# Optimal Patching in Clustered Malware Epidemics

## NSE ML+Security Reading Group

Kim Hammar

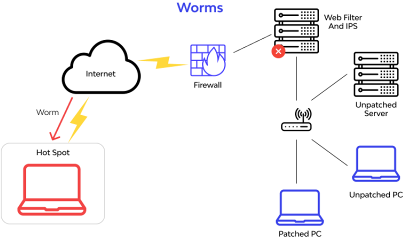
*kimham@kth.se*

Division of Network and Systems Engineering
KTH Royal Institute of Technology

February 16, 2023

# The Context and Key Points of the Paper

- The paper proposes a formal framework for deriving optimal patching policies to deal with **heterogeneous** malware epidemics
  - Models the spread of malware using a **stratified epidemic model**.
  - Derives structural results of the optimal controller using Pontryagin's Maximum Principle (PMP).
  - Evaluates patching strategies in simulation.



# Outline

- **Background**
  - Malware epidemics
  - Stratified epidemic models
  - Pontryagin's maximum principle
- **The Paper**
  - Approach
  - System model
  - Formulation of the optimal control problem
  - Analysis of the optimal controller using Pontryagin's principle
- **Conclusions**
- **Discussion**
  - Strong points
  - Limitations of the paper

# Outline

- **Background**
  - Malware epidemics
  - Stratified epidemic models
  - Pontryagin's maximum principle

- **The Paper**
  - Approach
  - System model
  - Formulation of the optimal control problem
  - Analysis of the optimal controller using Pontryagin's principle

- **Conclusions**

- **Discussion**
  - Strong points
  - Limitations of the paper

# Outline

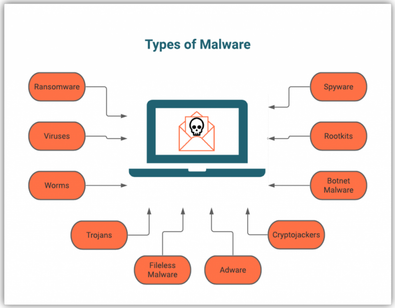
- **Background**
  - Malware epidemics
  - Stratified epidemic models
  - Pontryagin's maximum principle
- **The Paper**
  - Approach
  - System model
  - Formulation of the optimal control problem
  - Analysis of the optimal controller using Pontryagin's principle
- **Conclusions**
- **Discussion**
  - Strong points
  - Limitations of the paper

# Outline

- **Background**
  - Malware epidemics
  - Stratified epidemic models
  - Pontryagin's maximum principle
- **The Paper**
  - Approach
  - System model
  - Formulation of the optimal control problem
  - Analysis of the optimal controller using Pontryagin's principle
- **Conclusions**
- **Discussion**
  - Strong points
  - Limitations of the paper

# Malware epidemics

- **Malware**
  - Software intentionally designed to cause disruption to a computer system or network.
- **Types of Malware**
  - *Virus*: malware that spreads through execution of some other program.
  - *Worm*: virus that can spread by itself.
  - *Trojan*: virus that infects computers through social engineering.
  - *Ransomware*: locks down a computer until a ransom is paid.



# Case Study: Ransomware Attack Against Coop July 2021

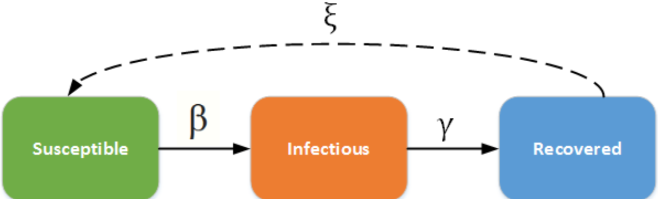
- The ransomware was deployed on the systems through a **zero-day exploit**.
- The original target was Kaseya, an American company, which provide cashier equipment to Coop.
- The people behind the attack are linked to Russia, group is called "REvil", Hackers from Ukraine/Russia were arrested.
- **700 out of 800 Coop stores** nationwide had to close because payments could not be made.
- The ransom to get the payment systems working again was 600 million SEK.

# Stratified Epidemic Models

- Stratified model: the **population is divided into sub-populations**
- SIR model: each sub population is divided into three states:
  - (**S**)usceptible: individuals susceptible to the virus
  - (**I**)infected: infected individuals
  - (**R**)ecovered: recovered (immune) individuals
- Individuals move between states. Evolution of states can be modeled with non-linear differential equations, e.g.

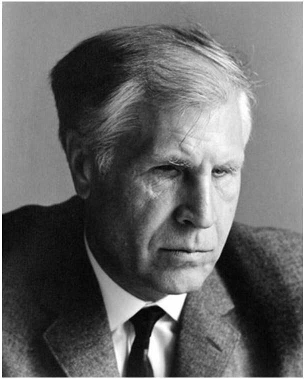
$$\frac{dS}{dt} = -\frac{\beta IS}{N}, \quad \frac{dI}{dt} = -\frac{\beta IS}{N} - \gamma I, \quad \frac{dR}{dt} = \gamma I$$

- Folkhälsomyndigheten used a SEIR (Susceptible, Exposed, Infected, Recovered) model to analyze Covid 19.



# Pontryagin's Maximum Principle

- The maximum principle provides local optimality conditions for continuous and constrained control problems.
- Developed by Soviet mathematician **Lev Pontryagin** in the 50s.
- Pontryagin became blind at the age of 14 due to an explosion.
- His mother wrote all the formulas and read papers aloud to him.
- The principle was originally developed to maximize the speed of missiles and rockets during the cold war.



Pontryagin, 1908-1988

# Pontryagin's Maximum Principle

Consider a control problem on Bolza form:

$$\overbrace{\min_{\boldsymbol{u}(\cdot)} \left[\phi(x(t_f)) + \int_{t_0}^{t_f} f_o(t, \boldsymbol{x}(t), \boldsymbol{u}(t))dt\right]}^{J(u(t))} \tag{1}$$

$$\text{subject to } \begin{cases} \dot{\boldsymbol{x}} = f(t, \boldsymbol{x}(t), \boldsymbol{u}(t)) & \forall t \in [0, t_f] \\ \boldsymbol{x}(0) = \boldsymbol{x}_0 & \\ \boldsymbol{x}(t) \in \mathbb{R}^n & \forall t \in [0, t_f] \\ \boldsymbol{u}(t) \in \mathbb{R}^m & \forall t \in [0, t_f] \end{cases} \tag{2}$$

Goal is to optimize a functional $J(u(t))$. Since $u(t)$ is not parameterized we are optimizing over an infinite space of continuous parameters.

$f_o$ is the **running cost** (e.g. fuel used by the rocket). $\phi$ is the **terminal cost** (e.g. time to reach destination). $f$ is the **dynamics model** (e.g. a system of ODEs).

# Pontryagin's Maximum Principle

We can find optimal control candidates using variational arguments from **calculus of variations**.

If $\boldsymbol{u}^*$ is optimal and we make a small perturbation to $\boldsymbol{u}^*$ (a variation), the cost cannot decrease. We obtain the variational inequality:

$$J(\boldsymbol{u}^*(t) + \delta u) - J(\boldsymbol{u}^*(t)) \geq 0 \qquad \forall t \tag{3}$$

Pontryagin's principle maps the above optimality condition in the primal space to simpler conditions in the dual space.

# Pontryagin's Maximum Principle

Define the **Hamiltonian**:

$$H(t, \boldsymbol{x}(t), \boldsymbol{u}(t), \boldsymbol{\lambda}(t)) = f_o(t, \boldsymbol{x}(t), \boldsymbol{u}(t)) + \boldsymbol{\lambda}^T(t) f(t, \boldsymbol{x}(t), \boldsymbol{u}(t))$$

**Hamiltonian minimization condition:**

$$u^*(t) = \tilde{\mu}(t, \boldsymbol{x}(t), \boldsymbol{\lambda}(t)) = \arg\min_u H(t, \boldsymbol{x}(t), \boldsymbol{u}(t), \boldsymbol{\lambda}(t))$$

**Adjoint equation**:

$$\dot{\boldsymbol{\lambda}}(t) = \nabla_{\boldsymbol{x}} H(t, \boldsymbol{x}(t), \boldsymbol{u}^*(t), \boldsymbol{\lambda}(t)) \quad \text{subject to } \boldsymbol{\lambda}(t_f) = \nabla_{\boldsymbol{x}} \phi(x(t_f))$$

**State equation**:

$$\dot{\boldsymbol{x}}(t) = \nabla_{\lambda} H(t, \boldsymbol{x}(t), \boldsymbol{u}^*(t), \boldsymbol{\lambda}(t)) \qquad \text{subject to } x(0) = x_0$$

i.e. we transformed the control problem to a two-point boundary value problem and a pointwise minimization.

# Remarks

- **Necessary but not sufficient:**
  - Any controller $u(t)$ that satisfies Pontryagin's conditions is possibly optimal. (Necessary conditions but not sufficient.)
  - Under certain convexity assumptions Pontryagin's conditions are sufficient.

- **Computations:**
  - Applying PMP involves pointwise minimization and solving a two-point boundary value problem of ODEs.
  - Compare this to solving the Hamilton-Jacobi-Bellman equation (HJBE), which involves a complicated PDE.

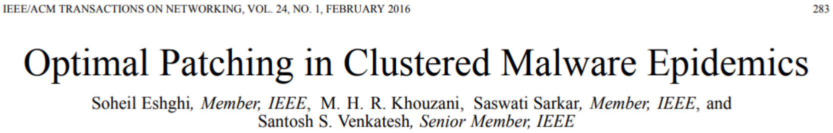
- **Open-loop solution**:
  - PMP gives you an optimal trajectory, i.e. an open-loop solution. It does not give you a feedback controller (closed-loop solution).

# Outline

- **Background**
  - Malware epidemics
  - Stratified epidemic models
  - Pontryagin's maximum principle
- **The Paper**
  - Approach
  - System model
  - Formulation of the optimal control problem
  - Analysis of the optimal controller using Pontryagin's principle
- **Conclusions**
- **Discussion**
  - Strong points
  - Limitations of the paper

# Approach

1. Model virus spread with a stratified SIR model
2. Formulate the problem of minimizing the spread as an optimal control problem
3. Analyze the structure of the optimal controller using Pontryagin's principle
4. Use numerical methods to compute the solution and evaluate through simulations



IEEE/ACM TRANSACTIONS ON NETWORKING, VOL. 24, NO. 1, FEBRUARY 2016 283

## Optimal Patching in Clustered Malware Epidemics

Soheil Eshghi, *Member, IEEE*, M. H. R. Khouzani, Saswati Sarkar, *Member, IEEE*, and Santosh S. Venkatesh, *Senior Member, IEEE*

# System Model

- We have $N$ nodes (e.g. computing devices)
- We have $M$ types of nodes that form subpopulations
- A node of type $i \in \{1, \ldots, M\}$ can be in three states: (S)usceptible, (I)nfected, (R)ecovered.
- Let $n_i^S(t), n_i^I(t), n_i^R(t)$ denote the number of susceptible, infected, and recovered nodes of type $i$, respectively.
- A subset of the recovered nodes are **"dispatchers"**. They can "heal" infected nodes and make susceptible nodes immune.
- The control signal $u(t) \in [0, 1]$ controls the rate at which dispatchers contact other nodes.
- Studies two versions of the model:
  - **Non-replicative patching**: There is a fixed set of dispatchers.
  - **Replicative patching**: When a node has been recovered it becomes a dispatcher.
- W.L.O.G I will focus on the non-replicative setting.

# System Model

- We have $N$ nodes (e.g. computing devices)
- We have $M$ types of nodes that form subpopulations
- A node of type $i \in \{1, \ldots, M\}$ can be in three states: (S)usceptible, (I)nfected, (R)ecovered.
- Let $n_i^S(t), n_i^I(t), n_i^R(t)$ denote the number of susceptible, infected, and recovered nodes of type $i$, respectively.
- A subset of the recovered nodes are **"dispatchers"**. They can "heal" infected nodes and make susceptible nodes immune.
- The control signal $u(t)$ controls the rate at which dispatchers contact other nodes.
- Studies two versions of the model:
  - **Non-replicative patching**: There is a fixed set of dispatchers.
  - **Replicative patching**: When a node has been recovered it becomes a dispatcher.
- W.L.O.G I will focus on the non-replicative setting.

# System Model

- We have $N$ nodes (e.g. computing devices)
- We have $M$ types of nodes that form subpopulations
- A node of type $i \in \{1, \ldots, M\}$ can be in three states: (S)usceptible, (I)nfected, (R)ecovered.
- Let $n_i^S(t), n_i^I(t), n_i^R(t)$ denote the number of susceptible, infected, and recovered nodes of type $i$, respectively.
- A subset of the recovered nodes are **"dispatchers"**. They can "heal" infected nodes and make susceptible nodes immune.
- The control signal $u(t)$ controls the rate at which dispatchers contact other nodes.
- Studies two versions of the model:
  - **Non-replicative patching**: There is a fixed set of dispatchers.
  - **Replicative patching**: When a node has been recovered it becomes a dispatcher.
- W.L.O.G I will focus on the non-replicative setting.

# System Model

- We have $N$ nodes (e.g. computing devices)
- We have $M$ types of nodes that form subpopulations
- A node of type $i \in \{1, \ldots, M\}$ can be in three states: (S)usceptible, (I)nfected, (R)ecovered.
- Let $n_i^S(t), n_i^I(t), n_i^R(t)$ denote the number of susceptible, infected, and recovered nodes of type $i$, respectively.
- A subset of the recovered nodes are **“dispatchers”**. They can “heal” infected nodes and make susceptible nodes immune.
- The control signal $u(t)$ controls the rate at which dispatchers heal/immunizes other nodes.
- Studies two versions of the model:
  - **Non-replicative patching**: There is a fixed set of dispatchers.
  - **Replicative patching**: When a node has been recovered it becomes a dispatcher.
- W.L.O.G I will focus on the non-replicative setting.

# System Model

- Studies the mean-field regime where $N \to \infty$
- Let $\beta_{ij}$ denote the rate at which nodes of type $i$ spread virus to type $j$ and let $\bar{\beta}_{ij}$ denote the rate at which dispatchers of type $i$ contact nodes of type $j$.
- When a dispatcher of type $j$ attempts to cure an infected node of type $i$ the cure is successful with probability $\pi_{j,i}$.
- Let $S_i(t), I_i(t), R_i(t)$ denote the fractions of susceptible, infected and recovered nodes of type $i$ at time $t$.
- The dynamics model is:

$$\dot{S}_i = -\sum_{j=1}^{M} \beta_{ji} I_j S_i - S_i \sum_{j=1}^{M} \bar{\beta}_{ji} R_j^0 u_j \tag{4}$$

$$\dot{I}_i = \sum_{j=1}^{M} \beta_{ji} I_j S_i - I_i \sum_{j=1}^{M} \pi_{ji} \bar{\beta}_{ji} R_j^0 u_j \tag{5}$$

- Initial conditions:

$$\boldsymbol{S}(0) = \boldsymbol{S}^0 \succeq 0, \quad \boldsymbol{I}(0) = \boldsymbol{I}^0 \succeq \boldsymbol{0} \tag{6}$$

# System Model

- Studies the mean-field regime where $N \to \infty$
- Let $\beta_{ij}$ denote the rate at which nodes of type $i$ spread virus to type $j$ and let $\bar{\beta}_{ij}$ denote the rate at which dispatchers of type $i$ contact nodes of type $j$.
- When a dispatcher of type $j$ attempts to cure an infected node of type $i$ the cure is successful with probability $\pi_{j,i}$.
- Let $S_i(t), I_i(t), R_i(t)$ denote the fractions of susceptible, infected and recovered nodes of type $i$ at time $t$.
- The dynamics model is:

$$\dot{S}_i = -\sum_{j=1}^{M} \beta_{ji} I_j S_i - S_i \sum_{j=1}^{M} \bar{\beta}_{ji} R_j^0 u_j \tag{7}$$

$$\dot{I}_i = -\sum_{j=1}^{M} \beta_{ji} I_j S_i - I_i \sum_{j=1}^{M} \pi_{ji} \bar{\beta}_{ji} R_j^0 u_j \tag{8}$$

- Initial conditions:

$$\boldsymbol{S}(0) = \boldsymbol{S}^0 \succeq 0, \quad \boldsymbol{I}(0) \succeq \boldsymbol{0} \tag{9}$$

# System Model

- Studies the mean-field regime where $N \to \infty$
- Let $\beta_{ij}$ denote the rate at which nodes of type $i$ spread virus to type $j$ and let $\bar{\beta}_{ij}$ denote the rate at which dispatchers of type $i$ contact nodes of type $j$.
- When a dispatcher of type $j$ attempts to cure an infected node of type $i$ the cure is successful with probability $\pi_{j,i}$.
- Let $S_i(t), I_i(t), R_i(t)$ denote the fractions of susceptible, infected and recovered nodes of type $i$ at time $t$.
- The dynamics model is:

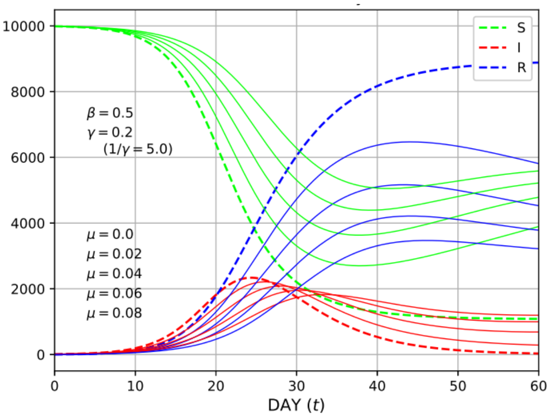
$$\dot{S}_i = -\sum_{j=1}^{M} \beta_{ji} I_j S_i - S_i \sum_{j=1}^{M} \bar{\beta}_{ji} R_j^0 u_j \tag{10}$$

$$\dot{I}_i = -\sum_{j=1}^{M} \beta_{ji} I_j S_i - I_i \sum_{j=1}^{M} \pi_{ji} \bar{\beta}_{ji} R_j^0 u_j \tag{11}$$

- Initial conditions:

$$\boldsymbol{S}(0) = \boldsymbol{S}^0 \succeq 0, \quad \boldsymbol{I}(0) \succeq \boldsymbol{0} \tag{12}$$

# Formulation of the Optimal Control Problem



- We are somewhere on the x-axis. Depending on the control signal $u(t)$ (how aggressive patching do we use?) the epidemic will evolve in different ways
- Aggressive patching is costly but can help reach herd immunity faster

# Formulation of the Optimal Control Problem

- Let $f(\boldsymbol{I})$ and $h_i(u_i)$ denote the cost of infection and patching, respectively.
- Let $L(\boldsymbol{R})$ denote the reward of recovered/patching nodes.
- The total cost can then be defined as

$$J = \int_0^{t_f} \left( f(\boldsymbol{I}) - L(\boldsymbol{R}) + \sum_{i=1}^{M} R_i^0 h_i(u_i) \right) dt \tag{13}$$

# Formulation of the Optimal Control Problem

We have the control problem on Lagrange form

$$\min_{\boldsymbol{u}(\cdot)} \left[ \int_0^{t_f} \left( f(\boldsymbol{I}) - L(\boldsymbol{R}) + \sum_{i=1}^{M} R_i^0 h_i(u_i) \right) dt \right]$$

$$\text{subject to} \begin{cases} \dot{S}_i = \overbrace{-\sum_{j=1}^{M} \beta_{ji} I_j(t) S_i(t) - S_i(t) \sum_{j=1}^{M} \bar{\beta}_{ji} R_j^0 u_j(t)}^{v_i} \\ \dot{I}_i = \overbrace{-\sum_{j=1}^{M} \beta_{ji} I_j(t) S_i(t) - I_i(t) \sum_{j=1}^{M} \pi_{ji} \bar{\beta}_{ji} R_j^0 u_j(t)}^{\mu_i} \\ \boldsymbol{S}(0) = \boldsymbol{S}^0 \\ \boldsymbol{I}(0) = \boldsymbol{I}^0 \\ \boldsymbol{u}(t) \in [0,1] & \forall t \in [0, t_f] \end{cases}$$

# Analysis of the Optimal Controller using PMP

- Hamiltonian:

$$H(t, \boldsymbol{u}, \boldsymbol{I}, \boldsymbol{R}, \boldsymbol{\lambda}) = f(\boldsymbol{I}) - L(\boldsymbol{R}) + \sum_{i=1}^{M} R_i^0 h_i(u_i) + \sum_{i=1}^{m} (\lambda_i^S v_i + \lambda_i^I \mu_i)$$

- Adjoint equations:

$$\begin{aligned} \dot{\lambda}_i^S &= -\frac{\partial H}{\partial S_i} & \forall i \in \{1, \ldots, M\} \\ \dot{\lambda}_i^I &= -\frac{\partial H}{\partial I_i} & \forall i \in \{1, \ldots, M\} \end{aligned}$$

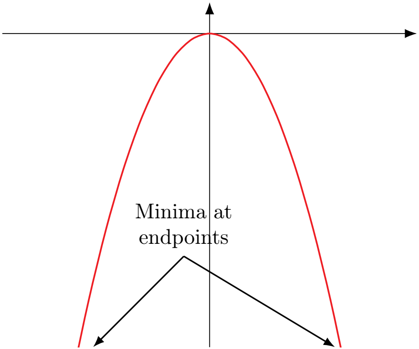
- Since there is no terminal cost, the transversality conditions are $\lambda_i^S(t_f) = \lambda_i^I(t_f) = 0$.

# Analysis of the Optimal Controller using PMP

- Recall that the first condition of PMP is that $u^*(t)$ should minimize the Hamiltonian pointwise:

$$u^*(t) = \tilde{\mu}(t, \boldsymbol{I}(t), \boldsymbol{R}(t), \boldsymbol{\lambda}(t)) = \arg\min_{u} H(t, \boldsymbol{I}(t), \boldsymbol{R}(t), \boldsymbol{u}(t), \boldsymbol{\lambda}(t))$$

- By assumption, $H$ is concave in $u$:



# Analysis of the Optimal Controller using PMP

- Since $u(t)_i \in [0,1]$, we have that $u^*(t) \in \{0,1\}$ for all $t$.
- We note that $u^*(t) = 0 \implies H(t) = 0$.
- Let the cost of the Hamiltonian when $u^*(t) = 1$ be denoted by $H(u = 1)$.
- We then have that a necessary condition for any optimal controller is:

$$u^*(t) = \begin{cases} 1 & \text{if } H(u=1) < 0 \\ [0,1] & \text{if } H(u=1) = 0 \\ 0 & \text{if } H(u=1) > 0 \end{cases} \tag{14}$$

- Hence $H(u = 1)$ is a switching function. If we take the time derivative $\dot{H}(u = 1)$ at the point where $\dot{H}(u = 1) = 0$ we see that the derivative has constant sign, which means that at most one switch can occur.

# Analysis of the Optimal Controller using PMP

- Since $u(t)_i \in [0,1]$, we have that $u^*(t) \in \{0,1\}$ for all $t$.
- We note that $u^*(t) = 0 \implies H(t) = 0$.
- Let the cost of the Hamiltonian when $u^*(t) = 1$ be denoted by $H(u = 1)$.
- We then have that a necessary condition for any optimal controller is:

$$u^*(t) = \begin{cases} 1 & \text{if } H(u=1) < 0 \\ [0,1] & \text{if } H(u=1) = 0 \\ 0 & \text{if } H(u=1) > 0 \end{cases} \tag{15}$$

- Hence $H(u = 1)$ is a switching function. If we take the time derivative $\dot{H}(u = 1)$ at the point where $\dot{H}(u = 1) = 0$ we see that the derivative has constant sign, which means that at most one switch can occur.

# Analysis of the Optimal Controller using PMP

- Since $u(t)_i \in [0,1]$, we have that $u^*(t) \in \{0,1\}$ for all $t$.
- We note that $u^*(t) = 0 \implies H(t) = 0$.
- Let the cost of the Hamiltonian when $u^*(t) = 1$ be denoted by $H(u = 1)$.
- We then have that a necessary condition for any optimal controller is:

$$u^*(t) = \begin{cases} 1 & \text{if } H(u=1) < 0 \\ [0,1] & \text{if } H(u=1) = 0 \\ 0 & \text{if } H(u=1) > 0 \end{cases} \tag{16}$$

- Hence $H(u = 1)$ is a switching function. If we take the time derivative $\dot{H}(u = 1)$ at the point where $\dot{H}(u = 1) = 0$ we see that the derivative has constant sign, which means that at most one switch can occur.

# Analysis of the Optimal Controller using PMP

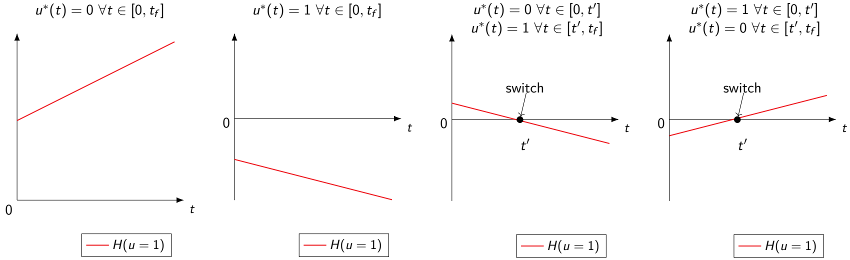
- Since $u(t)_i \in [0,1]$, we have that $u^*(t) \in \{0,1\}$ for all $t$.
- We note that $u^*(t) = 0 \implies H(t) = 0$.
- Let the cost of the Hamiltonian when $u^*(t) = 1$ be denoted by $H(u = 1)$.
- We then have that a necessary condition for any optimal controller is:

$$u^*(t) = \begin{cases} 1 & \text{if } H(u=1) < 0 \\ [0,1] & \text{if } H(u=1) = 0 \\ 0 & \text{if } H(u=1) > 0 \end{cases} \tag{17}$$

- Hence $H(u = 1)$ is a switching function. If we take the time derivative $\dot{H}(u = 1)$ at the point where $\dot{H}(u = 1) = 0$ we see that the derivative has constant sign, which means that at most one switch can occur.

# Analysis of the Optimal Controller using PMP

- Since $\dot{H}(u = 1)$ always has the same sign when $H(u = 1) = 0$, at most one switch can occur.
- This means that there are four possible switching sequences are $(0), (1), (0, 1), (1, 0)$:



The switching function $H(u = 1)$ defines four cases for the bang-bang controller $u^*(t)$.

# Analysis of the Optimal Controller using PMP

- Based on certain assumptions the sign of $\dot{H}(u=1)$ is positive $H(u=1, t=0) < 0$ and $H(u=1, t=t_f) > 0$, which means that the optimal control has the form:

$$u^*(t) = \begin{cases} 1 & \text{if } t < t_i \\ 0 & \text{if } t \geq t_i \end{cases} \tag{18}$$

- Which is the main theorem of the paper.

- **What does this structural result mean intuitively?**
  - Patch as much as possible in the beginning to achieve herd immunity
  - Once herd immunity is achieved, don't patch anything.

# Analysis of the Optimal Controller using PMP

- Based on certain assumptions the sign of $\dot{H}(u = 1)$ is positive $H(u = 1, t = 0) < 0$ and $H(u = 1, t = t_f) > 0$, which means that the optimal control has the form:

$$u^*(t) = \begin{cases} 1 & \text{if } t < t_i \\ 0 & \text{if } t \geq t_i \end{cases} \tag{19}$$

- Which is the main theorem of the paper.

- **What does this structural result mean intuitively?**
  - Patch as much as possible in the beginning to achieve herd immunity
  - Once herd immunity is achieved, don't patch anything.

# Outline

- **Background**
  - Malware epidemics
  - Stratified epidemic models
  - Pontryagin's maximum principle
- **The Paper**
  - Approach
  - System model
  - Formulation of the optimal control problem
  - Analysis of the optimal controller using Pontryagin's principle
- **Conclusions**
- **Discussion**
  - Strong points
  - Limitations of the paper

# Conclusions

- This paper studied malware epidemics from a control-theoretic perspective
- Formulated the problem of optimal patching to contain malware spread as an optimal control problem
- Derived that the optimal controller has a bang-bang structure.

# Discussions

- Is their patching model realistic?
  - Do you really deploy patching nodes that “spread” their patches in a decentralized manner?
- Is their spreading model realistic?
  - Do malwares spread in the same way as biological viruses?
- Other use cases in cyber security where similar approaches are applicable?
- Questions?