ネットワーク阻止ゲームにおける動的阻止について

01504810　防衛大学校情報工学科　宝崎 隆祐　HOHZAKI Ryusuke

1. はじめに

感染症ルートの阻止やテロに対する施設防御，情報通信網等のインフラネット防御のように悪意ある侵入者の阻止問題を取り扱うネットワーク阻止ゲーム [1] では，ネットワーク上での阻止資源の静的配備を議論するものが多い [2-5]．しかし，侵入者の動きは時間を伴う動的なものであることが多いため，阻止資源の配備計画も動的なものとする必要がある．この発表では，ネットワーク阻止ゲームにおける動的阻止を扱う．

2. モデルと侵入パスの構造

侵入者と阻止者が対立する次のようなネットワーク阻止ゲームを考える．

A1. ノード集合 $\boldsymbol{N}$ と有向アーク集合 $\boldsymbol{A}$ から成る閉路を持たないグラフ $G(\boldsymbol{N},\boldsymbol{A})$ が，ゲームの空間である．

A2. 侵入者及び阻止者の２人のプレイヤーが存在し，侵入者は複数の侵入ノード群 $\boldsymbol{S}\subseteq\boldsymbol{N}$ の各ノード $s\in\boldsymbol{S}$ から初期量 R_s で侵入を開始し，目的ノード群 $\boldsymbol{T}$ のいずれかへ到達しようとする．

阻止者は初期資源量 B_0 を分割してアークや待機ノードに配置し，侵入者の阻止を図る．アークに置かれた阻止資源は以後移動はできず，そこを通過する侵入者のみを阻止できる．阻止者は，侵入者の侵入開始直後にその侵入パス組 $\boldsymbol{l}$ の情報を獲得し，待機ノード群 $\boldsymbol{W}$ に置かれた阻止資源を侵入者の通過前にアークに届けることができれば，そこでの阻止に利用できる．待機ノード $r\in\boldsymbol{W}$ からアーク e への資源配備時間を $D(r,e)$ とする．

A3. アーク $e\in\boldsymbol{A}$ を通過しようとする侵入者はそこに配備された阻止資源により損耗し，減少する．資源量 y による量 x の侵入者の残存量は次式で与えられる．パラメータ γ_e を戦力交換比と呼ぶ．

$$\max\{0,\ x-\gamma_e y\} \tag{1}$$

A4. ゲームの支払は目的ノード群 $\boldsymbol{T}$ のいずれかに到達する侵入者の総残存量であり，侵入者はそれをできるだけ大きく，阻止者は小さくしようとする．

仮定 A4 から，問題は同時手番の２人ゼロ和ゲームである．$\boldsymbol{S}$ から $\boldsymbol{T}$ に至る侵入パス組の集合を Ω とすれば，侵入者の純粋戦略は１つのパス組 $\boldsymbol{l}\in\Omega$ の選択であり，その混合戦略は Ω 上の確率分布 $\pi=\{\pi(\boldsymbol{l}),\boldsymbol{l}\in\Omega\}$ で表される．$\pi(\boldsymbol{l})$ はパス組 $\boldsymbol{l}$ を採る確率である．侵入者の移動時間として，パス組 $\boldsymbol{l}$ を移動する侵入者が侵入からアーク e に到達するまでの時間を $C(\boldsymbol{l},e)$ とする．

一方の阻止側戦略は，アークと待機ノードへの阻止資源の初期配備及び侵入パス情報を得た後の待機ノードからの資源の投入計画である．初期配備を，アーク e 及び待機ノード r への配備量 y_e, y_r から成る $\boldsymbol{y}=\{y_e,y_r,e\in\boldsymbol{A},r\in\boldsymbol{W}\}$ で表す．また，侵入パス組 $\boldsymbol{l}$ の獲得情報を使った資源投入計画を $\boldsymbol{z}=\{z_l(r,e),r\in\boldsymbol{W},e\in\boldsymbol{A},\boldsymbol{l}\in\Omega\}$ で表す．$z_l(r,e)$ は，パス組 $\boldsymbol{l}$ の侵入情報を得た場合の待機ノード r からアーク e への配備資源量である．$\boldsymbol{z}$ の実行可能条件は，以下のとおりである．

$$\sum_{e\in A} z_l(r,e)=y_r,\ r\in\boldsymbol{W},\ \boldsymbol{l}\in\Omega \tag{2}$$

侵入者のとるパス組は，複数の侵入ノード $\boldsymbol{S}$ から進みつつ途中での合流後は同じ経路をとるツリー状の経路となる．１つのパス組 $\boldsymbol{l}\in\Omega$ に対し，その通過アークの集合を $\widehat{\boldsymbol{A}}_l$，到達する目的ノードの集合を $\boldsymbol{T}_l$，１つの到達ノード $t\in\boldsymbol{T}_l$ に到る $\boldsymbol{l}$ から成る連結グラフを G_t^l，その中の出発ノードの集合を $\boldsymbol{S}_t^l$，複数のパスが合流するノード（会合ノードと呼ぶ）を $\boldsymbol{R}_t^l$ で表す．さらに，G_t^l のノード k から出て次の隣接ノード k' に至る区間のアーク集合を M_k^l，ノード k に入るアークに接続する隣接ノード集合を $\widehat{\boldsymbol{L}}_k^l$ とする．図１は G_t^l の１例である．因みに，２つの異なる到達ノード $t,t'\in\boldsymbol{T}_l$ のそれぞれを根とするグラフ G_t^l と $G_{t'}^l$ 同士は，非連結である．

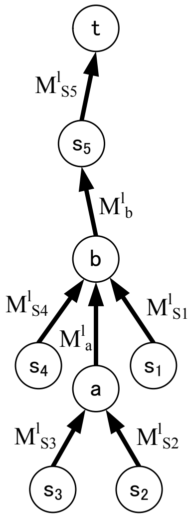

図１．パス組

3. 支払関数と均衡解

１つのパス組 $\boldsymbol{l}\in\Omega$ をとる侵入者と資源配備 $\boldsymbol{y}$，$\boldsymbol{z}$ をとる阻止者により，グラフ G_t^l の目的ノード $t\in\boldsymbol{T}_l$ に到達する侵入者の残存量を求める．G_t^l のノード k を通過後，アーク集合 M_k^l での損耗を経て，次の隣接ノードに入る直前の侵入者残存量を μ_k^l で表す．

出発ノード $s\in\boldsymbol{S}_t^l$ 通過直後の残存量 μ_s^l は

$$\mu_s^l=\max\left\{0,R_s+\sum_{k\in\widehat{L}_s^l}\mu_k^l-\sum_{e\in M_s^l}\gamma_e x_e^l\right\} \tag{3}$$

で表される．ただし，x_e^l は阻止資源の事前配備量及び待機ノードからの投入量の和であり，

$$x_e^l \equiv y_e + \sum_{r \in W | C(l,e) \geq D(r,e)} z_l(r,e) \tag{4}$$

で定義される．出発ノードでない会合ノード $d \in \boldsymbol{R}_t^l$ 通過後の残存量は次式で表される．

$$\mu_d^l = \max \left\{ 0, \sum_{k \in \widehat{L}_d^l} \mu_k^l - \sum_{e \in M_d^l} \gamma_e x_e^l \right\} \tag{5}$$

さらに，到着ノード t の残存量 v_t^l と，すべての $t \in \boldsymbol{T}_l$ での残存量の総和である支払関数は次式となる．

$$v_t^l = \sum_{k \in \widehat{L}_t^l} \mu_k^l, \qquad R(\boldsymbol{l}; \boldsymbol{y}, \boldsymbol{z}) = \sum_{t \in T_l} v_t^l \tag{6}$$

したがって，侵入者の混合戦略 π による侵入者の期待残存量は次式で与えられる．

$$R(\pi; \boldsymbol{y}, \boldsymbol{z}) = \sum_{l \in \Omega} \pi(\boldsymbol{l}) R(\boldsymbol{l}; \boldsymbol{y}, \boldsymbol{z}) \tag{7}$$

以後，期待支払 (7) 式をもつ同時手番ゲームの均衡解を求める．まず，$R(\pi; \boldsymbol{y}, \boldsymbol{z})$ のミニマックス最適化は，

$$\begin{aligned} &\min_{y,z} \max_{\pi} R(\pi; \boldsymbol{y}, \boldsymbol{z}) = \min_{y,z} \max_{l \in \Omega} R(\boldsymbol{l}; \boldsymbol{y}, \boldsymbol{z}) \\ &= \min_{y,z} \{ \xi \mid \xi \geq R(\boldsymbol{l}; \boldsymbol{y}, \boldsymbol{z}),\ \boldsymbol{l} \in \Omega \} \end{aligned}$$

と変形できる．$R(\boldsymbol{l}; \boldsymbol{y}, \boldsymbol{z})$ を (3)∼(6) 式を使って式展開し，演算 $\max\{\cdot,\cdot\}$ を２つの不等式で置き換えた次の結果が，最適な阻止資源の配備計画 $\boldsymbol{y}^*, \boldsymbol{z}^*$ を導出する定式化である．$\boldsymbol{z}^*$ が侵入者の移動を考慮した阻止資源の動的な配備計画であり，複数の侵入パス $\boldsymbol{l}$ をカバーする有効な資源利用となり得る．また，待機ノードからの阻止資源投入に時間が掛かる場合は，侵入者を待ち受ける静的な配備として $\boldsymbol{y}^*$ が使用される．

$$\begin{aligned} P_B^T: \quad & \min_{z,y,\xi,v,\mu} \xi \\ s.t. \quad & \xi \geq \sum_{t \in T_l} v_t^l,\ \boldsymbol{l} \in \Omega, \\ & v_t^l = \sum_{k \in \widehat{L}_t^l} \mu_k^l,\ t \in \boldsymbol{T}_l, \boldsymbol{l} \in \Omega, \\ & \mu_s^l \geq R_s + \sum_{k \in \widehat{L}_s^l} \mu_k^l - \sum_{e \in M_s^l} \gamma_e x_e^l, \\ & \qquad s \in \boldsymbol{S}_t^l, t \in \boldsymbol{T}_l, \boldsymbol{l} \in \Omega, \\ & \mu_s^l \geq 0,\ s \in \boldsymbol{S}_t^l, t \in \boldsymbol{T}_l, \boldsymbol{l} \in \Omega, \\ & \mu_d^l \geq \sum_{k \in \widehat{L}_d^l} \mu_k^l - \sum_{e \in M_d^l} \gamma_e x_e^l, \\ & \qquad d \in \boldsymbol{R}_t^l, d \notin \boldsymbol{S}_t^l, t \in \boldsymbol{T}_l, \boldsymbol{l} \in \Omega, \\ & \mu_d^l \geq 0,\ d \in \boldsymbol{R}_t^l, d \notin \boldsymbol{S}_t^l, t \in \boldsymbol{T}_l, \boldsymbol{l} \in \Omega, \\ & \sum_{e \in A} z_l(r,e) = y_r,\ r \in \boldsymbol{W},\ \boldsymbol{l}, \in \Omega, \\ & \sum_{e \in A} y_e + \sum_{r \in W} y_r \leq B_0, \\ & y_e \geq 0,\ e \in \boldsymbol{A}, \quad y_r \geq 0,\ r \in \boldsymbol{W}, \\ & z_l(r,e) \geq 0,\ r \in \boldsymbol{W},\ e \in \boldsymbol{A},\ \boldsymbol{l} \in \Omega, \\ & z_l(r,e) = 0,\ r \in \boldsymbol{W},\ e \notin \widehat{\boldsymbol{A}}_l,\ \boldsymbol{l} \in \Omega. \end{aligned}$$

$R(\pi; \boldsymbol{y}, \boldsymbol{z})$ のマックスミニ最適化は，まず最小化問題 $\min_{y,z} R(\pi; \boldsymbol{y}, \boldsymbol{z}) = \min_{y,z} \{ \sum_{l \in \Omega} \pi(l) w_l | w_l = \sum_{t \in T_l} v_t^l \}$ の双対問題として最大化問題を作り，さらに変数 π について最大化を行う．その結果，侵入者の最適混合戦略 π^* を求める問題が次のように定式化できる．ρ_k^l，σ_r^l 及び λ は，定式化の過程で導入した双対変数である．

$$\begin{aligned} P_R^T: \quad & \max_{\pi,\rho,\sigma,\lambda} \sum_{l \in \Omega} \sum_{s \in S} R_s \rho_s^l - B_0 \lambda \\ s.t. \quad & \rho_k^l \leq \pi(l),\ k \in \widehat{\boldsymbol{L}}_t^l,\ t \in \boldsymbol{T}_l, l \in \Omega, \\ & \rho_{k'}^l \leq \rho_k^l,\ k' \in \widehat{\boldsymbol{L}}_k^l, k \in \widehat{\boldsymbol{N}}_t^l, t \in \boldsymbol{T}_l, l \in \Omega, \\ & \gamma_e \sum_{(l,k) | e \in M_k^l, l \in \Omega} \rho_k^l \leq \lambda,\ e \in \boldsymbol{A}, \\ & \sum_{l \in \Omega} \sigma_r^l \leq \lambda,\ r \in \boldsymbol{W}, \\ & \gamma_e \sum_{k | e \in M_k^l, C(l,e) \geq D(r,e)} \rho_k^l \leq \sigma_r^l, \\ & \qquad r \in \boldsymbol{W}, e \in \widehat{\boldsymbol{A}}_l, \boldsymbol{l} \in \Omega, \\ & \rho_k^l \geq 0,\ k \in \widehat{\boldsymbol{N}}_t^l, t \in \boldsymbol{T}_l, l \in \Omega, \\ & \sum_{l \in \Omega} \pi(\boldsymbol{l}) = 1. \end{aligned}$$

4. おわりに

今回のモデル化では，ネットワーク上でツリー構造をもつパス組の作成や侵入者の移動時間の計算が必要となるため，ネットワーク理論で開発された幾つかのアルゴリズムを利用することができる．

参考文献

[1] 宝崎隆祐：社会の安全とネットワーク阻止モデル，オペレーションズ・リサーチ, **60** (5), 266–273, 2015.

[2] R. Hohzaki and T. Chiba: *J. of the Operational Research Society*, **66** (6), 979–992, 2015.

[3] R. Hohzaki and K. Sunaga: *JORSJ*, **59** (2), 195–217, 2016.

[4] R. Hohzaki and T. Higashio: *J. of the Operational Research Society*, **67** (5), 691-707, 2016.

[5] R. Hohzaki and M. Tanaka: *JORSJ*, **60** (3), 353-378, 2017.