Fundamental Scaling Laws of Covert DDoS Attacks

[1]Amir Reza Ramtin, [2]Philippe Nain, [3]Daniel S. Menasche,
[1]Don Towsley, [3]Edmundo de Souza e Silva

[1]UMass Amherst, USA, [2]INRIA, France, [3]UFRJ, Brazil

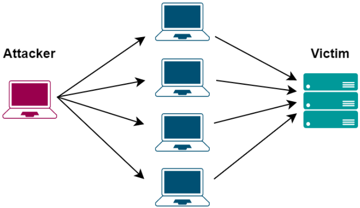
November 2021

Outline

- Problem Overview
  - Motivation
  - System description
- Analysis
  - Theoretical results
  - Evaluation

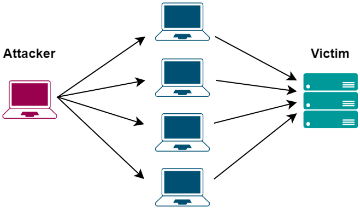
Distributed Denial of Service Attacks

- A Distributed Denial of Service (DDoS) attack is an attempt to crash system by overwhelming it with data.



Distributed Denial of Service Attacks

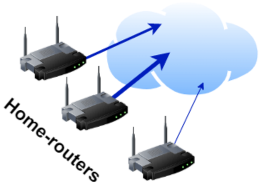
- A Distributed Denial of Service (DDoS) attack is an attempt to crash system by overwhelming it with data.



- Next generation of botnets will attempt to be undetectable.

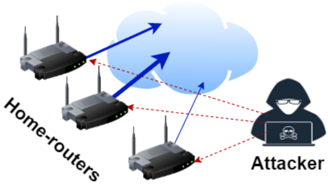
System Description (Attacker)

- Collection of homes connected to Internet through ISP.



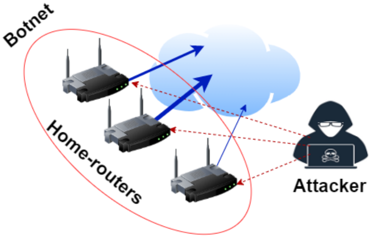
System Description (Attacker)

- Collection of homes connected to Internet through ISP.
- Attacker compromises homes to form botnet.



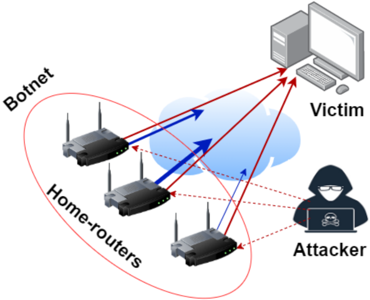
System Description (Attacker)

- Collection of homes connected to Internet through ISP.
- Attacker compromises homes to form **botnet**.



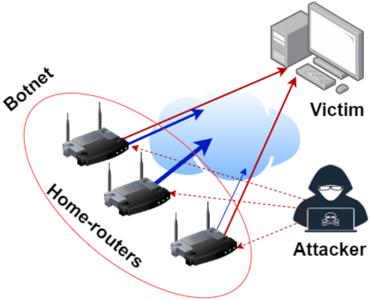
System Description (Attacker)

- Attacker may use **all homes** or fraction of them to issue attack.



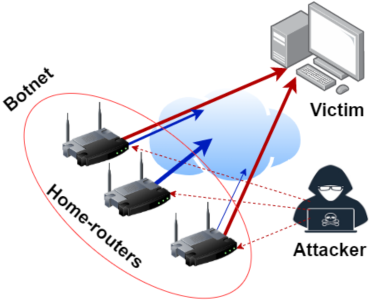
System Description (Attacker)

- Attacker may use all homes or **fraction of them** to issue attack.

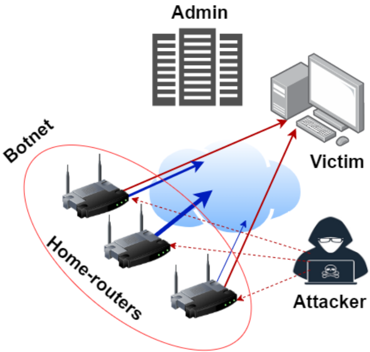


System Description (Attacker)

- Attacker can determine rate at which each home should inject attack traffic into network.

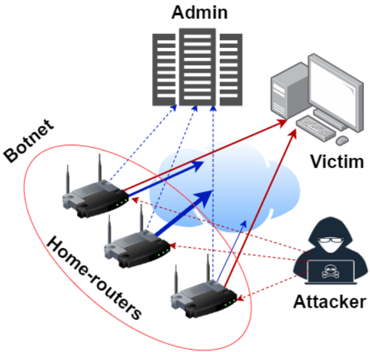


System Description (Defender)



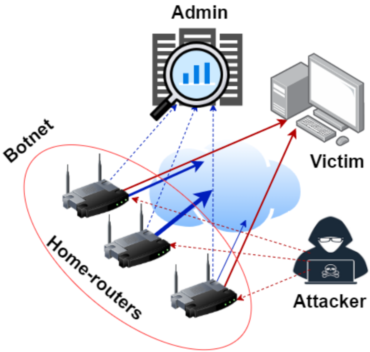
System Description (Defender)

- Sample collected every minute and transmitted to admin.



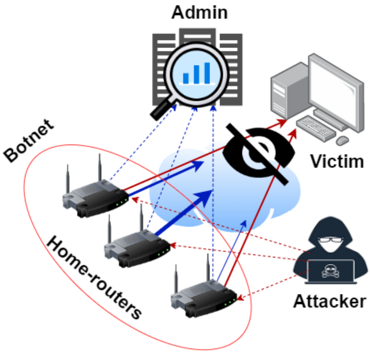
System Description (Defender)

- Sample collected every minute and transmitted to admin.
- Admin runs detector on samples.



System Description (Defender)

- Sample collected every minute and transmitted to admin.
- Admin runs detector on samples.
- An attack is **covert** if admin cannot detect attack.



Question

- **Can attacker launch covert attack?**

Question

- Can attacker launch covert attack? **if so, how large an attack can he launch?**

Model

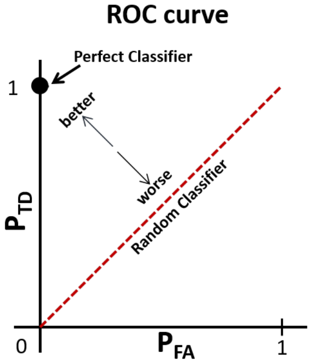
- n: number of homes.
- X_r: regular traffic from home r,
  - $\{X_r\}$: independent sequence of r.v.'s
- Y_r: attack traffic from home r
  - $\{Y_r\}$: iid sequence of r.v.'s
- $\chi_r \in \{0, 1\} \to \chi_r = 1$ if attacker uses home r
  - $q(n) \equiv \mathbb{P}(\chi_r = 1)$
- Z_r: amount of observed traffic at home r,

$$Z_r = \begin{cases} X_r & \text{if no attack occurs,} \\ X_r + \chi_r Y_r & \text{otherwise.} \end{cases}$$

Attack Detection

- If density functions are known, admin can construct an optimal statistical hypothesis test.
  - H_0 (no attack taking place): $Z_r = X_r$
  - H_1 (attack taking place): $Z_r = X_r + \chi_r Y_r$
- Admin can tolerate false alarms: $p_{FA} < \alpha$
- Admin may fail to detect attacks: p_{MD}

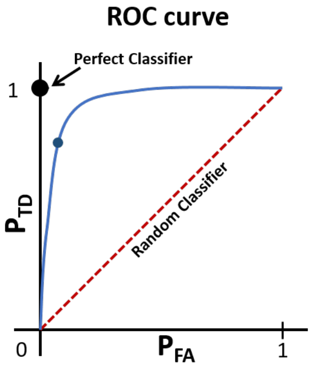
Covertness



ROC curve
Perfect Classifier
1
better
worse
Random Classifier
P_{TD}
0
P_{FA}
1

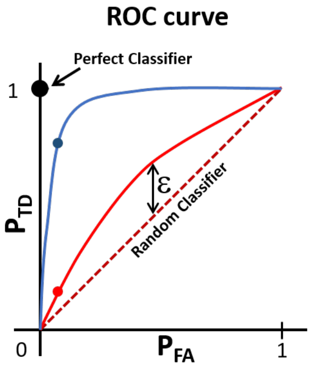
Covertness

- Admin fixes P_{FA} and uses an optimal detector, which maximizes P_{TD}.



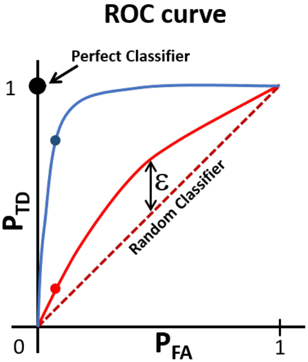
Covertness

- Attacker lower bounds $P_{FA} + P_{MD} \geq 1 - \varepsilon$ to drive ROC curve to diagonal ($P_{FA} + P_{MD} = 1$), making detector useless!



Covertness

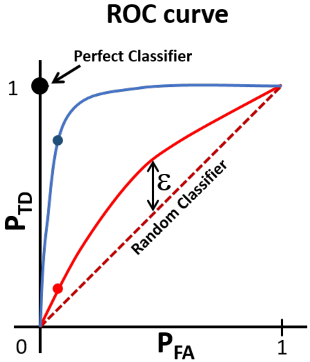
- $P_E = P_{FA} + P_{MD}$



Covertness

- $P_E = P_{FA} + P_{MD}$
- Attack is covert provided, for any $\varepsilon > 0$, attacker has strategy for each n such that

$$P_E \geq 1 - \varepsilon$$



Covertness

- $P_E^\star$ - error of optimal detector
- $f_i^{(n)}$ - joint pdf of $\underline{Z}_1, \ldots, \underline{Z}_n$ under H_i, $i = 0, 1$
- T_V - relates to L_1 norm, $T_V(P, Q) = \frac{1}{2}\|P - Q\|_1$

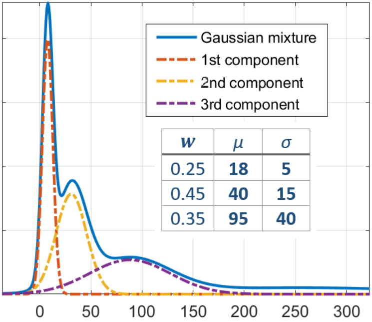
$$P_E^\star = 1 - T_V\left(f_0^{(n)}, f_1^{(n)}\right)$$

Achievability (traffic models)

- X_r - Gaussian Mixture
  - mean $\mu_{0,r}$, variance $\sigma_{0,r}^2$
- Y_r - Gaussian Mixture
  - mean $\mu_1(n)$, variance $\sigma_1^2(n)$

Achievability (traffic models)

- X_r - Gaussian Mixture
  - mean $\mu_{0,r}$, variance $\sigma^2_{0,r}$
- Y_r - Gaussian Mixture
  - mean $\mu_1(n)$, variance $\sigma^2_1(n)$
- Example: X_k
  - $\mu_{0,k} = \sum_{i=1}^{3} w_i \mu_i = 33.25$
  - $\sigma^2_{0,k} = \sum_{i=1}^{3} w_i \sigma^2_i = 667.5$



w	μ	σ
0.25	**18**	**5**
0.45	**40**	**15**
0.35	**95**	**40**

Achievability

Theorem (Achievability)

Under some mild conditions attack traffic is covert if

$$q(n)\mu_1(n) = \mathcal{O}(1/\sqrt{n}), \quad q(n)\sigma_1^2(n) = \mathcal{O}(1/\sqrt{n}).$$

Achievability (Proof Sketch)

- Total variation distance is not easy to work!
- Upper bound on total variation distance

$$T_V\left(f_0^{(n)}, f_1^{(n)}\right) \leq \frac{1}{2}\sqrt{(1+q(n)^2 C(n))^n - 1}$$

where $C(n)$ is

$$C(n) = -1 + \int_{\mathbb{R}} \frac{f_1(x,n)^2}{f_0(x)} dx.$$

- If $q(n)\sqrt{C(n)} = \mathcal{O}(1/\sqrt{n})$ then $T_V\left(f_0^{(n)}, f_1^{(n)}\right) \leq \varepsilon$.

Converse

- Traffic Models
  - X_r - arbitrary distributions, mutually independent
  - Y_r - arbitrary distribution, iid

Converse

Theorem (Converse)

Under some mild conditions attacker is not covert if

$$\begin{aligned} q(n)\mu_1(n) =& \omega(1/\sqrt{n}) \\ \mathrm{var}(\chi_r Y_r) =& \mathcal{O}(1). \end{aligned}$$

Converse (Proof Sketch)

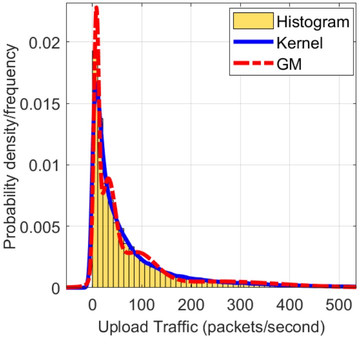
- Apply detector of form $\frac{1}{n}\sum_{r=1}^{n} z_r \lesseqgtr \tau$
- We should have been able to use CLT.
  - Problem: z_r depends on n!
  - Apply Berry-Esseen theorem.

Two important notes

- Achievability theorem holds **when admin does not know attack traffic distribution statistics** as it cannot perform better with less knowledge.
- Converse theorem holds **when admin knows attack traffic distribution** as it cannot perform less effectively with more knowledge.

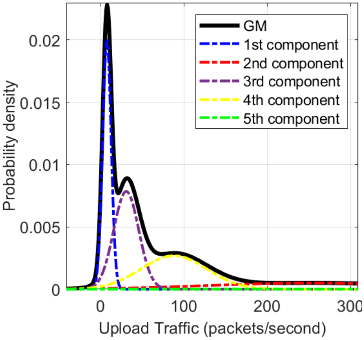
Evaluation (data)

- Regular traffic collected at minute intervals from more than 5000 home-routers between March 1st 2020 and April 30th 2020.
- Traffic feature: packet counts of upstream traffic.



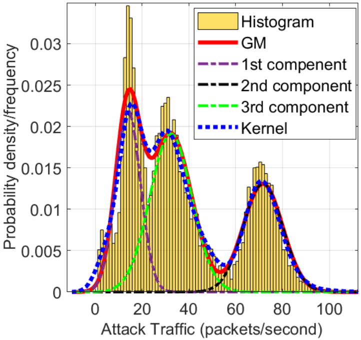
Evaluation (data)

- Regular traffic collected at minute intervals from more than 5000 home-routers between March 1st 2020 and April 30th 2020.
- Traffic feature: packet counts of upstream traffic.
- Distribution model: mixture of five Gaussians



Evaluation (data)

- Estimate distribution of traffic generated by typical DDoS attack in lab.
- Traffic feature: packet counts of upstream traffic.
- Distribution model: mixture of three Gaussians

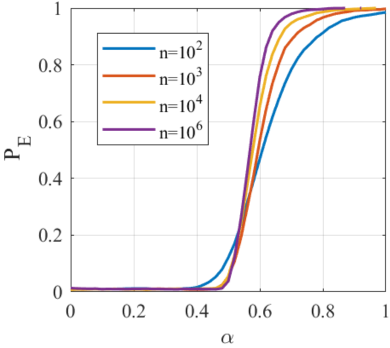


Evaluation (setup)

- Two different tests
  - Likelihood ratio test: $\Lambda < \tau \rightarrow$ attack, where Λ is likelihood ratio
  - Volume test: $\frac{1}{n}\sum_{r=1}^{n} z_r > \tau \rightarrow$ attack
- Find threshold τ given $p_{FA} = 0.01$
  - Monte Carlo methods
- $P_E = P_{FA} + P_{MD}$
- Two scenarios
  - Attacker uses all homes to launch attacks
  - Attacker uses fraction of homes to launch attacks

Scenario 1: attack from all homes

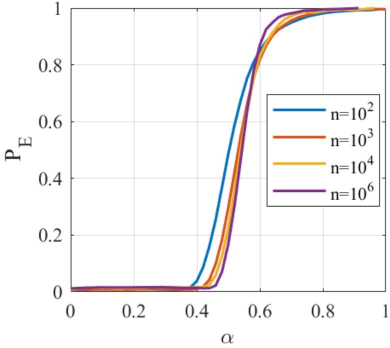
- $\mu_1(n) \propto n^{-\alpha}$
- $\sigma_1(n)^2 \propto n^{-\alpha}$
- $q(n) = 1$



LRT detector

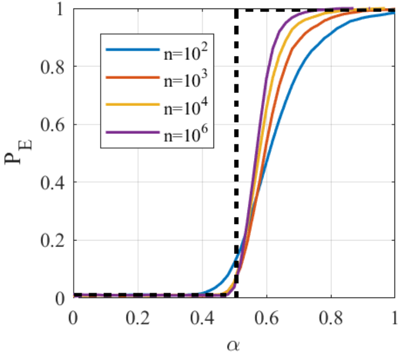
Scenario 1: attack from all homes

- $\mu_1(n) \propto n^{-\alpha}$
- $\sigma_1(n)^2 \propto n^{-\alpha}$
- $q(n) = 1$

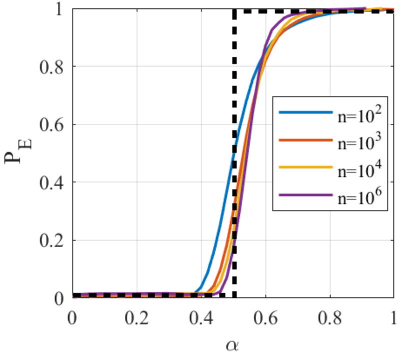


VT detector

Phase Transition (scenario 1)



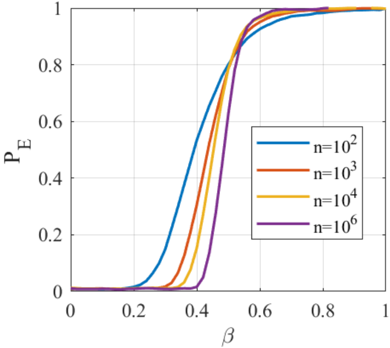
LRT detector



VT detector

Scenario 2: attack from subset of homes

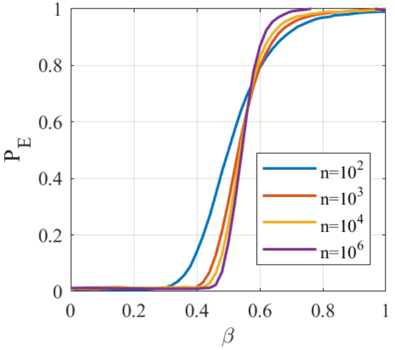
- $\mu_1(n) = c_1$
- $\sigma_1(n)^2 = c_2$
- $q(n) = n^{-\beta}$



LRT detector

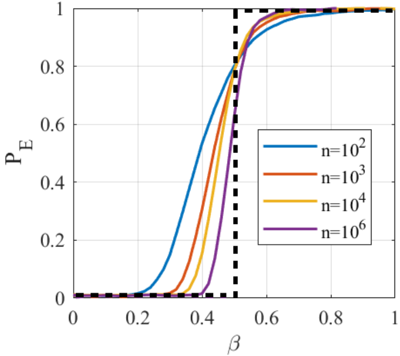
Scenario 2: attack from subset of homes

- $\mu_1(n) = c_1$
- $\sigma_1(n)^2 = c_2$
- $q(n) = n^{-\beta}$

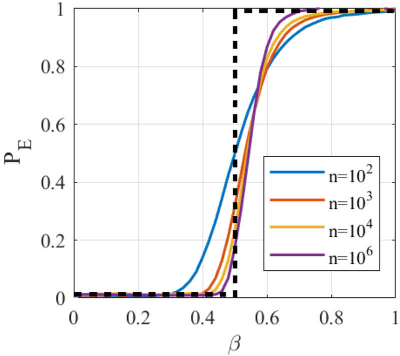


VT detector

Phase Transition (scenario 2)



LRT detector



VT detector

Summary

- We showed that attacker can launch covert attack generating $O(\sqrt{n})$ total aggregated attack traffic.
- Assumption: traffic follows Gaussian mixture distribution.
- Tightness of scaling law regardless of distribution type.

Thank you for listening!

?