KTH ROYAL INSTITUTE
OF TECHNOLOGY

Adversarial Attacks on Continuous Authentication Security: A Dynamic Game Approach

Serkan Sarıtaş[1] Ezzeldin Shereen[1]
Henrik Sandberg[2] György Dán[1]

[1]Division of Network and Systems Engineering, KTH Royal Institute of Technology, Sweden
[2]Division of Decision and Control Systems, KTH Royal Institute of Technology, Sweden

GameSec 2019 Stockholm, Sweden November 1, 2019

Continuous Authentication

Authenticating with

- movement
- facial features
- behavior
- voice
- . . .

Continuous Authentication

- **Workstations**: keystroke dynamics, mouse movements
- **Mobile/wearable electronic devices**: touch gestures, location, timing, hand movement, orientation and grasp (HMOG), . . .
- . . .

System Model

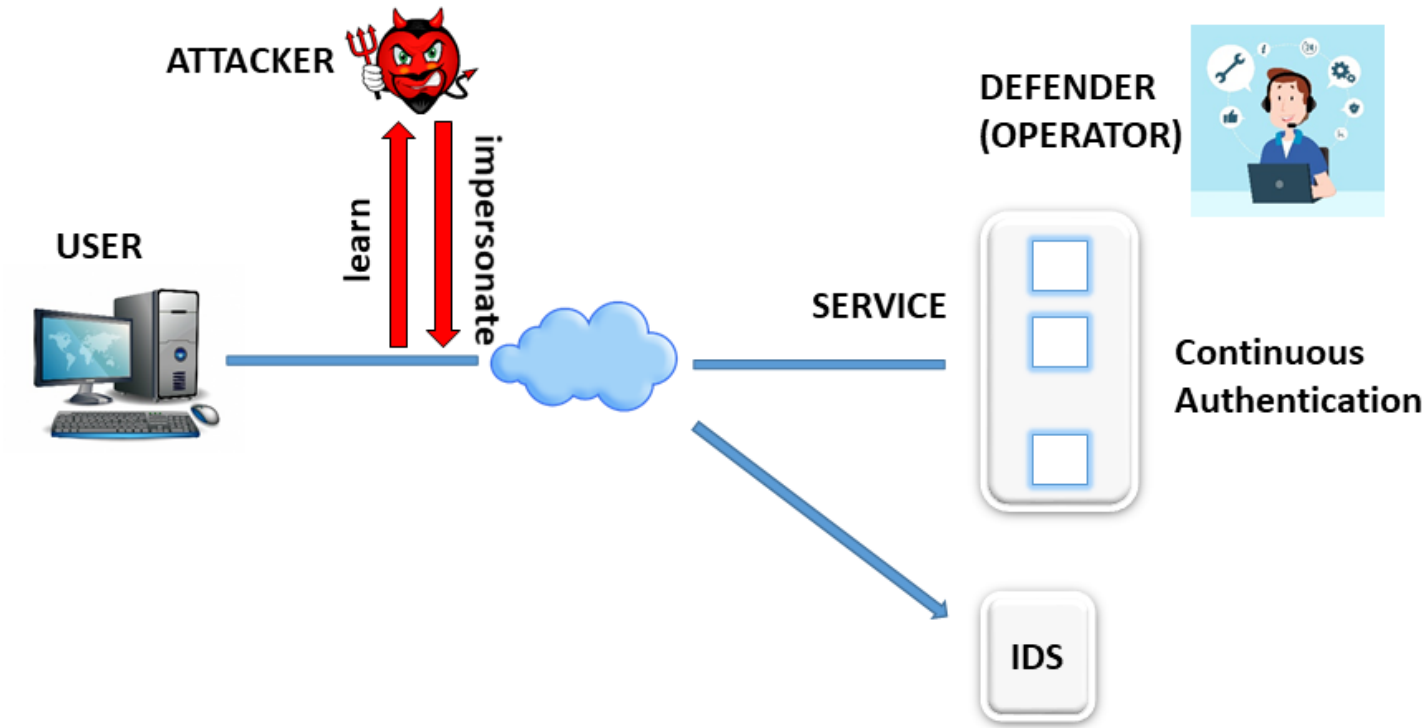


Figure: System model.

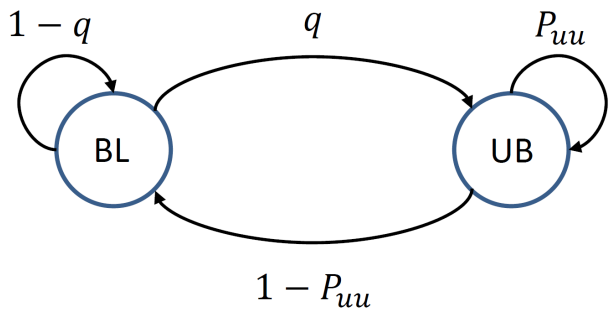
User Behavior

- Amount of user traffic in time-slot t
  $$\Lambda_u(t) \sim \text{Poisson}(\lambda_u)$$
- User behavior $\mathcal{B}_u \sim \mathcal{N}(b_u, \sigma_u)$
  - admittedly simple, but it allows for analytical tractability.
- Immediate reward v_r for the operator

Incident Detection

Continuous Authentication

- False positive rate η_u
- Single-threshold rule
  - Test result is positive if $\mathcal{B}_u > c$
  - Detection threshold $c = \Phi_u^{-1}(1 - \eta_u)$
- System states:
  - **Blocking state (BL)**: user can not interact with resources,
  - **Unblocking state (UB)**: user is authorized to interact.



Intrusion Detection System (IDS)

- Per time-slot operation cost m

Attack Model

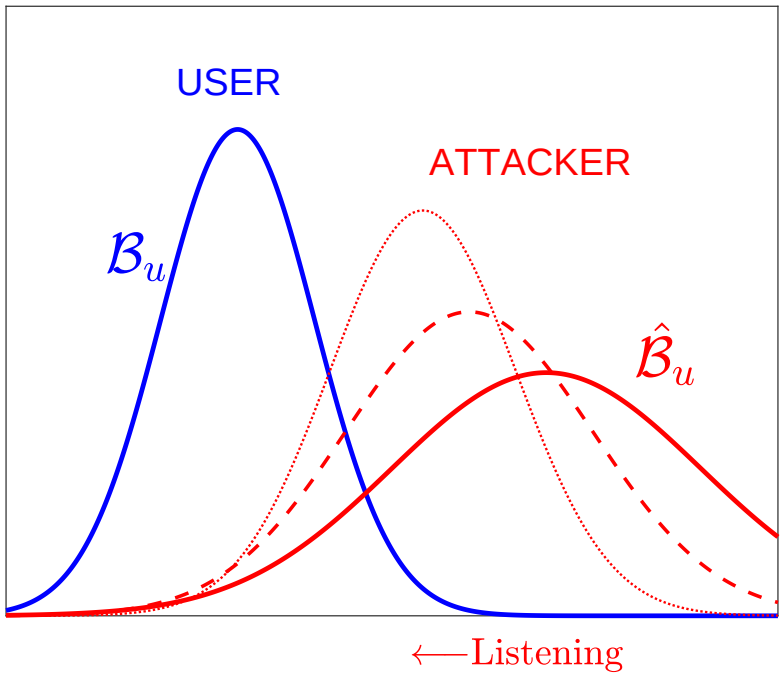
- Cost C_a of system compromise
- In every time-slot, the attacker chooses between
  - **Listening (**$I(t) = 1$**,** $a(t) = 0$**)**: learn to imitate legitimate user
  - **Attacking (**$I(t) = 0$**,** $a(t) = 1$**)**: imitates legitimate user behavior and executes a rogue command on the resource
  - **Waiting (**$I(t) = 0$**,** $a(t) = 0$**)**

Attack Model - Listening

- Total amount of observation $L(t) = \sum_{\tau=0}^{t-1} \mathbb{1}_{\{I(\tau)=1\}} \Lambda_u(\tau)$ of the attacker
- IDS detection probability $\delta_I(m)$

Attack Model - Attacking

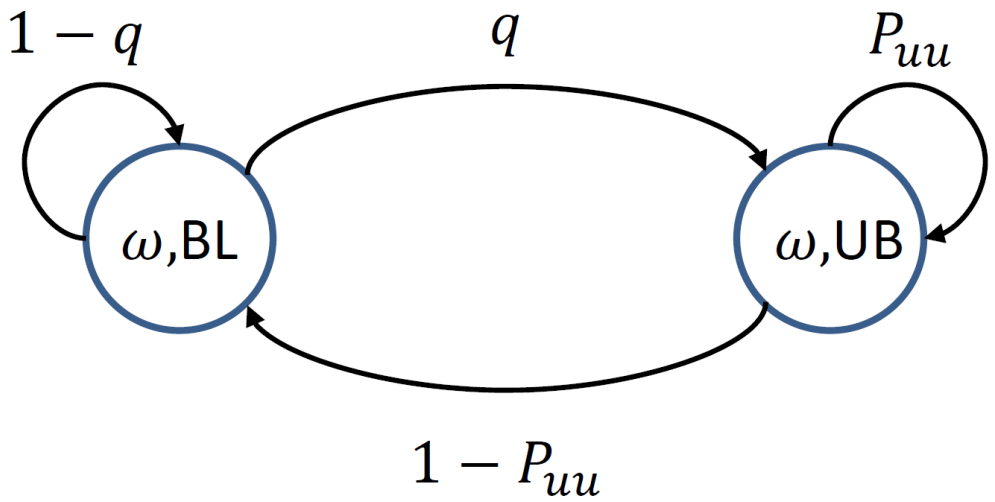
- Attacker-generated input
  $\hat{\mathcal{B}}_u(L(t)) \sim \mathcal{N}\left(\hat{b}_u\left(L(t)\right), \hat{\sigma}_u\left(L(t)\right)\right)$
  - $\hat{b}_u(L(t)) = b_u(1 + \mathrm{e}^{-\gamma L(t)})$
  - $\hat{\sigma}_u(L(t)) = \sigma_u(1 + \mathrm{e}^{-\gamma L(t)})$
- Receiver Operating Characteristic (ROC) curve
  - $\mathrm{ROC}(\eta_u, L(t)) = \Phi\left(\frac{b_u}{\sigma_u} - \frac{b_u - \sigma_u \Phi^{-1}(\eta_u)}{\sigma_u(1+\mathrm{e}^{-\gamma L(t)})}\right)$
  - False Negative $= 1 -$ ROC
- IDS detection probability $\delta_a(m)$



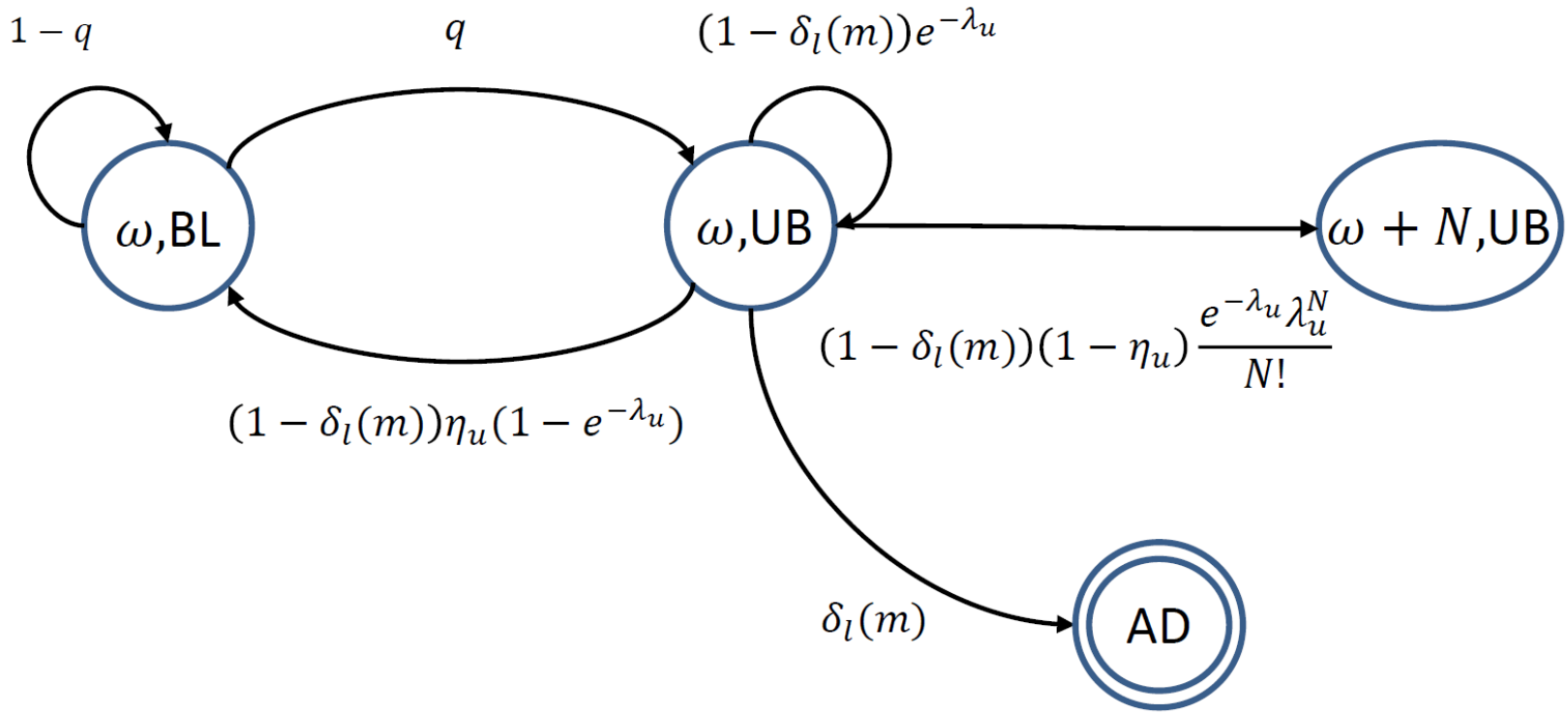
Continuous Authentication Game

- Defender (operator)
  - Chooses a defense strategy (m, η_u)
  - In order to maximize its average utility.
- Attacker (follower)
  - Decides whether or not to compromise the system,
  - If so, in every time-slot it decides whether to wait, listen, or attack
  - In order to maximize its expected reward.
- Game ends when the attacker is detected (AD) by the IDS.

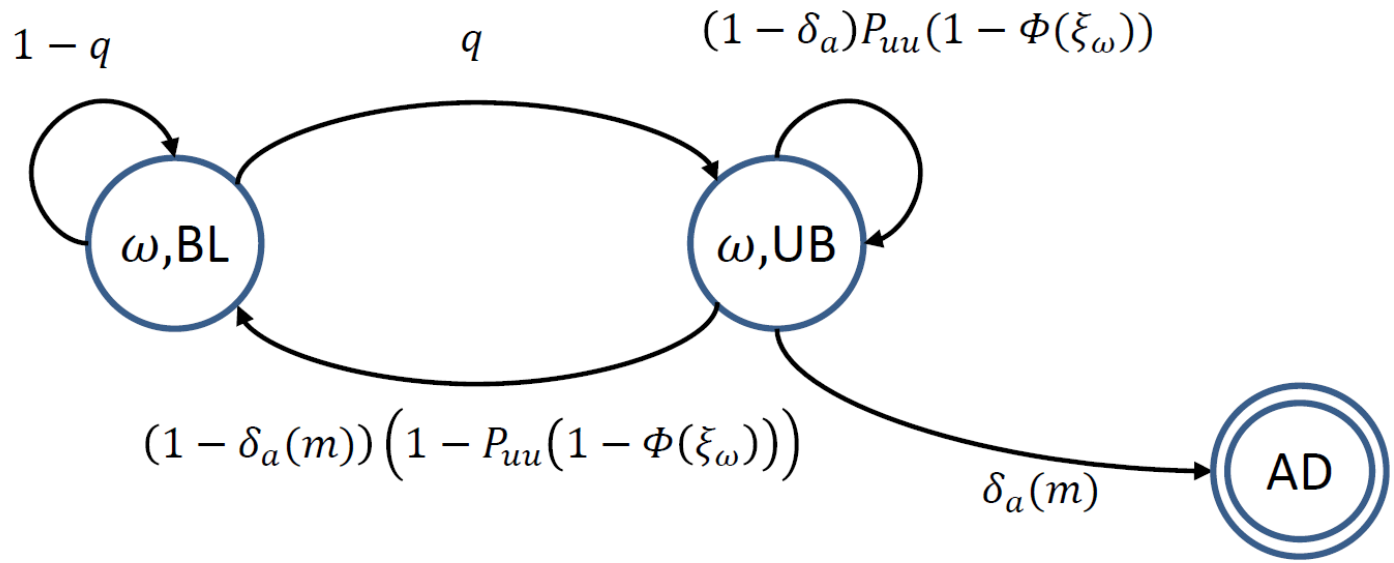
States and Transitions when Waiting



States and Transitions when Listening



States and Transitions when Attacking



Optimal Attacker Strategy

Theorem

The optimal attack strategy is

$$\begin{cases} \textit{Waiting } (I(t)=0,\ a(t)=0) & \textit{if } S(t)=BL,\ L(t) \textit{ arbitrary} \\ \textit{Listening } (I(t)=1,\ a(t)=0) & \textit{if } S(t)=UB,\ L(t)<\widetilde{\omega} \\ \textit{Attacking } (I(t)=0,\ a(t)=1) & \textit{if } S(t)=UB,\ L(t)\geq\widetilde{\omega} \end{cases}$$

where $\widetilde{\omega}$ is independent of time and can be calculated (before the game-play) for a given set of parameters.

Proof Sketch

- Express the optimal attacker reward as a backward dynamic programming recursion; i.e., Bellman optimality equations.
- The ratio between the listening and attacking rewards shows that listening is optimal for $L(t) < \widetilde{\omega}$.
- Since attacker cannot get any reward by only listening, for any amount of observation $\widehat{\omega} \geq \widetilde{\omega}$, there must be some $\overline{\omega} \geq \widehat{\omega}$, in which attacking is optimal.
- Bellman update of the attacker reward is a contraction mapping, thus the value iteration algorithm converges to a unique optimal, which shows that attacking is optimal for $L(t) \geq \widetilde{\omega}$.

The Optimal Defense Strategy

- Defender anticipates the optimal attacker strategy.
- However, she does not know the amount of observation $L(t) = \omega$ attacker has at time-slot t.
- At any time-slot t,
  - System may switch between $S(t) = \text{UB}$ and $S(t) = \text{BL}$.
  - Attacker may be detected (i.e., $S(t) = \text{AD}$).
- $L(t)$ may increase randomly if $L(t) = \omega < \widetilde{\omega}$.
- Attack may be successful if $L(t) = \omega \geq \widetilde{\omega}$.
- Express the average defender utility as stochastic averaging of the cases/transitions above.

Numerical Results - Attacker Strategies

Table: Default parameters.

λ_u	10
$\mathcal{B}_u$	$\mathcal{N}(100, 3)$
η_u	0.01
v_r	0.1
c_r	1
$\delta_l(m)$	0.1
$\delta_a(m)$	0.2
q	0.7
ρ	0.98
γ	0.1

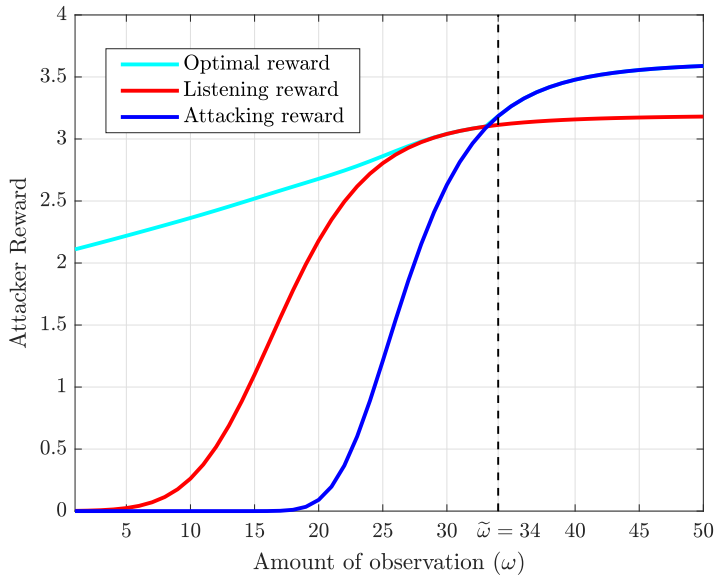
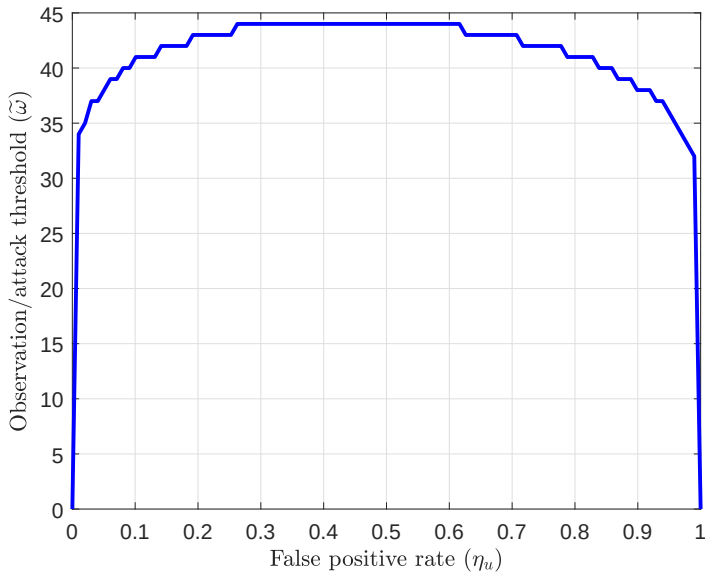
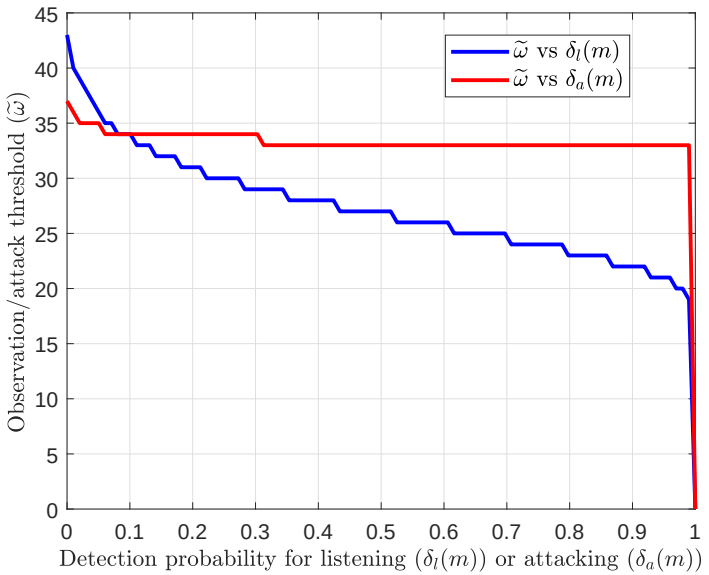


Figure: Attacker reward vs. amount of observation (ω) under different strategies.

Numerical Results - Threshold



(a) Threshold ($\widetilde{\omega}$) vs. η_u.

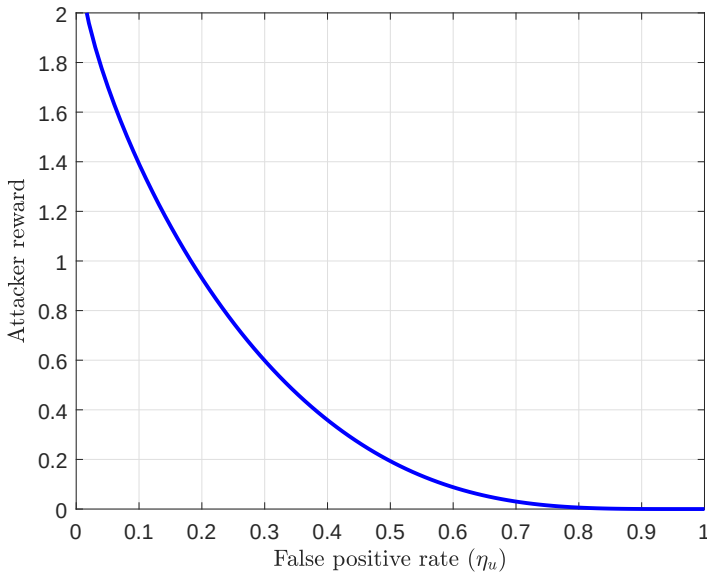


(b) Threshold ($\widetilde{\omega}$) vs. $\delta_l(m)$ and $\delta_a(m)$.

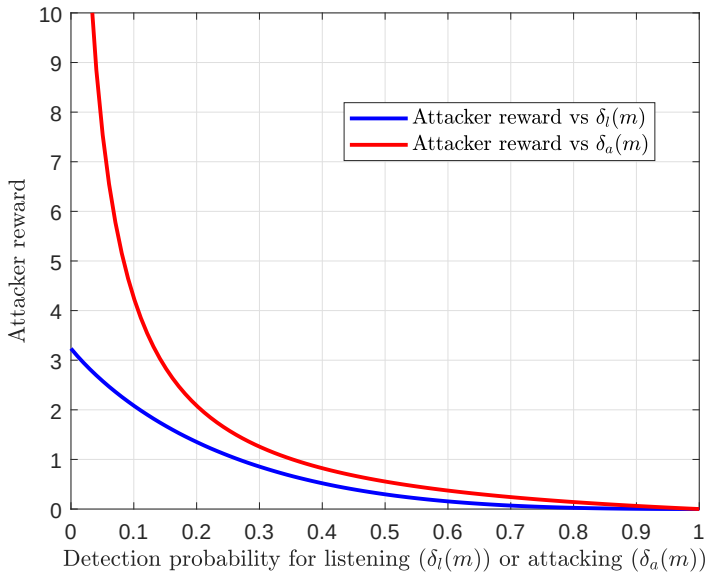
Figure: Observation/attack threshold ($\widetilde{\omega}$) vs. detection parameters

- Low FP rate $\Rightarrow$ higher success probability for attacking
- High FP rate $\Rightarrow$ the state BL is more dominant

Numerical Results - Attacker Reward



(a) Attacker reward vs. false positive rate (η_u).

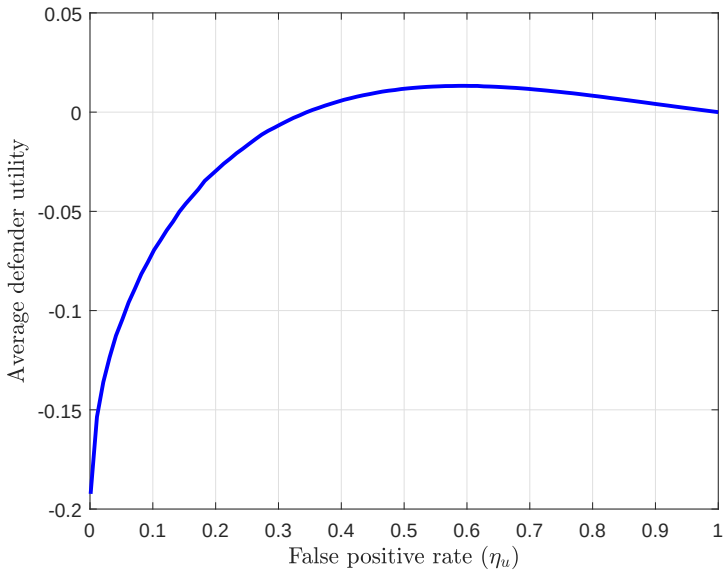


(b) Attacker reward vs. $\delta_l(m)$ and $\delta_a(m)$.

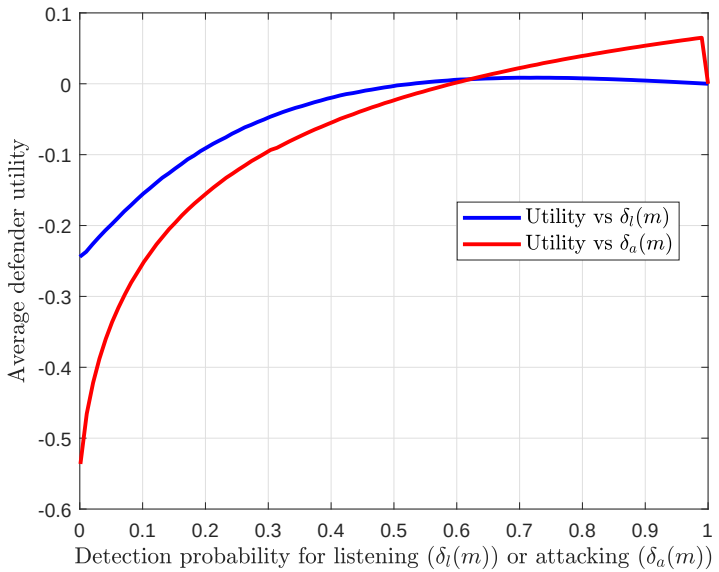
Figure: Attacker reward vs. detection parameters

- Low FP rate $\Rightarrow$ higher success probability for attacking
- Low $\delta_a(m) \Rightarrow$ IDS is essential

Numerical Results - Defender Utility



(a) Average defender utility vs. false positive rate (η_u).

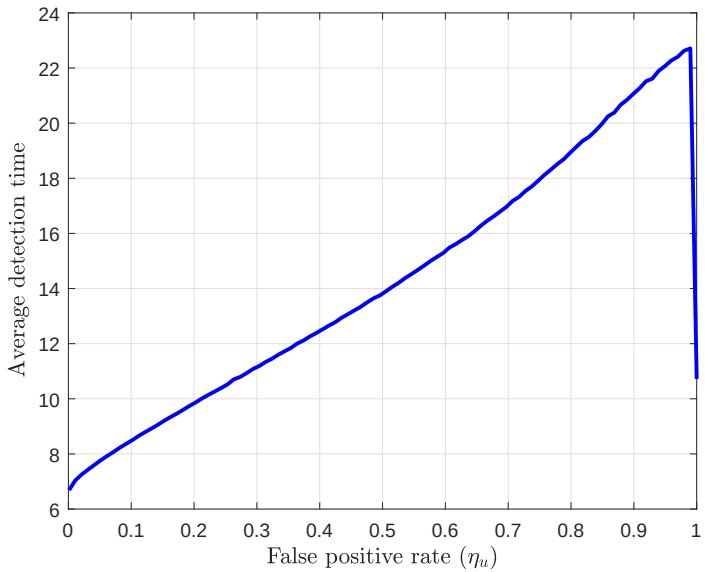


(b) Average defender utility vs. $\delta_l(m)$ and $\delta_a(m)$.

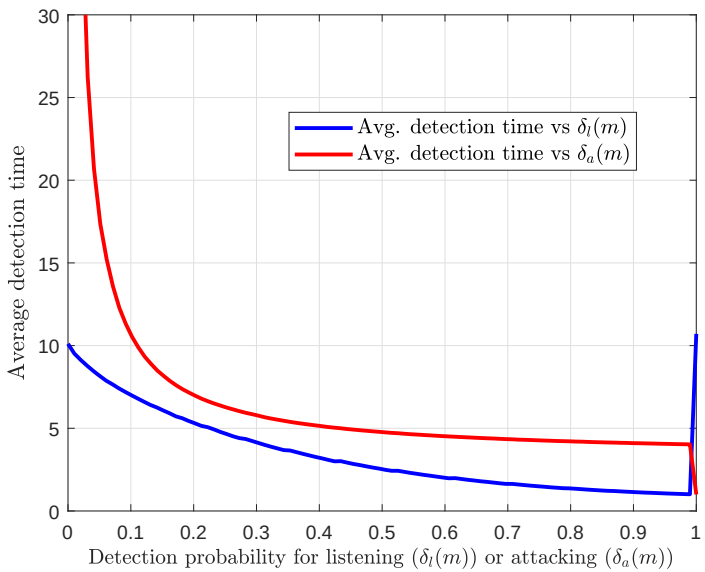
Figure: Average defender utility vs. detection parameters

- As FP increases, the attacker listens more but the success rate decreases

Numerical Results - Detection Time



(a) Average detection time vs. false positive rate (η_u).



(b) Average detection time vs. $\delta_l(m)$ and $\delta_a(m)$.

Figure: Average detection time vs. detection parameters

- Low FP rate $\Rightarrow$ the attacker is urged to attack early
- High FP rate $\Rightarrow$ the state BL is more dominant

Conclusion

- Evasion attack under strict black box model
- Security risk management using continuous authentication and IDS
  - Dynamic discrete stochastic leader-follower game
  - Imperfect information
- Optimality of threshold strategy for attacker
- Optimal defender strategy
  - Productivity vs. protection
  - Higher IDS cost without attacker
  - Lower IDS cost with attacker

KTH ROYAL INSTITUTE
OF TECHNOLOGY

Adversarial Attacks on Continuous Authentication Security: A Dynamic Game Approach

Serkan Sarıtaş[1] Ezzeldin Shereen[1]
Henrik Sandberg[2] György Dán[1]

[1]Division of Network and Systems Engineering, KTH Royal Institute of Technology, Sweden
[2]Division of Decision and Control Systems, KTH Royal Institute of Technology, Sweden

GameSec 2019 Stockholm, Sweden November 1, 2019