕様言語$K = L(G_K)$の可観測性について今後議論していく．オートマトンGとG_Kの違いは，状態x_1からx_3への事象cの有無である．つまり，今回のスーパーバイザ制御の目的はこの「ショートカット」を防ぐことである．また観測写像Pを

$$P(s) = \begin{cases} s, & \text{if } s \in \Delta \coloneqq \{a, b, d\} \\ \varepsilon, & \text{otherwise} \end{cases}$$

とし，３種類のサイバー攻撃A_1, A_2, A_3を，

$$A_1(s) = \Delta$$
$$A_2(a) = \{a, b\}, \quad A_2(b) = \{b\}, \quad A_2(d) = \{a, d\}$$
$$A_3(a) = \{a\}, \quad A_3(b) = \{b\}, \quad A_3(d) = \{\varepsilon\}$$

で定義する．すなわち，A_1は任意に観測文字を入れ替える攻撃であり，スーパーバイザは可観測な事象が起きたことだけを観測データから知ることができる．また攻撃A_2は文字aをbに，文字dをaにそれぞれ入れ替える攻撃である．攻撃A_3は常に文字dを除去する攻撃とみなすことができる．スーパーバイザはこれらのサイバー攻撃のうち，どの攻撃が実際に実行されるかわからないという状況下で，制御仕様であるG_K（が生成する言語K）を達成しなければならない．そのようなスーパーバイザが存在するかどうかについて，主要結果を述べたあとに再び議論する．

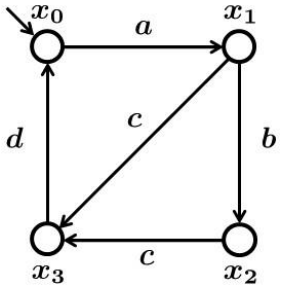

図２：オートマトンG

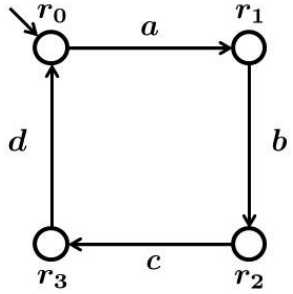

図３:オートマトンG_K

記法の単純化のため，$AP\colon \Delta^* \to 2^{\Delta^*}$を$A$と$P$の合成関数によって得られる関数とする．すなわち$AP$は攻撃された観測写像である．以下で攻撃集合の下での可観測性を定義する．この定義は，従来の可観測性の自然な拡張とみなすことができる．

定義２（サイバー攻撃の下での可観測性）：攻撃集合Ωに対して，閉じている言語$K \subset L$が攻撃集合Ωのもとで可観測であるとは，

$$R_{A,A'} \subset \mathrm{act}(K, L) \quad \forall A, A' \in \Omega \tag{1}$$

が成り立つことをいう．ここで，関係$R_{A,A'}$は攻撃された観測写像APと$A'P$を通すことで同じ出力文字列が得られる文字列の集合，つまり，

$$R_{A,A'} \coloneqq \{(w, w') \in \Sigma^* \times \Sigma^* \colon AP(w) \cap A'P(w) \neq \emptyset\}$$

である．また，(1)の定義は，以下のように書き直すこともできる：「すべての$w, w' \in K$に対して，

$$AP(w) \cap A'P(w) \neq \emptyset$$

をみたす$A, A' \in \Omega$が存在するならば，

$$ws \in K, \quad w's \in L \setminus K$$

あるいは

$$w's \in K, \quad ws \in L \setminus K$$

をみたす$s \in \Sigma$が存在しない」，あるいは「すべての$w, w' \in K$に対して，

$$AP(w) \cap A'P(w) \neq \emptyset$$

をみたす$A, A' \in \Omega$が存在するならば，任意の$s \in \Sigma$に対して

$$ws \notin L \ \text{ or } \ w's \notin L \ \text{ or } \ ws, w's \in K \ \text{ or } \ ws, w's \in L \setminus K$$

が成り立つ」．すなわち，サイバー攻撃の下での可観測性とは，$(w, w') \notin \mathrm{act}(K, L)$，つまり２つの文字列$w, w' \in K$のうち一方が制御仕様$K$に含まれるがもう一方は$K$に含まれないような組に対して，同じ観測データが得られるサイバー攻撃$A, A' \in \Omega$が存在しないことを意味する．

次の命題は，可制御な言語に対してサイバー攻撃のもとでの可観測性と等価な条件を与えるものである．サイバー攻撃が行われない場合，得られた条件は書籍[34]などで従来の可観測性の定義として用いられている．

命題３：閉じている言語$K \subset L$が可制御であるとする．このとき，Kが攻撃集合Ωのもとで可観測であるための必要十分条件は，すべての$w, w' \in K$，$s \in \Sigma_c$，$A, A' \in \Omega$に対して以下の条件が成り立つことである：

$$AP(w) \cap A'P(w) \neq \emptyset, \quad ws \in K, \quad w's \in L \qquad \Longrightarrow \qquad w's \in K.$$

例１（続き）：例１の言語$L(G)$，仕様言語$K = L(G_K)$，サイバー攻撃A_1, A_2, A_3を考える．可制御な事象集合が$\Sigma_c = \{a, c\}$，不可制御な事象集合が$\Sigma_d = \{b, d\}$で与えられるとする．明らかにKは可制御であり，さらに命題３よりKが攻撃集合$\Omega = \{A_1\}$のもとで可観測であることがわかる．一方，Kは攻撃集合$\Omega = \{A_2\}$，$\Omega = \{A_3\}$のもとで可観測であるが，$\Omega = \{A_2, A_3\}$のもとでは不可観測である．実際，もし

$$w = abcda, \qquad w' = wb$$

としたとき，

$$A_2P(w) = \{abaa, abab, abda, abdb, bbaa, bbab, bbda, bbdb\}$$
$$A_3P(w') = \{abab\}$$

であるため，

$$A_2P(w) \cap A_3P(w') \neq \emptyset$$

であるが，$c \in \Sigma_c$は

$$wc \in L \setminus K \quad \text{and} \quad w'c \in K$$

をみたす．そのため，Kは文字の入れ替えに関してはロバストであるが，入れ替えと除去の組み合わせに関しては脆弱であることがわかる．

3-2 スーパーバイザの存在条件

出力された文字列が改ざんされた状況下で制御仕様をみたすスーパーバイザが存在するための必要十分条件を述べる．そのためにまず，サイバー攻撃の下でのスーパーバイザと制御言語を定義する．

言語Lと攻撃集合Ωに対するスーパーバイザを

$$f: \bigcup_{A \in \Omega} AP(L) \to 2^{\Sigma}$$

とする．ここで，$AP(L)$はサイバー攻撃Aのもとで出力される文字列の集合，つまり，

$$AP(L) \coloneqq \{y \in \Delta^*: \ \exists w \in L \quad \text{s.t.} \quad y \in AP(w)\}$$

である．そして，スーパーバイザfが有効であるとは，

$$f(w) \supset \Sigma_u \qquad \forall w \in \bigcup_{A \in \Omega} AP(L)$$

であることをいう．

また言語Lと攻撃集合Ωに対するスーパーバイザfが与えられたとき，攻撃$A \in \Omega$のもとでfによって制御される最大言語$L_{f,A}^{\max}$を次のように帰納的に定義する：$\varepsilon \in L_{f,A}^{\max}$かつ

$$ws \in L_{f,A}^{\max} \quad \Leftrightarrow \quad w \in L_{f,A}^{\max} \ \text{ and } \ ws \in L \ \text{ and } \ \exists y \in AP(w) \ \text{ s.t. } \ s \in f(y).$$

そして，攻撃$A \in \Omega$のもとでfによって制御される最小言語$L_{f,A}^{\min}$を次のように帰納的に定義する：$\varepsilon \in L_{f,A}^{\min}$かつ

$$ws \in L_{f,A}^{\min} \quad \Leftrightarrow \quad w \in L_{f,A}^{\min} \ \text{ and } \ ws \in L \ \text{ and } \ \forall y \in AP(w), s \in f(y).$$

一般に，$L_{f,A}^{\min} \subset L_{f,A}^{\max}$ではあるが，サイバー攻撃が行われない場合，つまり，$A = A_{\mathrm{id}}$の場合には，これらの言語は一致する．また，定義より$L_{f,A}^{\max}$と$L_{f,A}^{\min}$はどちらも閉じている．

システム論的な解釈としては，$L_{f,A}^{\max}$はサイバー攻撃Aがスーパーバイザfに対して適切に出力情報を改ざんして得られる最大の言語であるとみなすことができる．一方，$L_{f,A}^{\min}$はサイバー攻撃Aが実行できる最小の言語である．つまり，サイバー攻撃Aはいかなるように出力情報を改ざんしても$L_{f,A}^{\min}$に含まれるどの言語も取り除

くことができない.
以下の結果は，攻撃集合Ωに属するすべての攻撃に対して最小言語と最大言語がどちらも制御仕様となるようなスーパーバイザが存在するための必要十分条件を与える：

定理４：任意の空でない閉じている言語$K \subset L$と攻撃集合Ωに関して以下が成り立つ：

①任意の$A \in \Omega$ に対して$L_{f,A}^{\min} = L_{f,A}^{\max} = K$が成り立つ有効なスーパーバイザ$f$が存在するための必要十分条件は，$K$が可制御かつΩのもとで可観測であることである.
②もし，Kが可制御かつΩのもとで可観測であるならば，次の写像

$$f: \bigcup_{A\in\Omega} AP(L) \to 2^{\Sigma}$$

は任意の$A \in \Omega$ に対して$L_{f,A}^{\min} = L_{f,A}^{\max} = K$をみたす有効なスーパーバイザである：

$$f(y) \coloneqq \Sigma_u \cup \{s \in \Sigma_c : \exists w \in K, A \in \Omega \text{ s.t. } y \in AP(w) \text{ and } ws \in K\} \qquad \forall y \in \bigcup_{A\in\Omega} AP(L).$$

【証明】文献[35]を参照のこと.

3-3 文字の付加・除去によるサイバー攻撃のもとでの可観測性

本節では，出力される文字列からある文字を付加・除去するサイバー攻撃を考える．そして従来の（攻撃を受けていない場合の）可観測性に，攻撃のもとでの可観測性を帰着させる.

観測される文字の集合$p \subset \Delta$に対して，付加・除去を行う攻撃A_p: $\Delta^* \to 2^{\Delta^*}$を次のように定義する：文字列$u \in \Delta^*$から$p$に含まれる文字を任意の回数だけ付加・除去して得られる文字列$v \in \Delta^*$の集合へと，もとの文字列uを移す写像．このような攻撃A_pはpに含まれる文字に関する攻撃といえる．また，pを除去する観測写像

$$R_p: \Delta \to (\Delta \cup \{\varepsilon\})$$

を

$$R_p(t) = \begin{cases} \varepsilon, & t \in p \\ t, & t \notin p \end{cases}$$

で定義する．観測写像Pと同様，R_pも文字列についての関数へと帰納的に拡張することができる．そして，このpを除去する観測写像R_pを用いることで攻撃A_pを次のように定義できる：

$$A_p(u) = \{v \in \Delta^* : R_p(u) = R_p(v)\}.$$

例６：文字集合pを$p = \{s\} \subset \{s, t\} = \Delta$とする．このとき，$R_p(st) = t$であるので,

$$A_p(st) = \{s^n t s^m : n, m \geq 0\} = \{v \in \Delta^* : R_p(st) = R_p(v)\}$$

が成り立つ.

次の結果は，定義２で述べた，付加・除去による攻撃の下での可観測性が，ある観測写像の集合に対する従来の可観測性と等価であることを示している．ここで，合成写像$R_p \circ P: \Delta \to (\Delta \cup \{\varepsilon\})$は従来の意味での観測写像となっていることに注意してほしい.

定理７：すべての空でない閉じている言語$K \subset L$と付加・除去による攻撃集合$\Omega = \{A_{p_1}, \dots, A_{p_M}\}$に対して，$K$が攻撃集合Ωのもとで可観測であるための必要十分条件は，集合

$$p \coloneqq p_i \cup p_j \qquad \forall i, j \in \{1,2, \dots, M\}$$

によって特徴づけられるすべての観測写像$R_p \circ P$に関してKが可観測であることである.
【証明】文献[35]を参照のこと.

定理７によって，攻撃を考慮しない従来の可観測性を判定するための手法[32]を用いて，付加・除去による攻撃の下での可観測性を判定することができる.
有限オートマトン$G = (X, \Sigma, z, x_0)$によって生成される言語$L = L(G)$と，同じく有限オートマトン$G_K =$

$(R, \Sigma, \varsigma, r_0)$によって生成される仕様言語$K = L(G_K)$を考える．定理７によって，付加・除去による攻撃集合Ωのもとでの可観測性を判定するためには，$|\Omega|^2$個のテストオートマトン（各々が通常の可観測性を判定するためのもとである）を構築すればよい．このテストオートマトンによって通常の可観測性を判定するために必要な計算複雑さは

$$O(|X| \cdot |R|^2 \cdot |\Sigma_c|)$$

であるので[34]，サイバー攻撃の下での可観測性を判定するための計算複雑さは

$$O(|X| \cdot |R|^2 \cdot |\Sigma_c| \cdot |\Omega|^2)$$

であることがわかる．

４ 結論

本稿では，サイバー攻撃下での離散事象システムのスーパーバイザ制御を考えた．サイバー攻撃の下での可観測性の新しい概念を定義し，それと従来の可制御性を組み合わせたものが，攻撃の下で仕様言語を実行するスーパーバイザが存在することの必要十分条件になっていることを述べた．そして従来の可観測性の概念を利用して，付加・除去によるサイバー攻撃のもとでの可観測性を判定できることを示した．このほかにも，例えば，文字の交換・除去によるサイバー攻撃のもとでのスーパーバイザのオートマン表現や可観測性の判定条件について文献[35]で述べている．今後の課題として，離散事象システムのスーパーバイザ制御における秘匿性とサイバー攻撃に対するロバスト性を同時に考慮することが挙げられる．

【参考文献】

[1] S. Checkoway, D. McCoy, B. Kantor, D. Anderson, Shacham, S. H. Savage, K. Kocher, A. Czeskis, F. Roesner, and T. Kohno, “Comprehensive experimental analyses of automotive attack surfaces,” in *Proc. USENIX Security Symposium*, 2011.

[2] A. J. Kerns, D. P. Shepard, J. A. Bhatti, and T. E. Humphreys, “Unmanned aircraft capture and control via GPS spoofing,” *J. Field Robot.*, vol. 31, pp. 617–636, 2014.

[3] J. Slay and M. Miller, “Lessons learned from the Maroochy water breach,” in *Proc. Critical Infrastructure Protection*, vol. 253, 2007, pp. 73–82.

[4] J. P. Farwell and R. Rohozinski, “Stuxnet and the future of cyber war,” *Survival*, vol. 53, pp. 23–40, 2011.

[5] T. De Maiziere, “Die Lage der IT-Sicherheit in Deutschland 2014,” Tech. Report, Federal Office for Information Security, 2014. [Online]. Available: http://www.wired.com/wp-content/uploads/2015/01/Lagebericht2014.pdf

[6] P. Falkman, B. Lennartson, and M. Tittus, “Specification of a batch plant using process algebra and petri nets,” *Control Eng. Practice*, vol. 17, pp. 1004–1015, 2009.

[7] X. Zhao, P. Shi, and L. Zhang, “Asynchronously switched control of a class of slowly switched linear systems,” *Systems Control Lett.*, vol. 61, pp. 1151–1156, 2012.

[8] M. Uzam and G. Gelen, “The real-time supervisory control of an experimental manufacturing system based on a hybrid method,” *Control Eng. Practice*, vol. 17, pp. 1174–1189, 2009.

[9] H. Fawzi, P. Tabuada, and S. Diggavi, “Secure estimation and control for cyber-physical systems under adversarial attacks,” *IEEE Trans. Automat. Control*, vol. 59, pp. 1454–1467, 2014.

[10] Y. Shoukry and P. Tabuada, “Event-triggered state observers for sparse noise/attacks,” *IEEE Trans. Automat. Control*, vol. 61, pp. 2079–2091, 2016.

[11] M. S. Chong, M. Wakaiki, and J. P. Hespanha, “Observability of linear systems under adversarial attacks,” in *Proc. ACC’15*, 2015.

[12] F. Lin, "Robust and adaptive supervisory control of discrete event systems," *IEEE Trans. Automat. Control*, vol. 38, pp. 1848–1852, 1993.
[13] S. Takai, "Robust supervisory control of a class of timed discrete event systems under partial observation," *Systems Control Lett.*, vol. 39, pp. 267–273, 2000.
[14] A. Saboori and S. H. Zad, "Robust nonblocking supervisory control of discrete-event systems under partial observation," *Systems Control Lett.*, vol. 55, pp. 839–848, 2006.
[15] A. M. S´anchez and F. J. Montoya, "Safe supervisory control under observability failure," *Discrete Event Dyn. System: Theory Appl.*, vol. 16, pp. 493–525, 2006.
[16] A. Paoli, M. Sartini, and S. Lafortune, "Active fault tolerant control of discrete event systems using online diagnostics," *Automatica*, vol. 47, pp. 639–649, 2011.
[17] S. Shu and F. Lin, "Fault-tolerant control for safety of discrete-event systems," *IEEE Trans. Autom. Sci. Eng.*, vol. 11, pp. 78–89, 2014.
[18] S. Amin, X. Litrico, S. Sastry, and A. M. Bayen, "Cyber security of water SCADA systems–Part I: Analysis and experimentation of stealthy deception attacks," *IEEE Trans. Control Systems Tech.*, vol. 21, pp. 1963–1970, 2013.
[19] A. Teixeira, H. Shames, I. Sandberg, and K. H. Johansson, "A secure control framework for resource-limited adversaries," *Automatica*, vol. 51, pp. 135–148, 2015.
[20] S. Takai and Y. Oka, "A formula for the supremal controllable and opaque sublanguage arising in supervisory control," *SICE J Control Meas. System Integr.*, vol. 1, pp. 307–311, 2008.
[21] J. Dubreil, P. Darondeau, and H. Marchand, "Supervisory control for opacity," *IEEE Trans. Automat. Control*, vol. 55, pp. 1089–1100, 2010.
[22] A. Saboori and C. N. Hadjicostis, "Opacity-enforcing supervisory strategies via state estimator constructions," *IEEE Trans. Automat. Control*, vol. 57, pp. 1155–1165, 2012.
[23] Y.-C. Wu and S. Lafortune, "Synthsis of insertion functions for enforcement of opacity security properties," *Automatica*, vol. 50, pp. 1336–1348, 2014.
[24] D. Thorsley and D. Teneketzis, "Intrusion detection in controlled discrete event systems," in *Proc. 45th IEEE CDC*, 2006.
[25] S.-J. Whittaker, M. Zulkernine, and K. Rudie, "Toward incorporating discrete-event systems in secure software develop-
ment," in *Proc. ARES'08*, 2008.
[26] N. Hubballi, S. Biswas, S. Roopa, R. Ratti, and S. Nandi, "LAN attack detection using discrete event systems," *ISA Trans.*,
vol. 50, pp. 119–130, 2011.
[27] L. K. Carvalho, Y.-C. Wu, R. Kwong, and S. Lafortune, "Detection and prevention of actuator enablement attacks in
supervisory control systems," in *Proc. WODES'16*, 2016.
[28] S. Xu and R. Kumar, "Discrete event control under nondeterministic partial observation," in *Proc. IEEE CASE'09*, 2009.
[29] T. Ushio and S. Takai, "Nonblocking supervisory control of discrete event systems modeled by Mealy automata with nondeterministic output functions," *IEEE Trans. Automat. Control*, vol. 61, pp. 799–804, 2016.
[30] R. Cieslak, C. Desclaux, A. S. Fawaz, and P. Varaiya, "Supervisory control of discrete event processes with partial observations," *IEEE Trans. Automat. Control*, vol. 33, pp. 249–260, 1988.
[31] F. Lin and W. M. Wonham, "On observability of discrete-event systems," *Inform. Sci.*, vol. 44, pp. 173–198, 1988.
[32] J. N. Tsitsiklis, "On the control of discrete-event dynamical systems," *Math. Control Signals Systems*, pp. 95–107, 1989.
[33] P. J. Ramadge and W. M. Wonham, "The control of discrete event systems," *Proc. IEEE*, vol. 77, pp. 81–98, 1989.

[34] C. Cassandras and S. Lafortune, *Introduction to Discrete Event Systems*. Boston, MA: Kluwer, 1999.
[35] M. Wakaiki, P. Tabuada, and J. P. Hespanha, "Supervisory control of discrete-event systems under attacks," Tech. Report, University of California, Santa Barbara, 2016. [Online]. Available: http://www.ece.ucsb.edu/~hespanha/published/DES under_attack_ver8_19_Tech_note.pdf

〈発　表　資　料〉

題　　名	掲載誌・学会名等	発表年月
SMT-based observer design for cyber-physical systems under sensor attacks	ACM/IEEE 7th International Conference on Cyber-Physical Systems	2016 年 4 月
Attacks to Discrete-event Systems	55th IEEE CDC Workshop: Taxonomies of Interconnected Systems: Large-Scale Networks	2016 年 12 月
未知外乱オブザーバを用いたサイバー攻撃の検出	第 4 回制御部門マルチシンポジウム	2017 年 3 月
SMT-based observer design for cyber-physical systems under sensor attacks	ACM Transactions on Cyber-Physical Systems	採択済み