Gui-lin Cai, Bao-sheng Wang, Qian-qian Xing, 2017. Game theoretic analysis for the mechanism of moving target defense. *Frontiers of Information Technology & Electronic Engineering*, **18**(12):2017-2034.
http://dx.doi.org/10.1631/FITEE.1601797

Game theoretic analysis for the mechanism of moving target defense

Front Inform Technol Electron Eng

Key words: Network security; Moving target defense; Defense mechanism; Defense model; Game theory

Contact: Gui-lin CAI
E-mail: caiguilin08@nudt.edu.cn
ORCID: http://orcid.org/0000-0002-9322-2539

Motivation

- Moving target defense (MTD) has emerged as one of the game-changing themes to alter the asymmetric situation between attacks and defenses in cyber-security.
- Numerous related works involving several facets of MTD have been published.
- Relevant analysis for the defense mechanism of the MTD technology is still absent.

Front Inform Technol Electron Eng

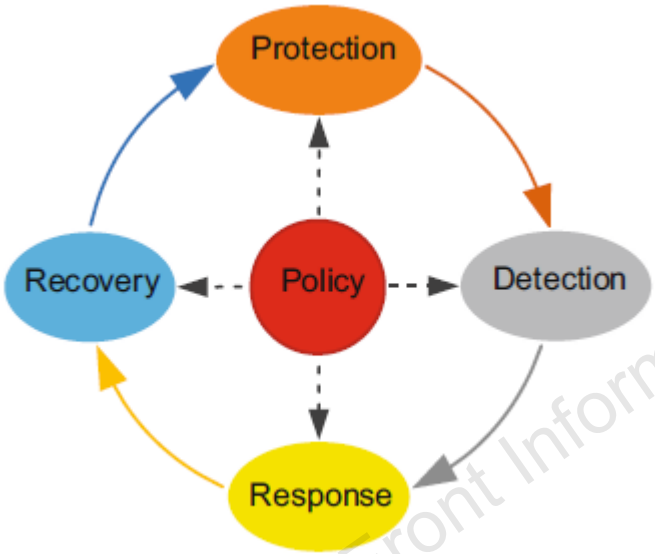
Main idea

1. Presenting a new defense model to describe the proactivity and effect of MTD technology intuitively.
   - A new security model MP2R is introduced to describe the changes on the defense paradigm and process.
2. Using the incomplete information dynamic game theory to verify the proactivity and effect of MTD technology.
   - Modeling the interaction between a defender who equips a server with different types of MTD techniques and a visitor who can be a user or an attacker.
   - Analyzing the equilibria and their conditions for these models.
   - Comparing with the equilibrium and its condition of an existing incomplete information dynamic game model for traditional defense.

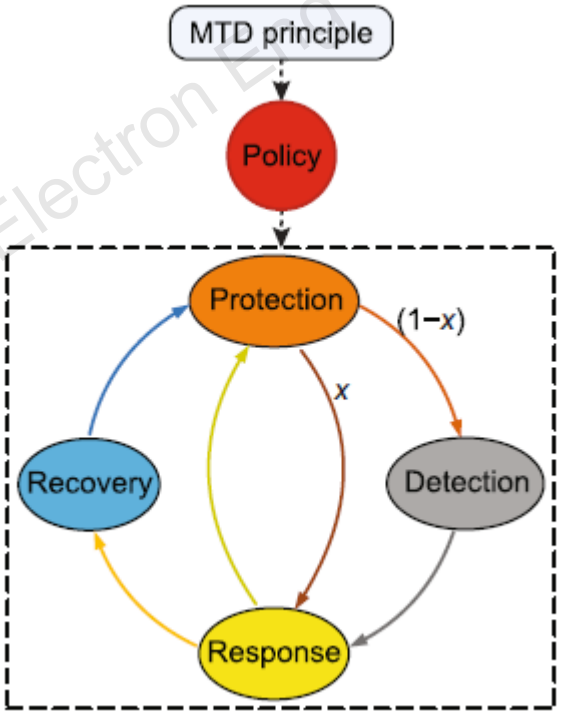
Front. Inform. Technol. Electron. Eng

Major results

1. The changes on the defense paradigm and process



(a) The PPDRR model for traditional defense



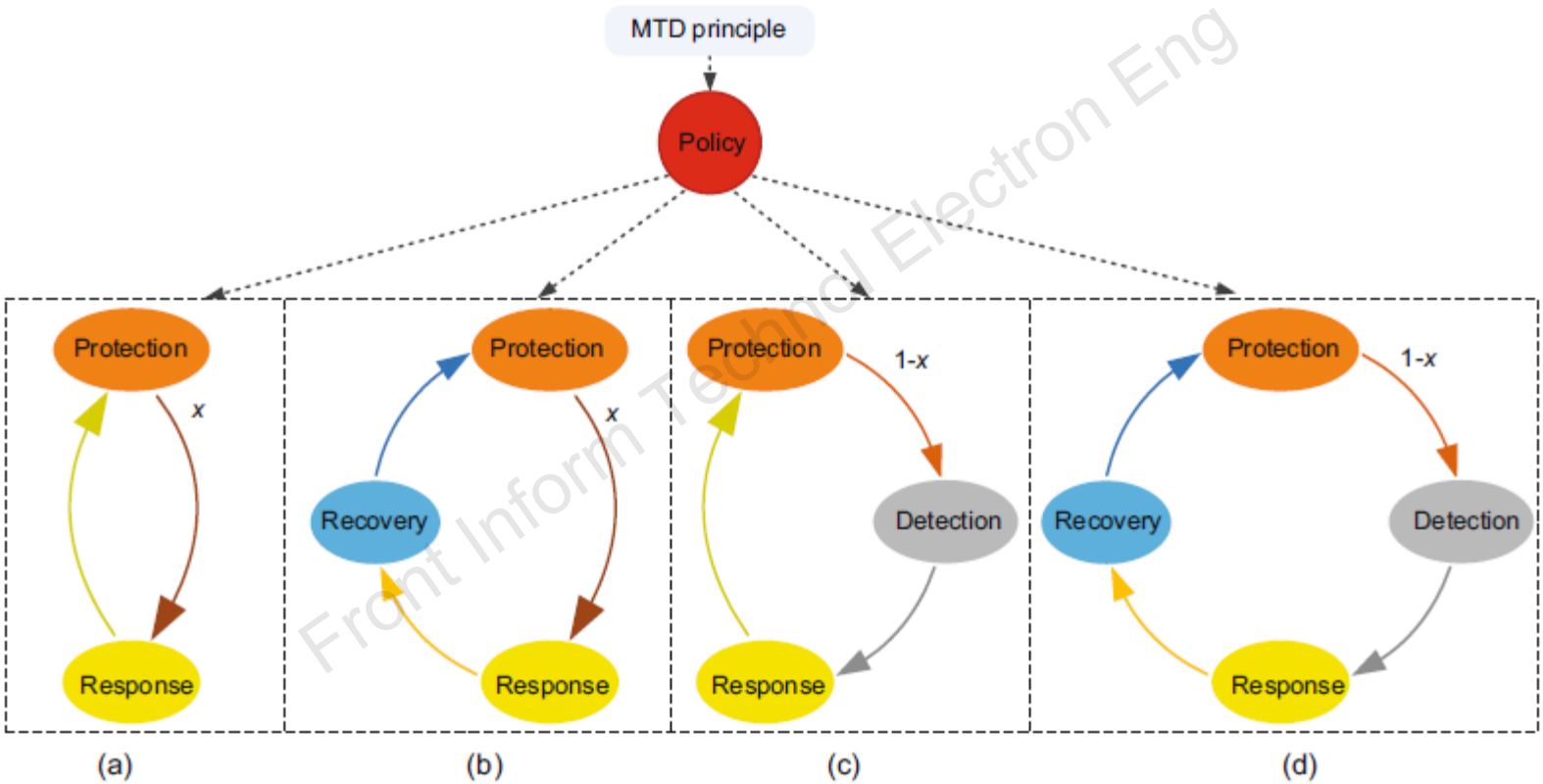
(b) The MP2R model for MTD

$0.5 < x < 1$, and the value of x is determined by the defender/administrator as a security-cost trade-off.

Front Inform Technol Electron Eng

Major results

1. The changes on the defense paradigm and process (Cont'd)

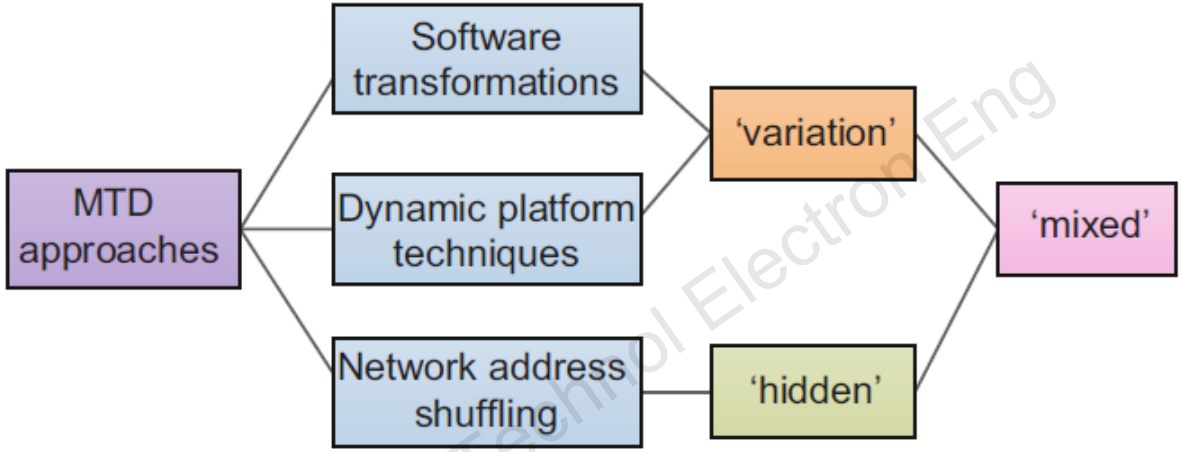


Front Inform Technol Electron Eng

The four complete and dynamic security cycles in MP2R

Major results

2. Classifying the major MTD approaches



The relationship between the categories and the running patterns of major MTDs

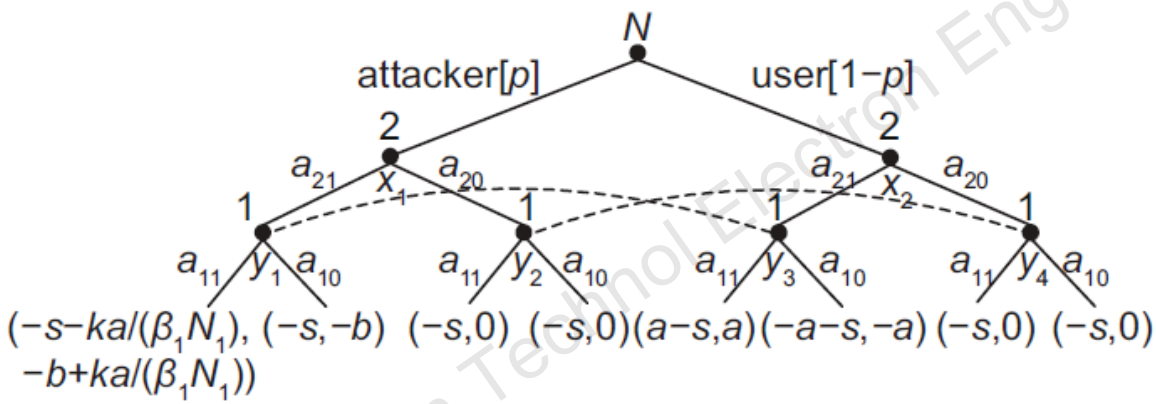
- 'variation' MTD :disrupt attack but cannot prevent the attacker to re-connecting with the target.
- 'hidden' MTD : make the attacker lose the target and thus break off the connection with the target.
- 'mixed' MTD: the combination of the "hidden" and "variation" MTD

Front Inform Technol Electron Eng

Major results

2.1 'Hidden' MTD

(1) The game model between the defender and attacker when deploying 'hidden' MTD



The extensive form presentation for the game with "hidden" MTD from the view of the defender

The equilibria for situation "hidden" and their conditions

Perfect Bayesian equilibrium	Condition
E_1 $((a_{11},(a_{21},a_{21})),p)$	$p<\frac{2}{2+k/(\beta_1 N_1)}$ and $\beta_1 N_1<\frac{ka}{b}$
E_2 $((a_{11},(a_{20},a_{21})),p)$	$\beta_1 N_1>\frac{ka}{b}$

Equilibrium	Condition
$(a_{11},(a_{21},a_{21}))$	$p<2/(2+k)$

The equilibrium and its condition for the game with traditional defense

Front Inform Technol Electron Eng

Major results

(2) Effect of the ‘hidden’ MTD

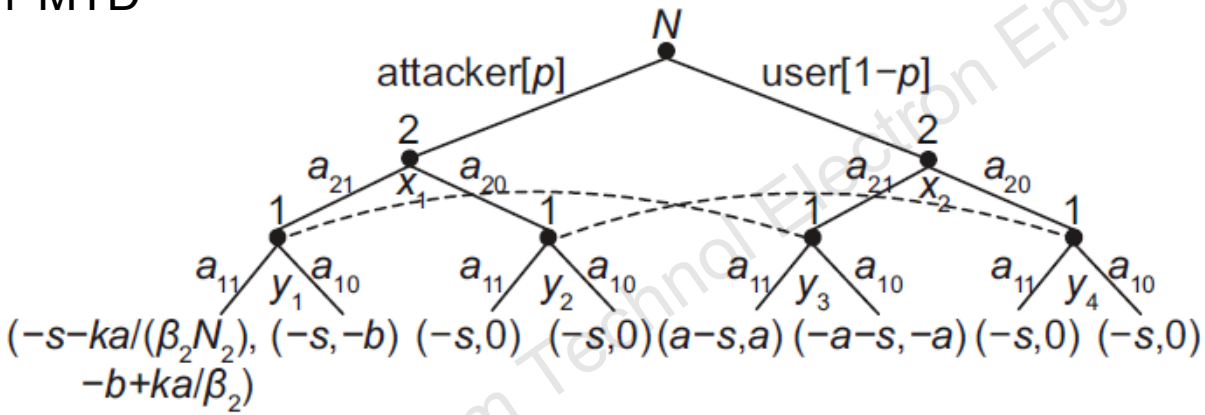
- The equilibrium E_1 is equivalent to the equilibrium result of the game when deploying traditional defense, but the conditions are changed.
- The conditions are not only related to the parameters *p* and *k* that are determined and controlled by the attacker, but also related to the parameters N_1 and β_1 that are determined and controlled by the defender.
- When the defender increases the value of $\beta_1 N_1$ under the limited condition that $\beta_1 N_1 < ka/b$, the attacker has to increase his attack probability to try to obtain his expected payoff.
- When the defender continues to increase the value of $\beta_1 N_1$ and make it satisfy the condition $\beta_1 N_1 > ka/b$, the equilibrium is changed to E_2 which means that the defender should provide service and user requests service normally while the attacker should stop attacking) to obtain his expected payoff.

Front Inform Technol Electron Eng

Major results

2.2 'Variation' MTD

(1) The game model between the defender and attacker when deploying 'variation' MTD



The extensive form presentation for the game with 'variation' MTD from the view of the defender

The equilibria for situation 'variation' and their conditions

Perfect Bayesian equilibrium	Condition
E_1 $((a_{11},(a_{21},a_{21})),p)$	$p<\dfrac{2}{2+k/(\beta_2 N_2)}$ and $\beta_2<\dfrac{ka}{b}$
E_2 $((a_{11},(a_{20},a_{21})),p)$	$\beta_2>\dfrac{ka}{b}$

Equilibrium	Condition
$(a_{11},(a_{21},a_{21}))$	$p<2/(2+k)$

The equilibrium and its condition for the game with traditional defense

Front Inform Technol Electron Eng

Major results

(2) Effect of the ‘variation’ MTD

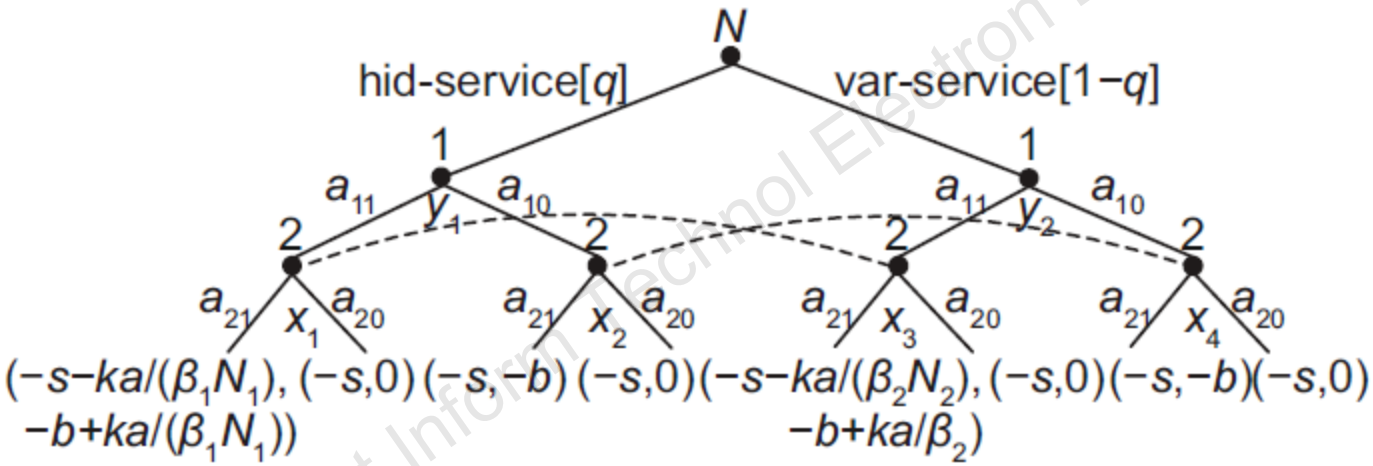
- The equilibrium E_1 is equivalent to the equilibrium result of the game when deploying traditional defense, but the conditions are changed.
- The conditions are not only related to the parameters *p* and *k* that are determined and controlled by the attacker, but also related to the parameters N_2 and β_2 that are determined and controlled by the defender.
- When the defender increases the value of $\beta_2 N_2$ under the limited condition that $\beta_2 < ka/b$, the attacker has to increase his attack probability to try to obtain his expected payoff
- When the defender continues to increase the value of β_2 and make it satisfy the condition $\beta_2 > ka/b$, the equilibrium is changed to E_2 which means that the defender should provide service and user requests service normally while the attacker should stop attacking) to obtain his expected payoff.

Front Inform Technol Electron Eng

Major results

2.3 ‘Mixed’ MTD

(1) The game model between the defender and attacker when deploying ‘mixed’ MTD



The extensive form presentation for the game with “mixed” MTD from the view of the attacker

Front Inform Technol Electron Eng

Major results

(1) The game model between the defender and attacker when deploying 'mixed' MTD (Cont'd)

Perfect Bayesian equilibrium	Condition
E_1 $(((a_{11}, a_{11}), (a_{21}, a_{21})), p)$	$p < \frac{2}{2+k/(\beta_1 N_1)}$ and $p < \frac{2}{2+k/(\beta_2 N_2)}$, and $\beta_2 < \beta_1 N_1 < \frac{ka}{b}$ or $p < \frac{2}{2+k/(\beta_1 N_1)}$ and $p < \frac{2}{2+k/(\beta_2 N_2)}$, and $q < \frac{1-\beta_2 b/(ka)}{1-\beta_2/(\beta_1 N_1)}$ when $\beta_2 < \frac{ka}{b} < \beta_1 N_1$
E_2 $(((a_{10}, a_{11}), (a_{21}, a_{21})), p)$	$\frac{2}{2+k/(\beta_1 N_1)} < p < \frac{2}{2+k/(\beta_2 N_2)}$, $q < \frac{1}{2}$, $q < 1 - \frac{\beta_2 b}{ka}$, and $\beta_2 < \frac{ka}{b}$, when $\beta_1 N_1 < \beta_2 N_2$,
E_3 $(((a_{11}, a_{10}), (a_{21}, a_{21})), p)$	$\frac{2}{2+k/(\beta_2 N_2)} < p < \frac{2}{2+k/(\beta_1 N_1)}$, $q > \frac{1}{2}$, $q > \frac{\beta_1 N_1 b}{ka}$, and $\beta_1 N_1 < \frac{ka}{b}$, when $\beta_1 N_1 > \beta_2 N_2$,
E_4 $(((a_{11}, a_{11}), (a_{20}, a_{21})), p)$	$q > \frac{1-\beta_2 b/(ka)}{1-\beta_2/(\beta_1 N_1)}$ when $\beta_1 N_1 > \frac{ka}{b} > \beta_2$ or $\beta_1 N_1 > \beta_2 > ka/b$

The equilibria for situation 'mixed' and their conditions

Equilibrium	Condition
$(a_{11}, (a_{21}, a_{21}))$	$p < 2/(2+k)$

The equilibrium and its condition for the game with traditional defense

Front Inform Technol Electron Eng

Major results

(2) Effect of the 'mixed' MTD

- The equilibrium E_1 – E_3 is equivalent to the equilibrium result of the game when deploying traditional defense, but the conditions are changed. The conditions are associated with not only parameters *p* and *k* determined and controlled by the attacker, but also the parameters β_1, β_2, N_1, N_2, and *q* that are determined and controlled by the defender
- From the conditions for equilibria E_1 - E_4, we can see that the defender can increase the value of β_2 and $\beta_1 N_1$ to force the attacker to increase his attack probability or even to not attack to obtain his expected payoff
- For equilibrium E_1, under the conditions $p < 2/\left(2 + k/\left(\beta_1 N_1\right)\right)$ and $p < 2/\left(2 + k/\left(\beta_1 N_1\right)\right)$, the defender can just increase the values of β_2 and $\beta_1 N_1$ without considering the value of *q*, to force the attacker to increase his/her attack probability if the attacker wants to obtain his/her expected payoff

Front Inform Technol Electron Eng

Major results

(2) Effect of the 'mixed' MTD (Cont'd)

- To increase the influence, the defender can continue to increase the values of β_2 and $\beta_1 N_1$. When the values of $\beta_1 N_1$ is increased to satisfy the limited condition $\beta_2 < ka/b < \beta_1 N_1$, he/she has to consider the range of factor *q*
  - When defender adjusts only the value of β_2 , the greater the shuffling frequency of the enabled 'variation' MTD, the stronger the ability to confuse attacker and disrupt attack
  - When defender adjusts only the value of $\beta_1 N_1$, i.e., if the defender sets a higher frequency or larger configuration space for the 'hidden' MTD, the probability that the defender has to enable the hid-service again is lower
- If the defender increases the value of *q* to make it satisfy $q > \left(1-\beta_2 b/(ka)\right)/\left(1-\beta_2/(\beta_1 N_1)\right)$, the equilibrium would change to E_4
- If the defender also increases the value of β_2 and makes it satisfy the limited condition $\beta_1 N_1 > \beta_2 > ka/b$, the equilibrium would still remain in E_4

From Inform Technol Electron Eng

Major results

(2) Effect of the 'mixed' MTD (Cont'd)

- For equilibrium E_2, the defender should just increase the value of β_2 to influence the action of the attacker.
  - Although the hid-service is not really serving, its existence can effectively confuse the attacker. But, with investigation and analysis, the belief that the defender actually provides only the var-service is gradually confirmed.
- For equilibrium E_3, the defender should just increase the value of $\beta_1 N_1$ to influence the action of the attacker.
  - Although the var-service is not really serving, its existence can effectively confuse the attacker. But, with investigation and analysis, the belief that the defender actually provides only the hid-service is gradually confirmed.

Front Inform Technol Electron Eng

Conclusions

- By comparing the MP2R model with the traditional PPDRR model, one can find the proactivity and effectiveness of MTD technology intuitively.
- By comparing the equilibria and their conditions of the game models when deploying different types of MTD with the equilibrium and its condition of the game when deploying traditional defense, we verified the proactivity and effectiveness of the MTD technology, and identified that the size of configuration space and the shifting frequency are the two key factors that would influence the effect of the MTD.

Front Inform Technol Electron Eng