Characterizing the Power of Moving Target Defense via Cyber Epidemic Dynamics

Yujuan Han	Fudan U & UTSA
Wenlian Lu	Fudan U & U Warwick
Shouhuai Xu	UTSA

HotSoS'14

Moving Target Defense (MTD)

- MTD is believed to be "game changer."
- There are a bag of MTD techniques.
- A classification of three classes (next slide)

Three Classes of MTD

- Network-based MTD Techniques
  - IP address and TCP port randomization etc.
- Host-based MTD Techniques
  - Instruction-level: ISR
  - Code-level: code randomization
  - Memory-level: ASLR
  - Application-level: N-version programming etc
- Instrument-based MTD Techniques
  - Dynamic honeypot

How to Characterize Power of MTD?

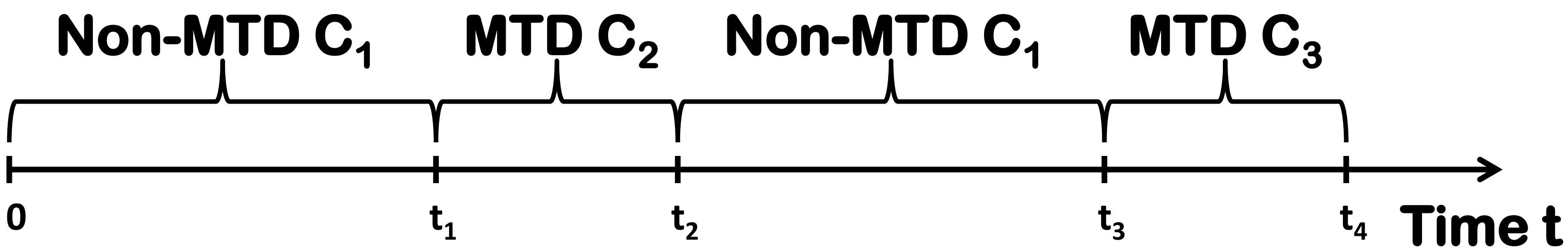
- There is no systematic quantitative understanding of the power of MTD techniques individually, let alone collectively.
- Consequence: Don’t know how to deploy them collectively and effectively or even optimally.
  - How to even define/formalize them exactly?
- This paper: Using cyber epidemic dynamics as the “lens” (or “ruler”) to characterize power of MTD.
  - First analytic approach
  - First-step within this approach

What Is This Paper Basically About?

- Cyber system often stays in some insecure/undesired configuration/posture (will be precisely defined).
- MTD often induces transient secure configurations, which however do not last permanently.
- How can we exploit MTD-induced secure configurations to rescue/tolerate the insecure ones, by (e.g.) making the dynamics converge to the clean state?

What Is This Paper Basically About?

One sentence summary: Suppose we know MTD-induced transient secure configurations, we can optimally orchestrate MTD to achieve some desired long-term goal.



- C_1: insecure configuration (e.g., due to the introduction of new attacks)
- C_2, C_3, …: MTD-induced transient secure configurations

Optimal in What Sense?

- <u>Maximizing the time</u> during which the cyber system can afford to stay in insecure configuration C_1, while still able to force the dynamics converge to the desired state.
  - Don't care about the cost imposed by launching MTD
- <u>Minimizing the cost</u> of deploying MTD, while allowing the cyber system to stay in insecure configuration for a given amount of time.
  - When cost matters

Roadmap

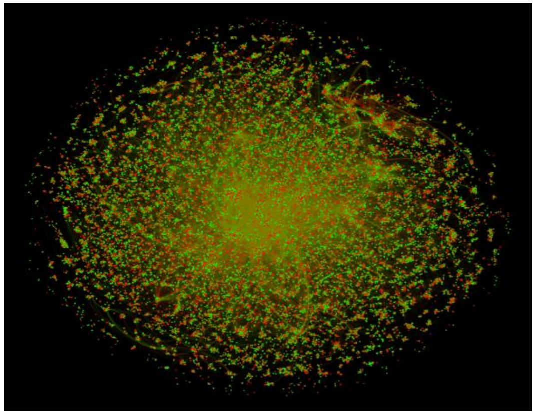
- Cyber epidemics model accommodating MTD
- Analysis: The case of dynamic parameters $\beta(t)$, $\gamma(t)$
- Analysis: The case of dynamic structures $G(t)$
- Related work
- Conclusion and future research directions

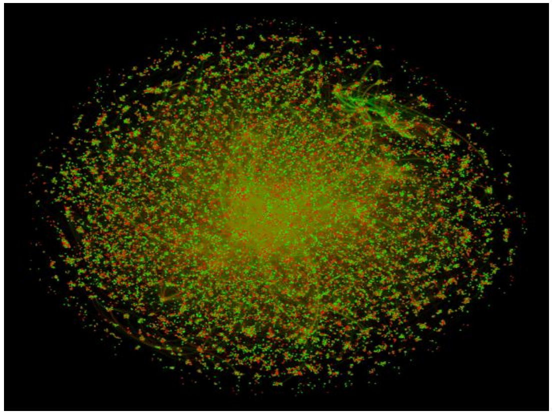
Cyber Epidemic Dynamics: Basics

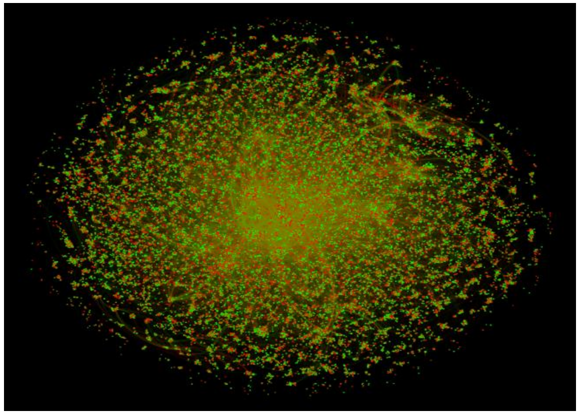
A specific kind of Cybersecurity Dynamics (see poster)

Complex Network based abstraction:

- ❑ Nodes abstract entities (e.g., computer)
  - ❖ Node state: green -- secure; red -- compromised
- ❑ Edges abstract the attack-defense interaction structure (system description/representation)





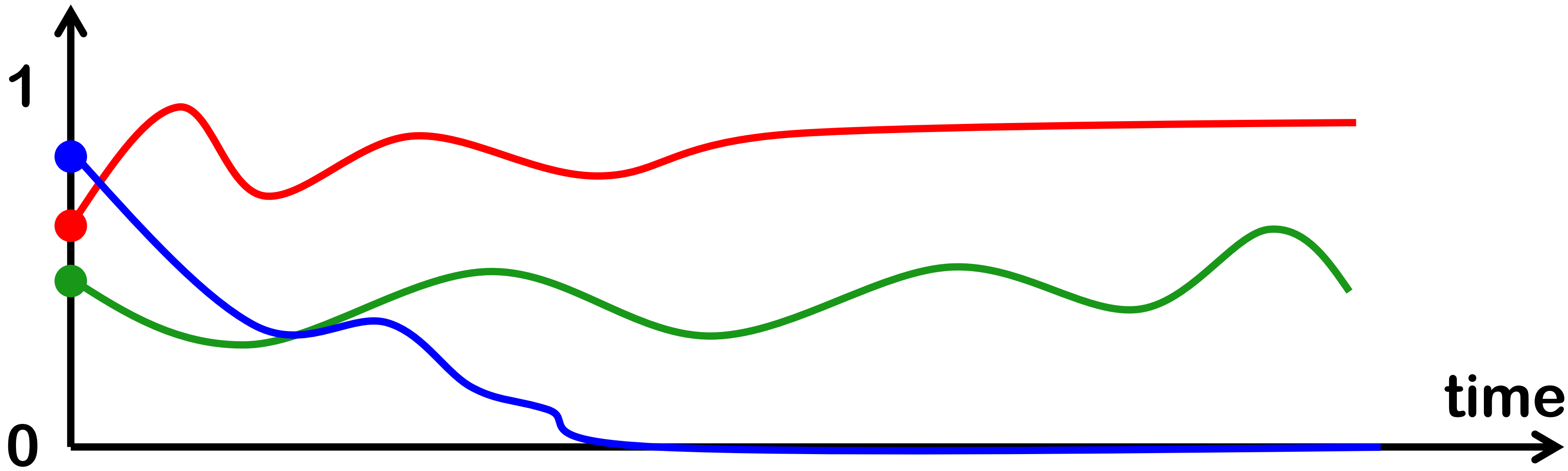


Three kinds of outcomes of evolution of global security state

Example Question: what are the governing/scaling laws?

Cyber Epidemic Dynamics: Basics

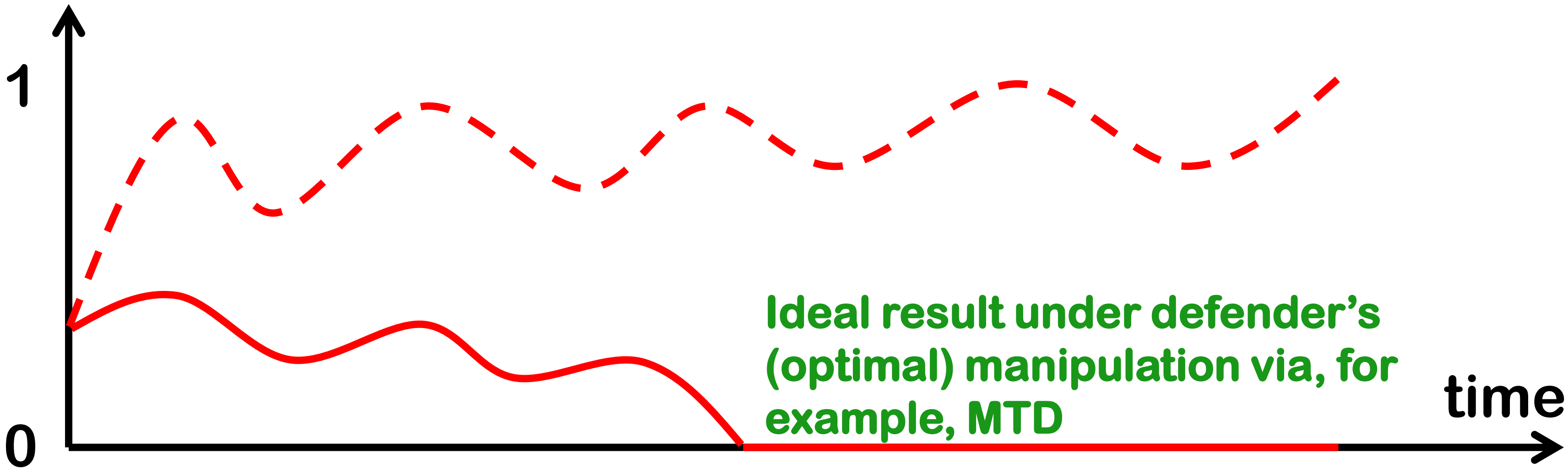
(Expected) portion of compromised nodes w.r.t. time

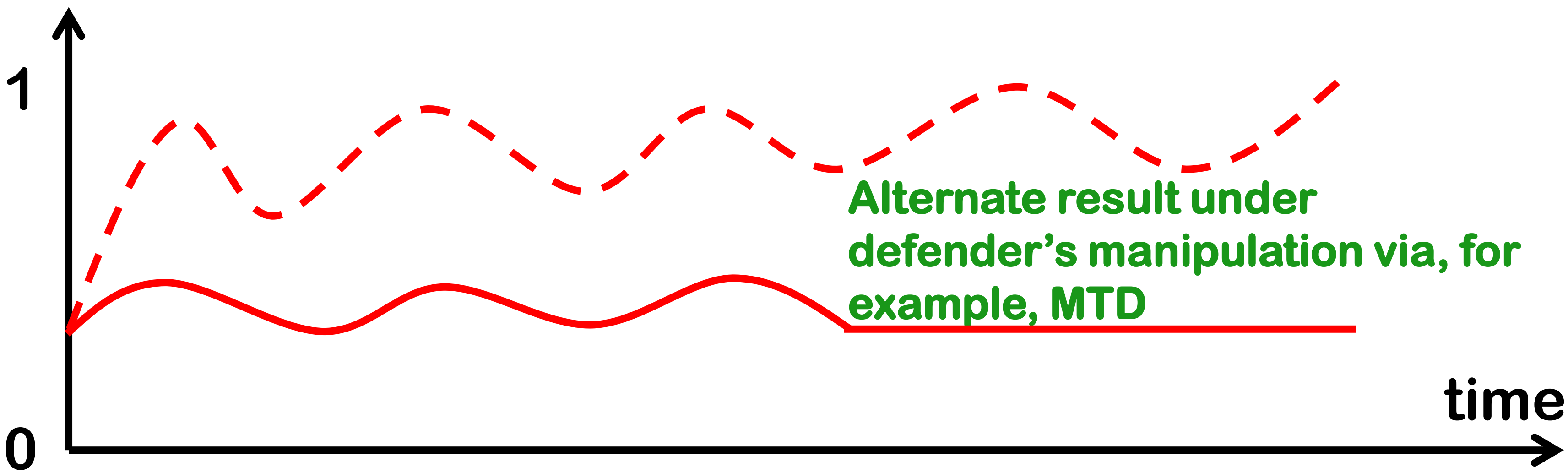


- This is perhaps the most natural ***cybersecurity metric***.
- With information about the probability that the nodes are compromised at time t, we can make better decisions. E.g., can a mission be disrupted at time t (< mission lifetime) with probability at most p?

Cyber Epidemic Dynamics: Basics

(Expected) portion of compromised nodes w.r.t. time





Equilibria can be "dynamic" due to the introduction of zero-day attacks.

Cyber Epidemics Model: Basics

- Using attack-defense structure to capture the (attacker, victim) relation: G=(V, E)
- Using parameters to capture "atomic" attack and defense capabilities:
  - γ: the probability an infected node u $\in$ V successfully attacks a secure node v $\in$ V over (u,v) $\in$ E at time t
  - β: the probability an infected node v becomes secure at time t

Cyber Epidemics Model: Basics

- ❑ Using attack-defense structure to capture the (attacker, victim) relation: G(t)=(V(t), E(t))
- ❑ Using parameters to capture "atomic" attacker and defense capabilities: $\beta(t)$, $\gamma(t)$
- ❑ Using epidemic threshold to describe the phase transition: sufficient condition under which the epidemic dynamics converges to equilibrium state — the clean state (i.e., spreading dies out) in this paper.

Cyber Epidemics Model with MTD

Idea: MTD can induce dynamic attack-defense structures $G(t)=(V(t), E(t))$ and/or dynamic parameters $\gamma(t)$ and $\beta(t)$

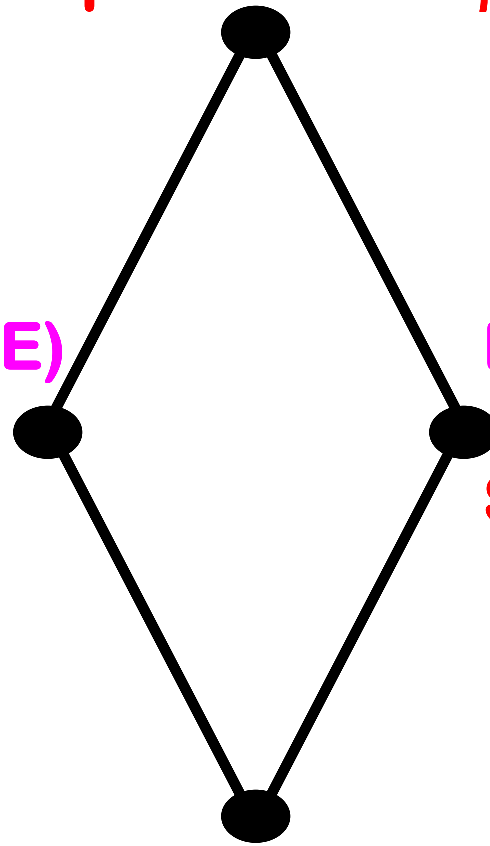
- Network-based MTD Techniques can induce dynamic attack-defense structures (e.g., dynamic IP addresses)
- Host-based MTD Techniques can induce dynamic parameters (e.g., harder to penetrate into computers)
- Instrument-based MTD Techniques can induce dynamic attack-defense structures (e.g., dynamic IP addresses) and dynamic parameters (e.g., detecting new attacks)

Problem Space: Assuming Fixed V

Dynamic structure: $G(t)=(V, E(t))$
Dynamic parameters: $\beta(t)$, $\gamma(t)$

See full version of the paper

Static structure: $G=(V, E)$
Dynamic parameters: $\beta(t)$, $\gamma(t)$



Dynamic structure: $G(t)=(V, E(t))$
Static parameters: β, γ

Static structure: $G=(V, E)$
Static parameters: β, γ

Definition: Configuration = ($G(t)$, $\beta(t)$, $\gamma(t)$)

A General Model

- Dynamic structure: $G(t)=(V, E(t))$, adjacency matrix $A(t)=[A_{vu}(t)]$
- Dynamic parameters: $\beta(t)$, $\gamma(t)$
- $i_v(t)$: probability node v is infected at time t (i.e., state)
- Assuming attacks are launched independently
  - See "a new approach to modeling and analyzing security …" for tackling adaptiveness/dependence
- We have, ***for each v***

$$\begin{aligned}\frac{di_v(t)}{dt} &= \xi_v(t)(1-i_v(t)) - \beta(t)i_v(t)\\ &= \left(1-\prod_{u\in V}(1-A_{vu}(t)i_u(t)\gamma(t))\right)(1-i_v(t)) - i_v(t)\beta(t).\end{aligned}$$

Threshold in the Simplest Case

Suppose both attack-defense structure e
time-invariant t: $G = (V, E)$ with adjace

Spreading dies out (clean state)

The dynamics converges to equilibrium $I^* = (0, \ldots, 0)$ if

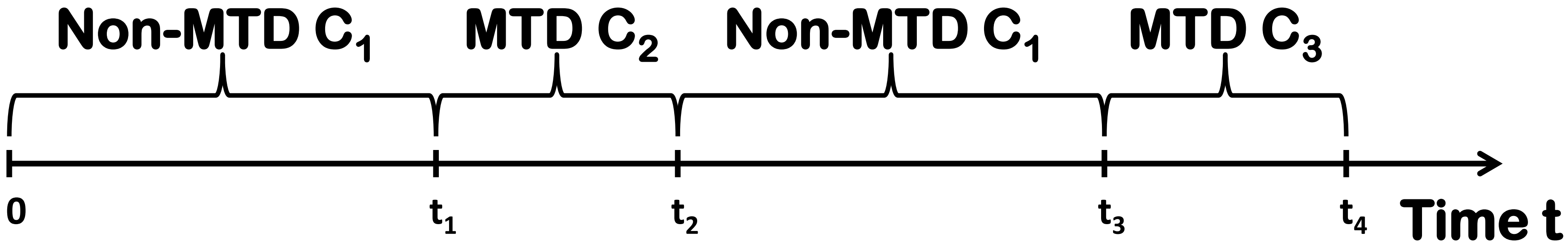
$$\mu \stackrel{def}{=} \beta - \gamma \lambda_1(A) > 0, \quad (1)$$

where $\lambda_1(A)$ is the larges ue of the
adjacent matrix A.

The threshold (sufficient condition)

If $\mu < 0$, the dynamics does not converge to $I^* = (0, \ldots, 0)$ at least for some initial values.

Idea of Tolerating Insecure Config.



- Definition: Insecure configuration $C_1=(G_1, \beta, \gamma)$: because it violates convergence condition (1).
- Suppose the system has to stay in configuration C_1
  - Justification: introduction of new attacks etc
- The defender can exploit MTD to force the system into some transient secure configuration C_2, C_3, …
- How to orchestrate MTD to make the dynamics converge to the desired equilibrium state?

Def: MTD-Power w/o Considering Cost

Definition

(($\mu_1, \mu_2, \ldots, \mu_J, \pi_1^*$)-powerful MTD, without considering cost)
Denote by $\mu_k = \beta_k - \gamma_k \lambda_1(A_k)$ for $k = 1, \ldots, J$, where A_k is the adjacency matrix of G_k.

1. Undesired c … $\mathcal{C}$ … $_1)$ with $\mu_1 < 0$.
2. MTD induce … o … $_j, \gamma_j)$ with $\mu_j > 0$, $j \geq 2$.

Given information

To maximize

We say MTD is *$(\mu_1, \mu_2, \ldots, \mu_J, \pi_1^*)$-powerful* if it can make the overall dynamics converge to $I^* = (0, \ldots, 0)$, while allowing the system to stay in configuration $\mathcal{C}_1$ for *the maximum π_1^*-portion of time* in the equilibrium.

Def: MTD-Power while Considering Cost

Definition

($(\mu_1, \mu_2, \cdots, \mu_J, \pi_1, \Upsilon)$-powerful, while considering cost)
Consider cost function $h(\cdot) : \mathbb{R}^+ \to \mathbb{R}^+$ such that $h(\mu_j)$ is the cost of launching MTD to induce configuration $\mathcal{C}_j$ for $j = 2, \ldots, J$, where $h'(\mu) \geq 0$ for $\mu > 0$.

1. Undesired c … $\mu_1 < 0$, π_1 is the potion of tin … m
2. MTD induced configurations $\mathcal{C}_j = (G_j, \beta_j, \gamma_j)$, $\mu_j > 0$, $j \geq 2$.

Given information

To minimize

We say MTD is $(\mu_1, \mu_2, \cdots, \mu_J, \pi_1, \Upsilon)$-powerful if the overall dynamics converges to $I^* = (0, \ldots, 0)$ at the minimum cost $\Upsilon(\pi_2^*, \cdots, \pi_J^*)$, where π_j^* $(2 \leq j \leq J)$ is the portion of time the system stays in configuration $\mathcal{C}_j$ in the equilibrium.

Roadmap

- Cyber epidemics model accommodating MTD
- **Analysis: The case of dynamic parameters $\beta(t)$, $\gamma(t)$**
- Analysis: The case of dynamic structures G(t)
- Related work
- Conclusion and future research directions

A General Result

Theorem

(Xu et al., ACM TAAS 2014) Consider configurations $(G, \beta(t), \gamma(t))$*, where* $(\beta(t), \gamma(t))$ *are driven by a homogeneous Markov process* η_t *with steady-state distribution* $[\pi_1, \cdots, \pi_N]$ *and support* $\{(\beta_1, \gamma_1), \ldots, (\beta_N, \gamma_N)\}$*, meaning* $\mathbb{E}(\beta_{\eta_t}) = \pi_1\beta_1 + \cdots + \pi_N\beta_N$ *and* $\mathbb{E}(\gamma_{\eta_t}) = \pi_1\gamma_1 + \cdots + \pi_N\gamma_N$. *If*

$$\frac{\pi_1\beta_1 + \cdots + \pi_N\beta_N}{\pi_1\gamma_1 + \cdots + \pi_N\gamma_N} > \lambda_1(A),$$

the dynamics will converge to $I^* = (0, \ldots, 0)$*; if*

$$\frac{\pi_1\beta_1 + \cdots + \pi_N\beta_N}{\pi_1\gamma_1 + \cdots + \pi_N\gamma_N} < \lambda_1(A),$$

the dynamics will not converge to $I^* = (0, \ldots, 0)$ *at least for some initial value scenarios.*

Max Tolerance of Insecure Configuration without Considering MTD Cost

Theorem

For configurations $\mathcal{C}_j = (G, \beta_j, \gamma_j)$ *with* $1 \leq j \leq N$*, we have* $\mu_j = \beta_j - \gamma_j \lambda_1(A)$ *where* $\mu_1 < 0 < \mu_2 < \cdots < \mu_N$*. The maximal potion of time the system can afford to stay in configuration* $\mathcal{C}_1$ *is*

$$\pi_1^* = \frac{\mu_N - \delta}{\mu_N - \mu_1},$$

which is reached by launc

The optimal orchestration strategy

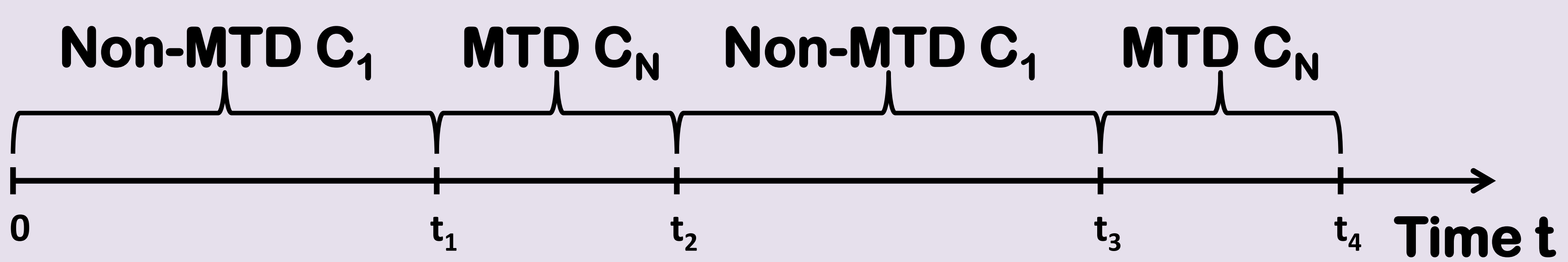
nly with portions of time given by

$$\pi_2^* = \ldots = \pi_{N-1}^* = 0, \quad \pi_N^* = \frac{\delta - \mu_1}{\mu_N - \mu_1}. \tag{2}$$

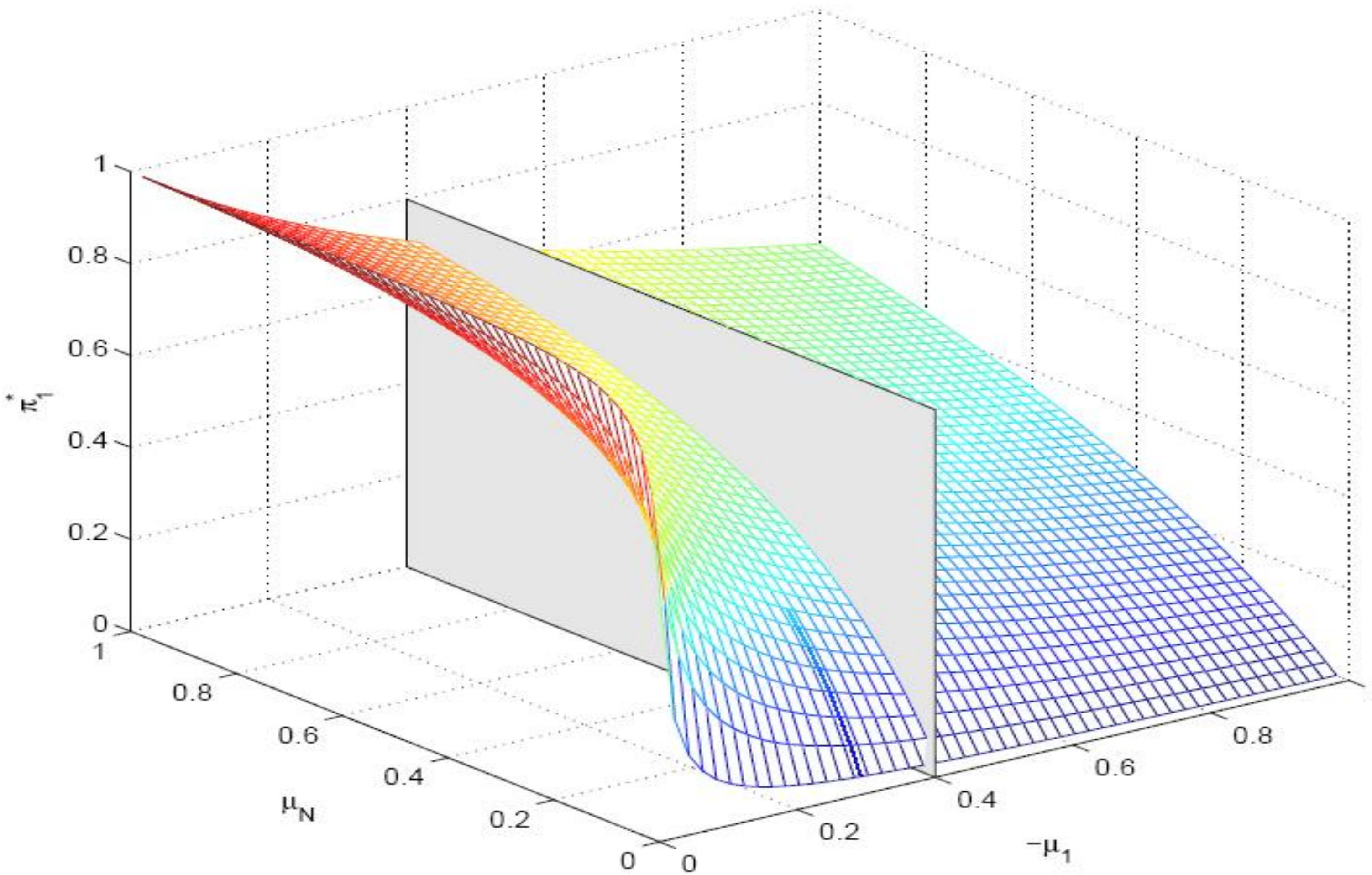
In other words, MTD is $(\mu_1, \cdots, \mu_N, \pi_1^*)$*-powerful.*

Algorithm for Orchestrating MTD to Achieve the Max Tolerance (without considering cost)

1. Compute π_1^* according to (2).
2. **while** TRUE **do**
3. Wait for time $T_1 \leftarrow \exp(a/\pi_1^*)$ {system in $\mathcal{C}_1$}
4. Launch MTD to make system stay in $\mathcal{C}_N$ for time $T_N \leftarrow \exp(a/(1-\pi_1^*))$
5. Stop launching MTD {system returns to $\mathcal{C}_1$}



Degree of Tolerance vs. Parameters: the case of not considering cost



Dependence of π_1^* on $-\mu_1$ and μ_N.

Minimizing Cost w.r.t. Given Degree of Tolerance

Suppose π_1 is the potion of time the system must stay in $\mathcal{C}_1$, it should satisfy $0 < \pi_1 \le \frac{\mu_N - \delta}{\mu_N - \mu_1}$. $f(\cdot)$ is the cost function. The cost of launching MTD is

$$\Phi(\pi_2, \cdots, \pi_N) = \pi_1 f(\mu_1) + \sum_{j=2}^{N} \pi_j f(\mu_j).$$

Define

$$\mu_{k^*} = \min\left\{\mu_k | \mu_k > \frac{-\pi_1 \mu_1}{(1-\pi_1)},\ 2 \le k \le N\right\} \tag{3}$$

and for $2 \le l < m \le N$,

$$\begin{aligned} F(\mu_l, \mu_m) =& \pi_1 f(\mu_1) + \frac{f(\mu_m) - f(\mu_l)}{\mu_m - \mu_l}(\delta - \pi_1 \mu_1) \\ &+ \frac{\mu_m f(\mu_l) - \mu_l f(\mu_m)}{\mu_m - \mu_l}(1 - \pi_1). \end{aligned} \tag{4}$$

Min Cost: Dynamic Parameters

Theorem

If $k^* = 2$, the minimal cost is

$$\min_{\pi_2,\cdots,\pi_N} \Phi(\pi_2,\cdots,\pi_N) = \pi_1 f(\mu_1) + (1-\pi_1) f(\mu_2),$$

which is reached by launching MTD to induce configuration $\mathcal{C}_2$ only. If $k^* > 2$, the minimal cost is

$$\min_{\pi_2,\cdots,\pi_N} \Phi(\pi_2,\cdots,\pi_N) = \min_{l<k^*\leq m} F(\mu_l,\mu_m) = F(\mu_{l^*},\mu_{m^*}). \quad (5)$$

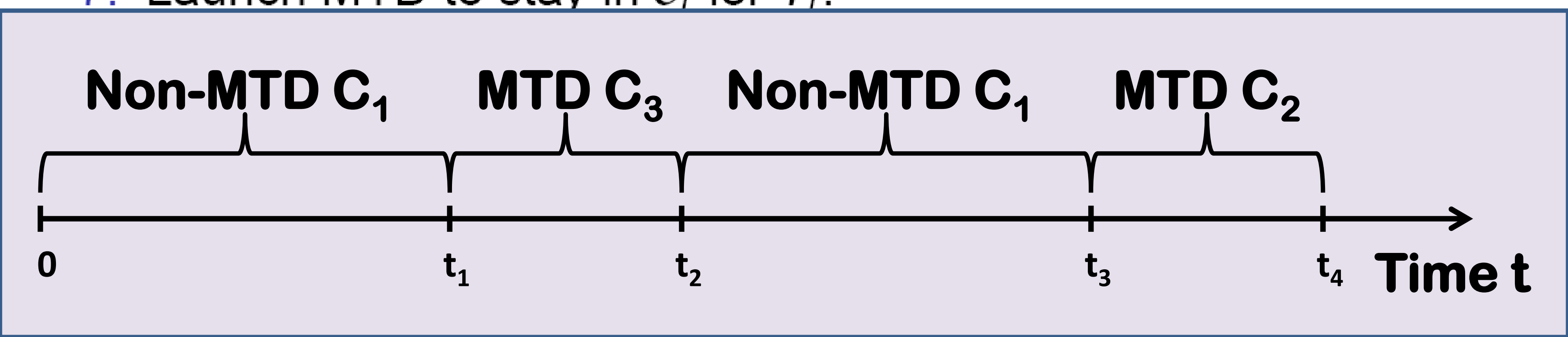
The minimal cost is reached by launching MTD to induce configurations $\mathcal{C}_{l^*}, \mathcal{C}_{m^*}$ respectively with portions of time:

$$\begin{bmatrix} \pi_{l^*} \\ \pi_{m^*} \end{bmatrix} = \frac{1}{\mu_{m^*} - \mu_{l^*}} \begin{bmatrix} (\mu_{m^*} - \delta) + \pi_1(\mu_1 - \mu_{m^*}) \\ -(\mu_{l^*} - \delta) + \pi_1(\mu_{l^*} - \mu_1) \end{bmatrix}. \quad (6)$$

where $0 < \delta \ll 1$ is some constant.

Algorithm for Orchestrating MTD to Achieve the Min Cost

1. Compute k^* according to (3)
2. **If** $k^* = 2$, wait in $\mathcal{C}_1$ for time $T_1 \leftarrow \exp(a/\pi_1)$ and launch MTD to stay in $\mathcal{C}_2$ for time $T_2 \leftarrow \exp(a/\pi_2)$ alternately.
3. **else** compute μ_{l^*}, μ_{m^*} & π_{l^*}, π_{m^*} according to (5)-(6). **endif**
4. Wait for time $T_1 \leftarrow \exp(a/\pi_1)$ {system in $\mathcal{C}_1$}
5. Set $\Delta = \{l^*, m^*\}$, $j \leftarrow_R \Delta$,
6. $T_j \leftarrow \exp(a/\pi_j)$.
7. Launch MTD to stay in $\mathcal{C}_j$ for T_j.



Simplifications

- When the cost functions are convex or concave, things can be simplified
  - True for many practical scenarios
- See paper for details

Roadmap

- ❑ Cyber epidemics model accommodating MTD
- ❑ Analysis: The case of dynamic parameters $\beta(t)$, $\gamma(t)$
- ❑ Analysis: The case of dynamic structures G(t)
- ❑ Related work
- ❑ Conclusion and future research directions

A General Result

Theorem

(a general result) Consider $\mathcal{C}_l = (G_l, \beta, \gamma)$, $l = 1, \cdots, N'$, where $\mathcal{C}_\ell = (G_\ell, \beta, \gamma)$ for $1 \le \ell \le j$ violate condition (1) but $\mathcal{C}_k = (G_k, \beta, \gamma)$ for $j < k \le N'$ satisfy condition (1). Then, MTD is effective if $G(t)$ are driven by Markov process strategy σ_t with infinitesimal generator $Q = (q_{uv})_{N' \times N'}$ defined as:

(i) for $k > j$, $-q_{kk} \le \frac{2a[\beta - \gamma\lambda_1(A_k) - \delta]}{\frac{jc + N' - 1 - j}{N' - 1} - a}$;

(ii) for $\ell \le j$, $-q_{\ell\ell} \ge \frac{2b[\gamma\lambda_1(A_\ell) - \beta + \delta]}{b - \frac{c(j-1)}{N'-1} - \frac{N'-j}{N'-1}}$;

(iii) $q_{rp} = \frac{-q_{rr}}{N'-1}$ for all $p \neq r$ and $p, r \in \{1, \ldots, N'\}$.

here $0 < \delta \ll 1$, c is related to the convergent speed, a, b, c are arbitrary constants with $a < 1 < b < c$.

Max Tolerance of Insecure Configuration without Considering MTD Cost

Theorem

For configurations $\mathcal{C}_j = (G_j, \beta_1, \gamma_1)$ *with* $1 \le j \le N'$, *we have* $\mu_j = \beta_1 - \gamma_1 \lambda_1(A_j)$ *and* $\mu_1 < 0 < \mu_2 < \cdots < \mu_{N'}$. *The maximal potion of time the system can afford to stay in configuration* $\mathcal{C}_1$ *is*

$$\pi_1^* = \frac{\frac{b-1}{2b[-\mu_1+\delta]}}{\frac{b-1}{2b[-\mu_1+\delta]} + \frac{c-a}{2a[\mu_{N'}-\delta]}}, \qquad (7)$$

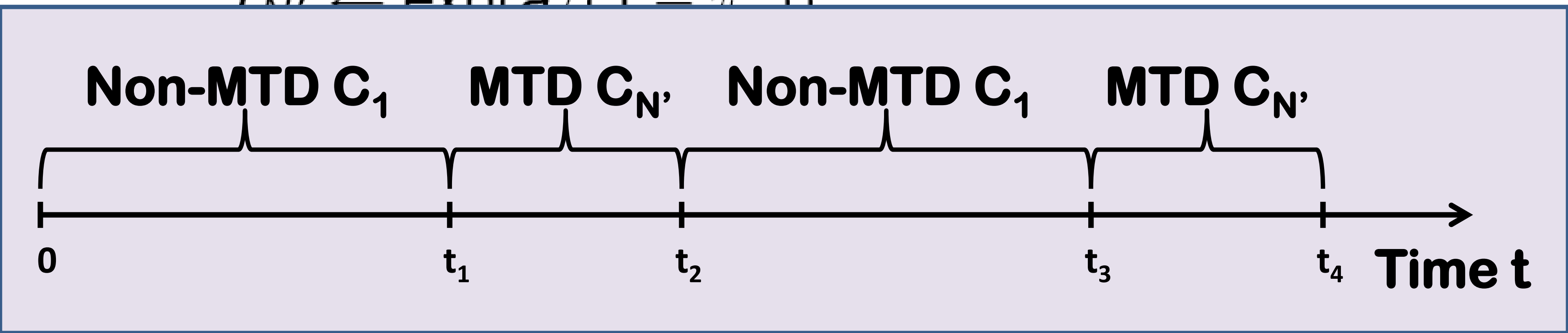
where $0 < \delta \ll 1, a < 1 <$ … *by launching MTD to induce* $\mathcal{C}_{N'}$ *only w*… *by*

The optimal orchestration strategy

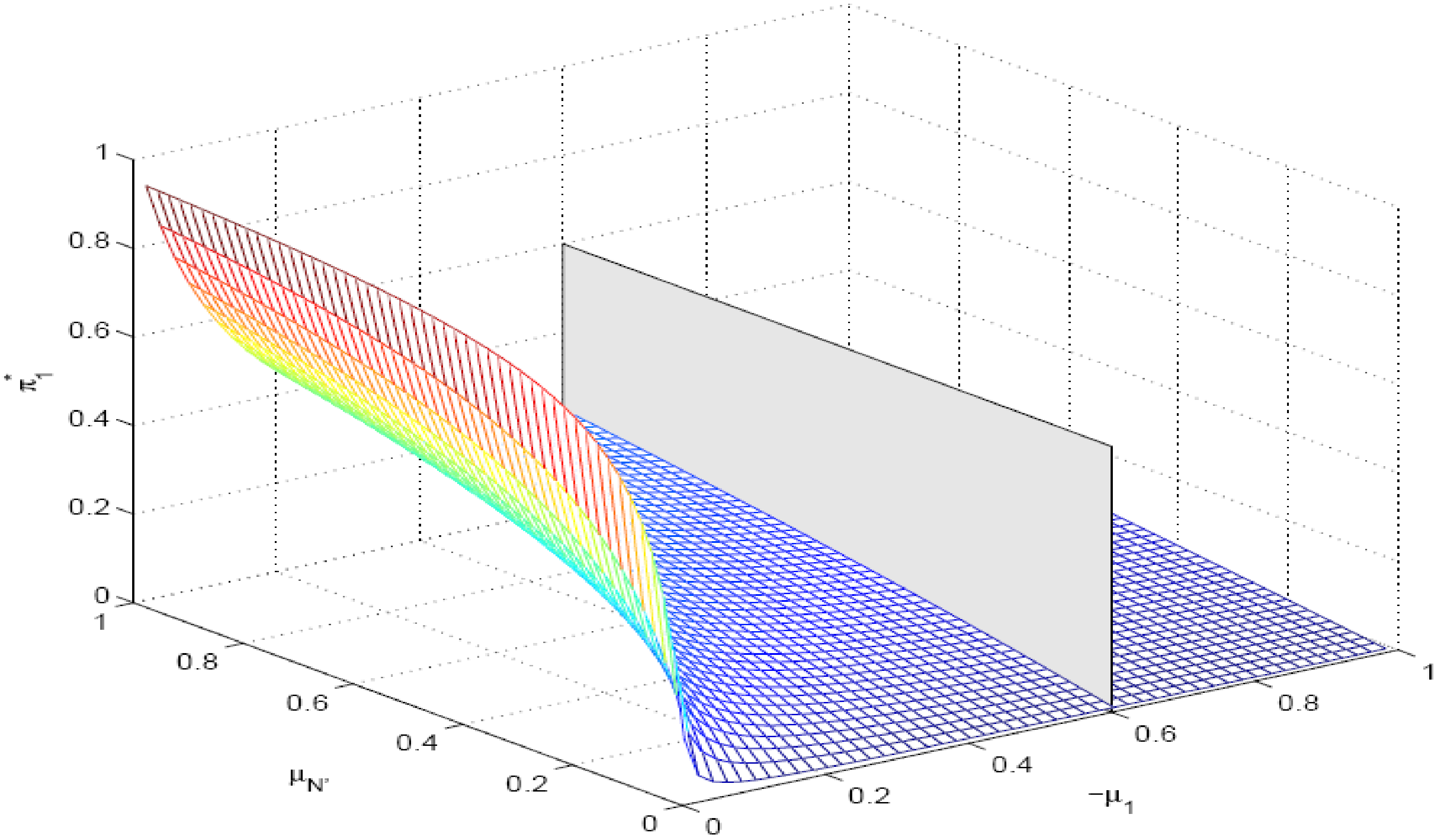
$$\pi_{N'}^* = 1 - \pi_1^*.$$

Algorithm for Orchestrating MTD to Achieve the Maximum Tolerance (without considering cost)

1. Compute π_1^* according to (7).
2. **while** TRUE **do**
3. Wait for time $T_1 \leftarrow \exp(a/\pi_1^*)$ {system in $\mathcal{C}_1$}
4. Launch MTD to make system stay in $\mathcal{C}_{N'}$ for time $T_{N'} \leftarrow \exp(a/((1-\pi^*))$



Degree of Tolerance vs. Parameters: the case of not considering cost



Dependence of π_1^* on $-\mu_1$ and $\mu_{N'}$.

Minimizing Cost w.r.t. Given Degree of Tolerance

Idea for finding min cost:

1. Consider possible combinations of MTD-induced configurations: $\mathcal{L}_1, \cdots, \mathcal{L}_{2^{N'}-1}$
2. Find σ_t (according to previous theorem) such that MTD forces the convergen
3. For each $\mathcal{L}_i$ with valid f time, denoted by π_1^i, the MTD allows the system to stay in $\mathcal{C}_1$. If $\pi_1^i \geq \pi_1$, keep $\mathcal{L}_i$; otherwise, eliminate $\mathcal{L}_i$.
4. For the remaining $\mathcal{L}_j$'s, compute the minimum cost of launching MTD corresponding to it.
5. Find the minimum cost among the costs.

Fortunately, the number of MTD-induced configurations is often small

Finding Minimum Cost

Suppose π_1, where $\pi_1 \leq \pi_1^*$, is the potion of time the system must stay in $\mathcal{C}_1$ and $g(\cdot)$ is the cost function.
σ_t defines the deployment of MTD: denote $Q = [q_{jk}]$ its infinitesimal generator, $x_l = \frac{1}{-q_{ll}}$ the expectation of sojourn time in $\mathcal{C}_l$. Then, the portion of time in $\mathcal{C}_l$ is $\pi_l = \frac{x_l}{\sum_j x_j}$.
Suppose MTD induces $\mathcal{C}_{k_1}, \cdots, \mathcal{C}_{k_{m'}}$, the cost of this MTD is

$$\begin{aligned}\Phi(\pi_2, \cdots, \pi_N) =& \pi_1 g(\mu_1) + \sum_{j=2}^{N} \pi_j g(\mu_j) \\ =& \pi_1 g(\mu_1) + (1 - \pi_1^*) \frac{\sum_{l=1}^{m'} x_{k_l} g(\mu_{k_l})}{\sum_{l=1}^{m'} x_{k_l}}.\end{aligned}$$

Finding Minimum Cost

Theorem

Find $\{k_1^*, \cdots, k_m^*\}$ *such that*

$$\{\mu_{k_1^*}, \cdots, \mu_{k_m^*}\} = \arg \min_{\{k_1, \cdots, k_{m'}\} \in \mathcal{K}} G(k_1, \cdots, k_{m'}) \qquad (8)$$

For given cost function $g(\cdot)$, *the minimum cost is*

$$\Psi(\bar{x}_1, \bar{x}_{k_1^*}(m) + \Delta, \cdots, \bar{x}_{k_m^*}(m)) = \pi_1 g(\mu_1) + (1 - \pi_1) G(k_1^*, \cdots, k_m^*),$$

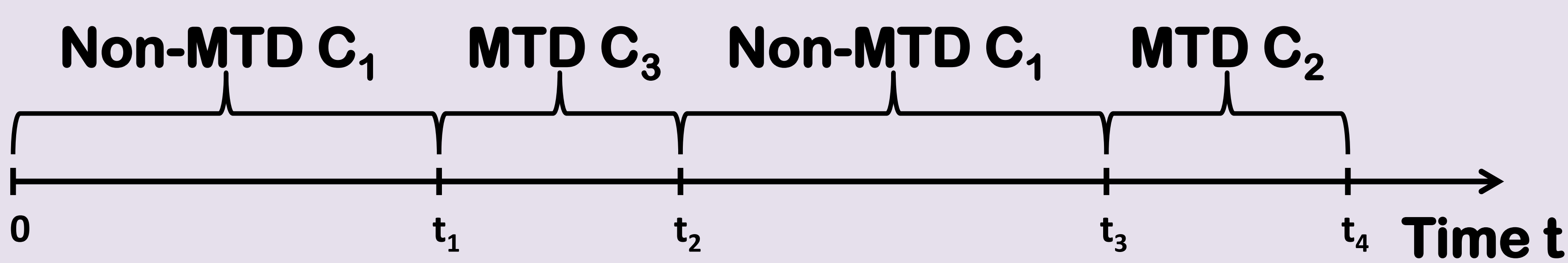
which is reached by launching MTD to induce configuration $\{(G_{k_l^*}, \beta, \gamma)\}_{l=1}^m$ *via the following deployment strategy:*

$$\pi_{k_1^*} = (1 - \pi_1) \frac{\bar{x}_{k_1^*}(m) + \Delta(k_1^*, \cdots, k_m^*)}{\sum_{l=1}^m \bar{x}_{k_l^*}(m) + \Delta(k_1^*, \cdots, k_m^*)}, \qquad (9)$$

$$\pi_{k_l^*} = (1 - \pi_1) \frac{\bar{x}_{k_l^*}(m)}{\sum_{l=1}^m \bar{x}_{k_l^*}(m) + \Delta(k_1^*, \cdots, k_m^*)}, l = 2, \cdots, m.$$

Algorithm for Orchestrating MTD to Achieve the Minimum Cost

1. Compute $k_1^*, \cdots, k_m^*$ and $\pi_{k_1^*}, \cdots, \pi_{k_1^*}$ according to (8)-(9)
2. Wait for time $T_1 \leftarrow \exp(a/\pi_1)$ {system in $\mathcal{C}_1$}
3. Set $\Delta = \{k_1^*, \cdots, k_m^*\}$, $k_j^* \leftarrow_R \Delta$
4. $T_{k_j^*} \leftarrow \exp(a/\pi_{k_j^*})$
5. Launch MTD to stay in $\mathcal{C}_{k_j^*}$ for time $T_{k_j^*}$
6. Set $\Delta = \{1, k_1^*, \cdots, k_m^*\} - \{k_j^*\}$, $k_j^* \leftarrow_R \Delta$



Roadmap

- Cyber epidemics model accommodating MTD
- Analysis: The case of dynamic parameters $\beta(t)$, $\gamma(t)$
- Analysis: The case of dynamic structures G(t)
- Related work
- Conclusion and future research directions

Related Work

- Characterizing effectiveness of MTD: two complementary perspectives (see paper for references):
  - Specific technique with localized view vs. classes of techniques with global view
  - *Step closer to real system: state → configuration*
- Cyber Epidemic Dynamics: an active research area rooted in biological epidemic dynamics
  - But beyond it because of unique technical barriers

Limitation of the Study

- Assume attack-defense structures and parameters (i.e., transient configurations) are given.
  - Eliminating it: An orthogonal thread of Cybersecurity Dynamics (see poster)
- Assume attacker cannot choose when to impose configuration C_1.
- Assume homogeneous parameters $\gamma(v, u) = \gamma$ and $\beta(v) = \beta$.

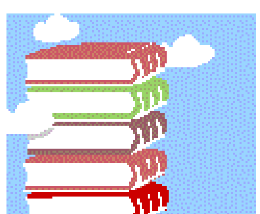
Eliminate them or weaken them as much as possible

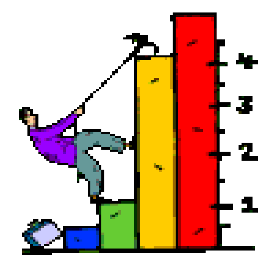
- Where is the boundary between analytic model and simulation model?

Conclusion and Future Work

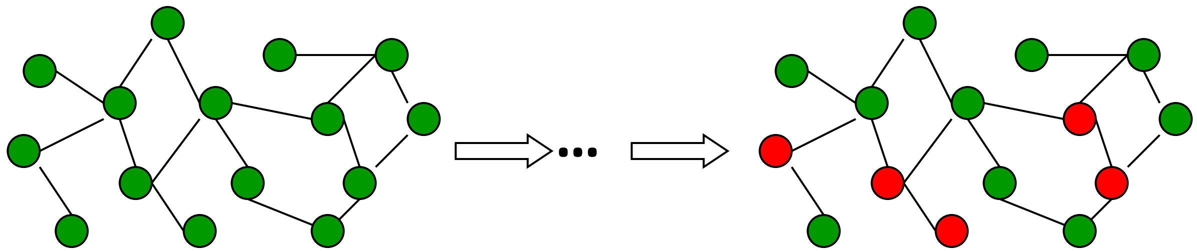
- An approach: using cyber epidemic dynamics to characterize the power of MTD.
- Two measures of MTD-power: Optimization
- Constructive proofs that lead to algorithms for orchestrating MTD to achieve the maximum tolerance or minimum cost
- Future work: Addressing the limitations

Enjoy exploring the unknown territory!





Cyber Epidemic Dynamics: Basics



(secure node compromised node)

- Can be instantiated at multiple resolutions: nodes represent (for example) computer, component, etc.
- Topology can be arbitrary in real-life: from complete graph to any structure

The Gap Need to Be Bridged to Practice

We assume we know "transient" capabilities of launching MTD (in terms of manipulating the model parameters).

- Justification: No single MTD defense (combination) would be "permanently" powerful to force the dynamics converge to desired state (e.g., due to zero-day attacks)
- Many desired "transient" configurations can tolerate some undesired configurations, when making the dynamics converge to the desired equilibrium state

Need to eliminate this assumption.