# Secure-by-Construction Optimal Path Planning for Linear Temporal Logic Tasks

**Shuo Yang**[1], **Xiang Yin**[1], **Shaoyuan Li**[1] **& Majid Zamani**[2,3]

[1]Department of Automation, Shanghai Jiao Tong University

[2]Computer Science Department, University of Colorado Boulder

[3]Computer Science Department, Ludwig Maximilian University of Munich

**xiang-yang@sjtu.edu.cn**

**IEEE Conference on Decision and Control (CDC)**

**Dec 14-18, 2020, Jeju Island, Republic of Korea (virtual)**

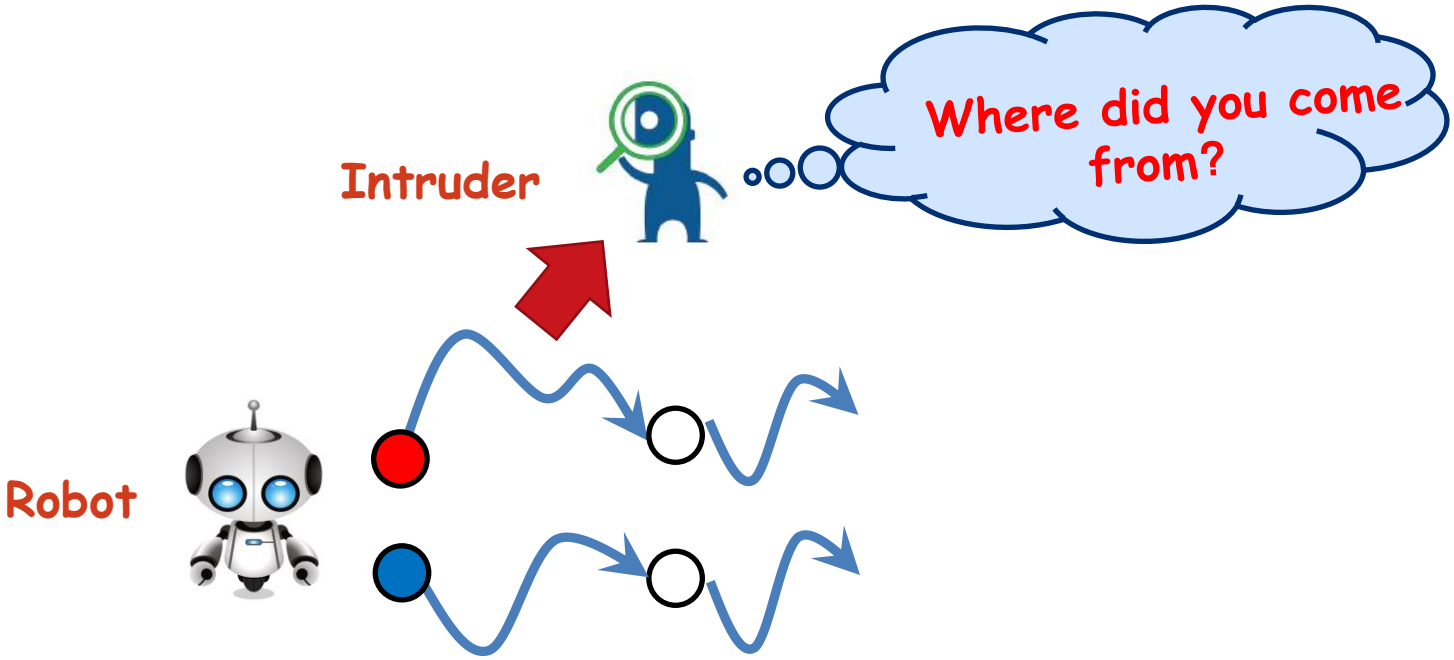
上海交通大學 SHANGHAI JIAO TONG UNIVERSITY

# Introduction



## Motivation

- Path planning is a fundamental problem in robotics
- Temporal-logic-based high-level path planning for complex tasks
- **Security** concerns in temporal-logic-based planning
- Outside intruder may infer robot's secret information

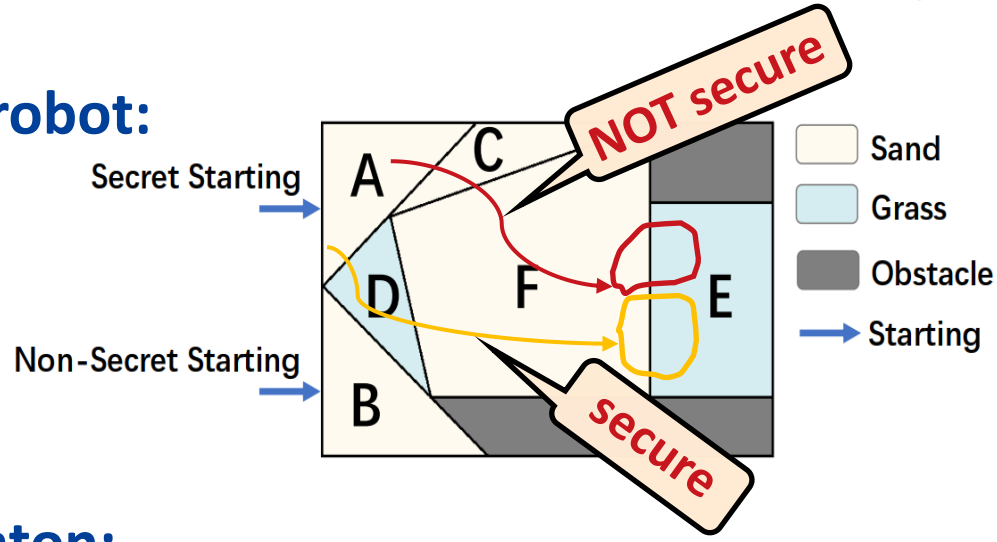


# Motivating Example

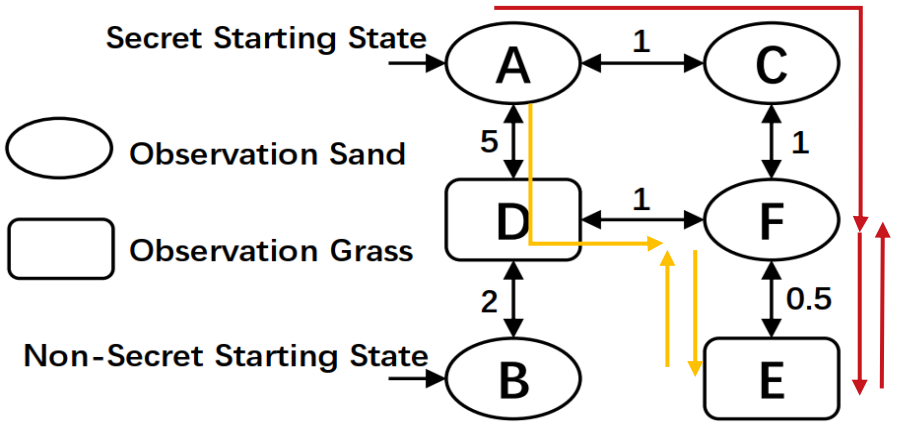


**Task: deliver goods between E and F (visit F and E infinitely often)**

## Work space of the single robot:




## The specification automaton:



# Weighted Transition System



**(Weighted Transition System) A weighted transition system (WTS) is a 6-tuple $T = (Q, Q_0, \rightarrow, w, AP, L)$, where $Q$ is the set of states, $Q_0 \subseteq Q$ is the set of initial states, $\rightarrow \subseteq Q \times Q$ is the transition relation, $w: Q \times Q \rightarrow R_+$ is a cost function, $AP$ is the set of atomic propositions and $L: Q \rightarrow 2^{AP}$ is the labelling function.**

- **The cost of a finite path:**

$$J(\tau) = \sum_{i=1}^{|\tau|-1} w(\tau(i), \tau(i+1))$$

- **Output function: $H: Q \rightarrow Y$, where $Y$ is the set of output.**
- **External path: $H(\tau) = H(\tau(1))\, H(\tau(2)) \ldots \in Y^{\omega}$**

# Linear Temporal Logic and Buchi Automata



A Linear Temporal Logic (LTL) formula is constructed based on atomic propositions, Boolean, and temporal operators.

$$\phi ::= true \mid p \mid \phi_1 \wedge \phi_2 \mid \neg\phi \mid \bigcirc\phi \mid \phi_1 U \phi_2$$

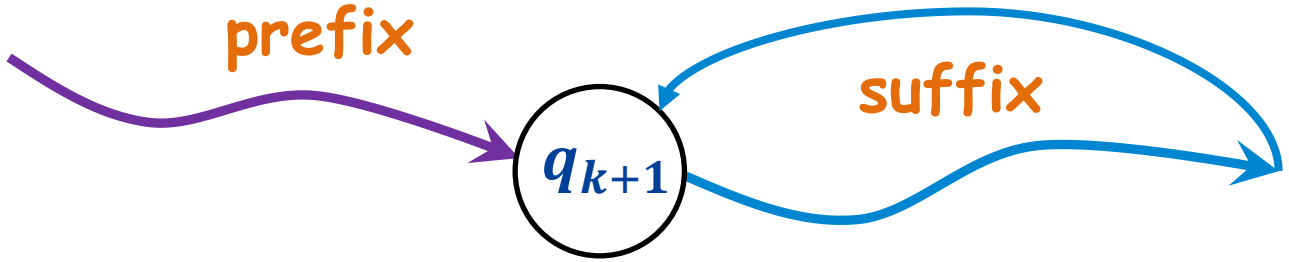
(Nondeterministic Buchi Automaton) A Nondeterministic Buchi Automaton (NBA) is a 5-tuple B= $(Q_B, Q_{0,B}, \Sigma, \rightarrow_B, F_B)$, where $Q_B$ is the set of states, $Q_{0,B} \subseteq Q_B$ is the set of initial states,$\Sigma$ is an alphabet, $\rightarrow_B \subseteq Q_B \times \Sigma \times Q_B$ is the transition relation and $F_B \subseteq Q_B$ is the set of accepting states.

For any LTL formula $\phi$, there always exists an NBA over $\Sigma = 2^{AP}$ that accepts exactly all infinite words satisfying $\phi$, i.e., $\mathcal{L}(B) = \text{Words}(\phi)$.

# Temporal Logic Path Planning



- **Standard LTL path planning problem: find an infinite path $\tau \in \mathbf{Path}^{\omega}(T)$ such that** $\mathrm{trace}(\tau) \vDash \phi$.
- **Prefix-Suffix structure:** $\tau = q_1 \dots q_k [\, q_{k+1} \dots q_{k+m} ]^{\omega} \in \mathbf{Path}^{\omega}(T)$
- **The cost of an infinite plan:** $\hat{J}(\tau) = J(\, q_1 \dots q_k \, q_{k+1} \dots q_{k+m} \, q_{k+1})$




$$\hat{J}(\tau) = J_{pre} + J_{suf}$$
$$= J(\, q_1 \dots q_k \, q_{k+1}) + J(q_{k+1} \dots q_{k+m} \, q_{k+1})$$

# Security



**(Security) Let $T = (Q, Q_0, \rightarrow, w, AP, L, H, Y, Q_S)$ be a WTS. An infinite path $\tau \in \mathbf{Path}^{\omega}(T)$ is said to be *secure* if there exists an infinite path $\tau' \in \mathbf{Path}^{\omega}(T)$ such that $\tau'(1) \notin Q_S$ and $H(\tau) = H(\tau')$**

- **Consider security as protecting the initial state of robot's path;**
- **For any secure path starting from secret state, there exists another observation-equivalent path starting from non-secret state.**

**Intruder model**

- **Knows the mobility of the robots, i.e., WTS *T*;**
- **Knows the external path generated by the robot, i.e., $H(\tau)$.**

# Problem Formulation

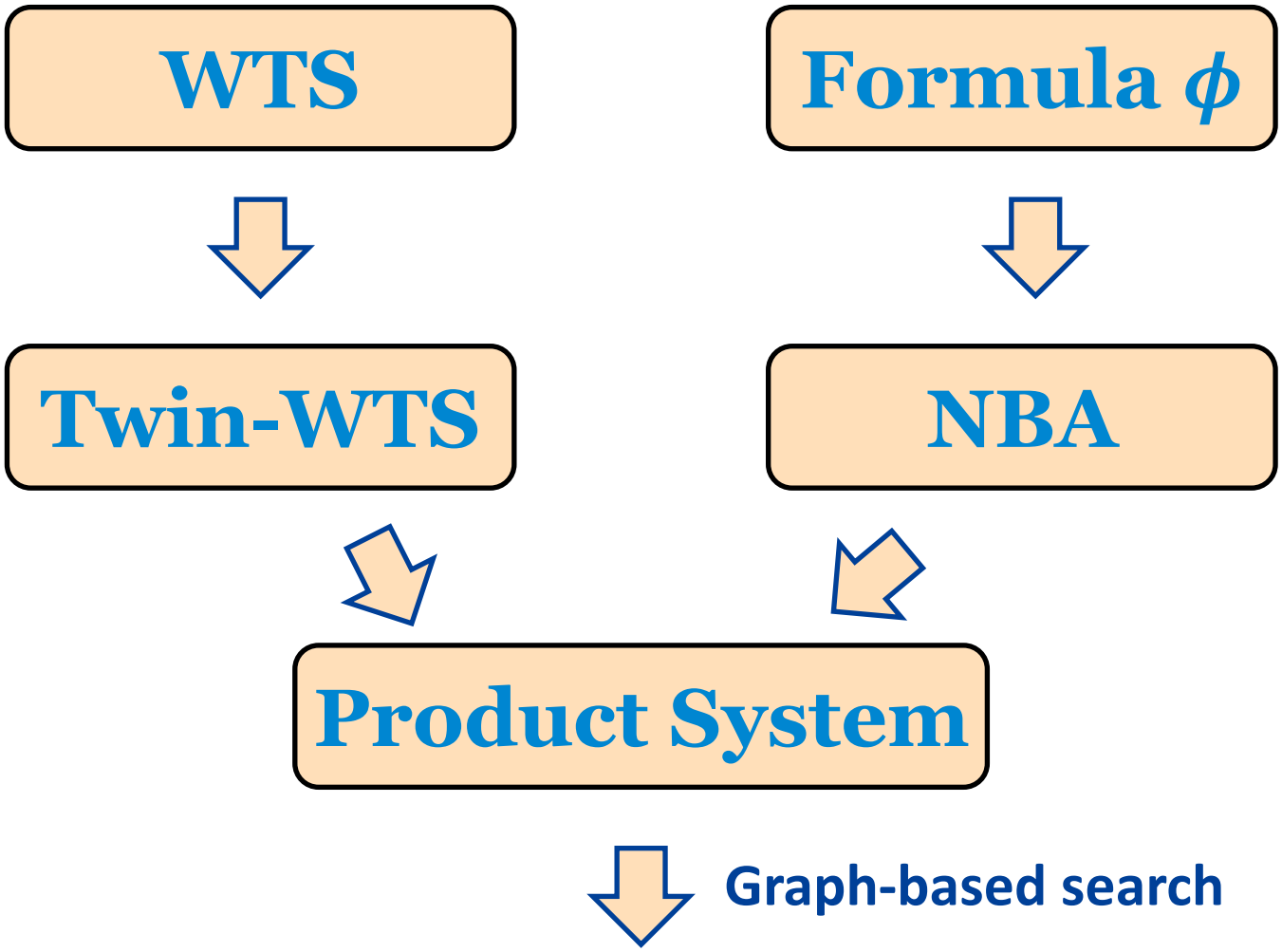


**(Security-Aware Optimal Path Planning Problem) Given a WTS $T$, secret states $Q_S \subseteq Q$, output function $H: Q \to Y$ and LTL formula $\phi$, for each possible initial-state $q_0 \in Q_0$, determine a plan: $\tau = \in \mathbf{Path}^{\omega}(T)$ with $\tau(1) = q_0$ such that the following conditions hold**

1) trace$(\tau) \vDash \phi$;
2) **$\tau$ is secure**
3) **For any other plan $\tau' = \in \mathbf{Path}^{\omega}(T)$ satisfying the above requirements, we have $\hat{J}(\tau) \leq \hat{J}(\tau')$.**

# Procedure Outline





# Twin-WTS



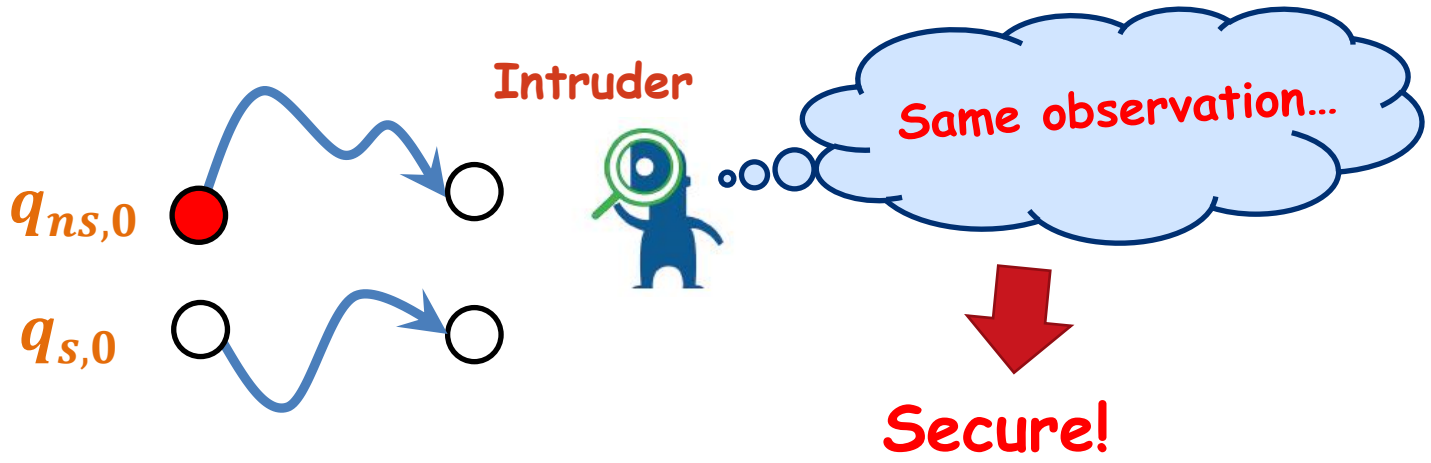
(Twin-WTS) Given a WTS $T = (Q, Q_0, \rightarrow, w, AP, L, H, Y, Q_S)$, its twin-WTS is a new WTS $V = (X, X_0, \rightarrow_V, w_V, AP, L_V)$, where

- $X \subseteq Q \times Q$ is the set of states,
- $X_0 = \{(q_1, q_2) \in Q_0 \times Q_0 : H(q_1) = H(q_2)\}$ is the set of initial states,
- $\rightarrow_V \subseteq X \times X$ is the transition relation defined by: for any $x = (q_1, q_2) \in X$ and $x' = (q'_1, q'_2) \in X$, we have $(x, x') \in \rightarrow_V$ if the followings hold:
  - $(q_1, q'_1) \in \rightarrow$;
  - $(q_2, q'_2) \in \rightarrow$;
  - $H(q'_1) = H(q'_2)$.
- $w_V : X \times X \rightarrow R_+$ is a cost function defined by: for any $x = (q_1, q_2) \in X$ and $x' = (q'_1, q'_2) \in X$, we have $w_V(x, x') = w(q_1, q'_1)$;
- $L_V : X \rightarrow 2^{AP}$ is the labelling function defined by: for any $x = (q_1, q_2) \in X$, we have $L_V(x) = L_V(q_1)$.

# Twin-WTS



- Track two internal paths generating the same external path
- The size of $V$ is polynomial in the size of $T$: it contains at most $|\mathrm{Q}|^2$ states.
- Capture the security constraint: For any secure path starting from a secret initial state $q_{s,0}$, there must exist an observation-equivalent path from a non-secret initial state $q_{ns,0}$. Such a path-pair exists in the twin-WTS $V$ from state $(q_{s,0}, q_{ns,0})$.



# Product System



**(Product System) Given a twin-WTS $V = (X, X_0, \rightarrow_V, w_V, AP, L_V)$ and NBA $B = (Q_B, Q_{0,B}, \Sigma, \rightarrow_B, F_B)$, the product of $V$ and $B$ is a new (unlabeled) WTS $T_\otimes = (Q_\otimes, Q_{0,\otimes}, \rightarrow_\otimes, w_\otimes)$, where**

- **$Q_\otimes \subseteq X \times Q_B$ is the set of states,**
- **$Q_{0,\otimes} = X_0 \times Q_{0,\otimes}$ is the set of initial states,**
- **$\rightarrow_\otimes \subseteq Q_\otimes \times Q_\otimes$ is the transition relation defined by: for any $q_\otimes = (x, q_B) \in Q_\otimes$ and $q'_\otimes = (x', q'_B) \in Q'_\otimes$, we have $(q_\otimes, q'_\otimes) \in \rightarrow_\otimes$ if the followings hold:**
  - **$(x, x') \in \rightarrow_V$;**
  - **$(q_B, L_V(x), q'_B) \in \rightarrow_B$.**
- **$w_\otimes: Q_\otimes \times Q_\otimes \rightarrow R_+$ is the cost function defined by: for any $q_\otimes = (x, q_B) \in Q_\otimes$ and $q'_\otimes = (x', q'_B) \in Q'_\otimes$, we have $w_\otimes(q_\otimes, q'_\otimes) = w(x, x')$;**

# Planning Algorithm



**Algorithm 1:** Security-Aware Optimal LTL Plan

**input** : LTL formula $\phi$, WTS $T$ with $H$ and $Q_S$, initial state $q_0$
**output**: Optimal plan $\tau$ from $q_0 \in Q_0$

Convert $\phi$ to NBA $B = (Q_B, Q_{0,B}, \Sigma, \rightarrow_B, F_B)$;
Construct twin-WTS $V = (X, X_0, \rightarrow_V, w_V, \mathcal{AP}, L_V)$;
Construct the product of $V$ and $B$ $T_\otimes = (Q_\otimes, Q_{0,\otimes}, \rightarrow_\otimes, w_\otimes)$;
**if** $\mathit{Reach}(\textsc{Int}_{q_0}(T_\otimes)) \cap \textsc{Goal}(T_\otimes) = \emptyset$ **then**
    **return** "no feasible plan from $q_0$";
**else**
    **for** $q_I \in \textsc{Int}_{q_0}(T_\otimes)$ **do**
        **for** $q_G \in \mathit{Reach}(\{q_I\}) \cap \textsc{Goal}(T_\otimes)$ **do**
            $\tau^{q_I,q_G} = \Pi[\mathtt{Shortpath}(q_I, q_G)]$;
            $\tau^{q_G,q_G} = \Pi[\mathtt{Shortpath}(q_G, q_G)]$;
        **end**
    **end**
    $(q_I^*, q_G^*) = \arg\min_{(q_I,q_G)} \hat{J}(\tau^{q_I,q_G}[\tau^{q_G,q_G}]^\omega)$;
    **return** optimal plan $\tau = \tau^{q_I^*,q_G^*}[\tau^{q_G^*,q_G^*}]^\omega$ for $q_0$;
**end**

- $\textsc{Int}_{q_0}(T_\otimes) \subseteq Q_{0,\otimes}$ is the set of initial states whose first components are $q_0$ while second components are non-secret states in $T$;
- $\textsc{Goal}(T_\otimes) \subseteq Q_{0,\otimes}$ is the set of states whose last components are in $F_B$ and they are in some cycles of $T_\otimes$;
- Find an optimal path of the form:

$$\textsc{Int}_{q_0}(T_\otimes) \rightarrow (\textsc{Goal}(T_\otimes) \rightarrow \textsc{Goal}(T_\otimes))^\omega$$

# Planning Algorithm



**Algorithm 1:** Security-Aware Optimal LTL Plan

**input** : LTL formula $\phi$, WTS $T$ with $H$ and $Q_S$, initial state $q_0$

**output**: Optimal plan $\tau$ from $q_0 \in Q_0$

1 Convert $\phi$ to NBA $B = (Q_B, Q_{0,B}, \Sigma, \rightarrow_B, F_B)$;
2 Construct twin-WTS $V = (X, X_0, \rightarrow_V, w_V, \mathcal{AP}, L_V)$;
3 Construct the product of $V$ and $B$ $T_\otimes = (Q_\otimes, Q_{0,\otimes}, \rightarrow_\otimes, w_\otimes)$;
4 **if** $\mathtt{Reach}(\textsc{Int}_{q_0}(T_\otimes)) \cap \textsc{Goal}(T_\otimes) = \emptyset$ **then**
5  **return** "no feasible plan from $q_0$";
6 **else**
7  **for** $q_I \in \textsc{Int}_{q_0}(T_\otimes)$ **do**
8  **for** $q_G \in \mathtt{Reach}(\{q_I\}) \cap \textsc{Goal}(T_\otimes)$ **do**
9  $\tau^{q_I, q_G} = \Pi[\mathtt{Shortpath}(q_I, q_G)]$;
10  $\tau^{q_G, q_G} = \Pi[\mathtt{Shortpath}(q_G, q_G)]$;
11  **end**
12  **end**
13  $(q_I^*, q_G^*) = \arg\min_{(q_I, q_G)} \hat{J}(\tau^{q_I, q_G}[\tau^{q_G, q_G}]^\omega)$;
14  **return** optimal plan $\tau = \tau^{q_I^*, q_G^*}[\tau^{q_G^*, q_G^*}]^\omega$ for $q_0$;
15 **end**

Constructions of NBA, twin-WTS, and product system

no feasible plan from the given initial state

prefix

suffix

Find the optimal plan among all feasible plans

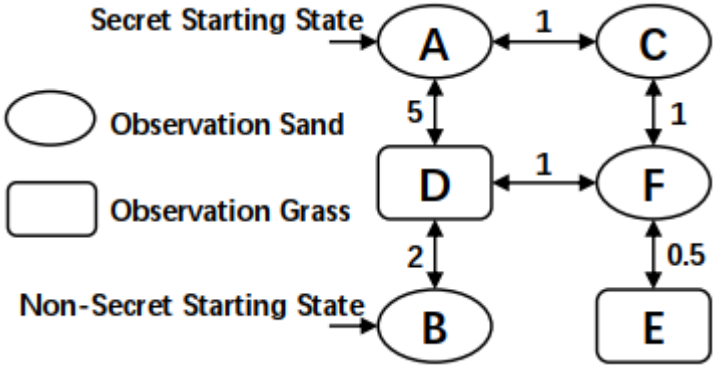
**Sound and complete!**

# Case Study

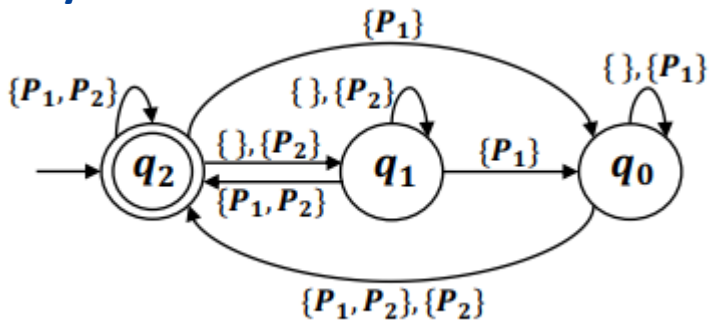


$L(F) = P_1, L(E) = P_2$

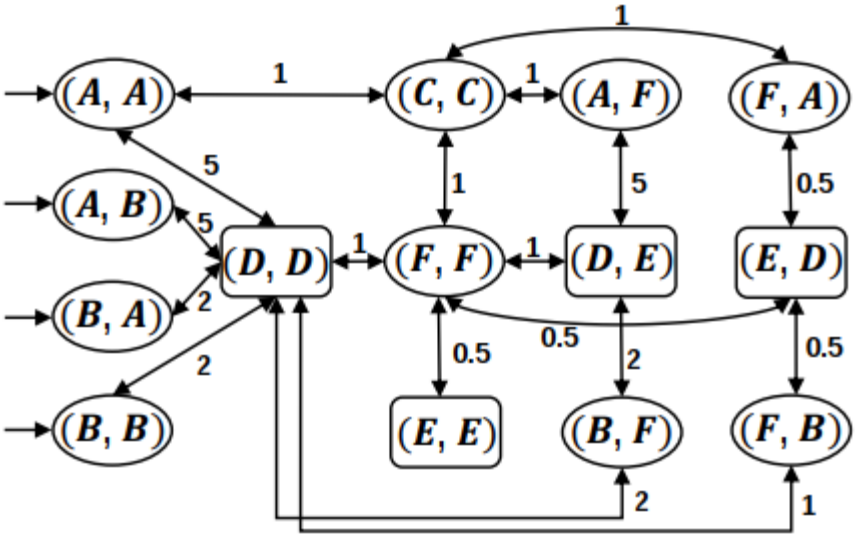
$L(q) = \emptyset$, for any other states



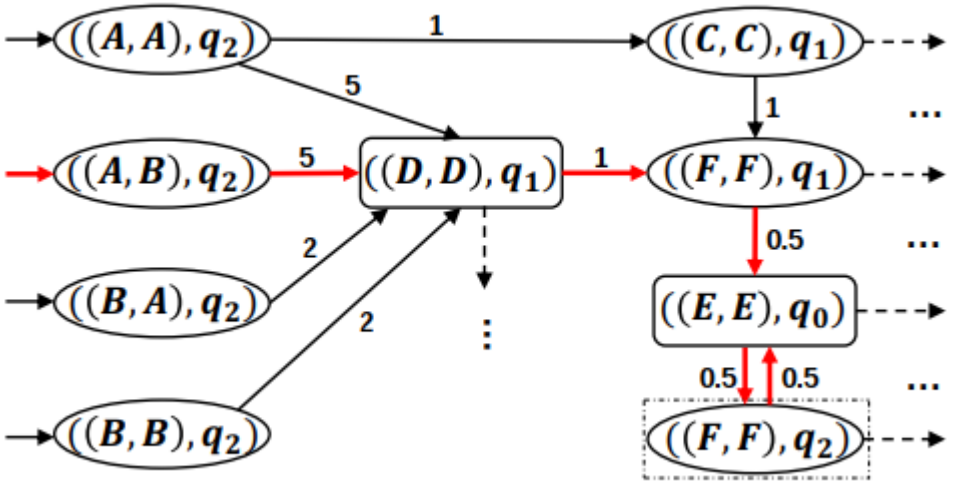

WTS




An NBA translated from $\phi$=□◇$P_1$ ∧ □◇$P_2$




Twin-WTS




$T_{\otimes}$

# Conclusion



## Contributions:

- Security-aware optimal path planning problem for LTL tasks
- Sound and complete algorithmic procedure
- Twin weighted transition systems
- Algorithm is polynomial in the size of system model

## Future Directions:

- Multi-robot systems
- Other types of security

**Thank You!**