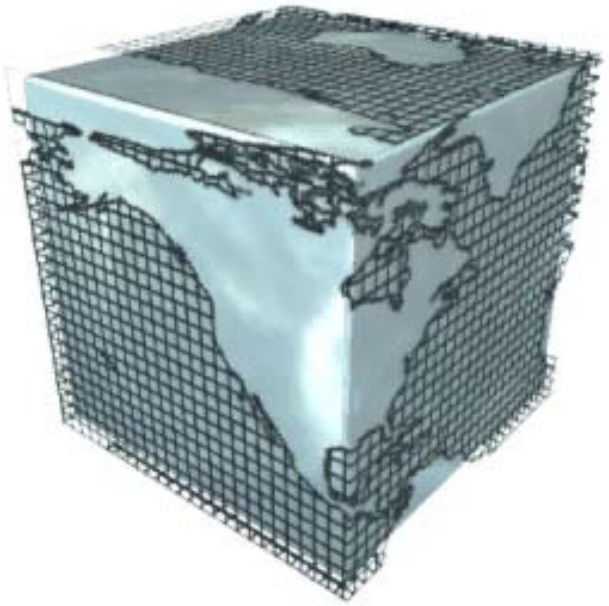
Distinguishing between FE and DDoS using Randomness Check

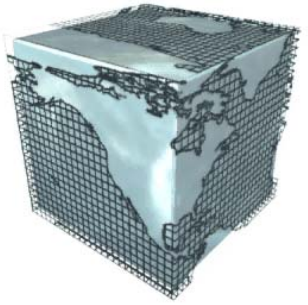
Hyundo Park, Peng Li, Debin Gao,
Heejo Lee and Robert Deng



Presented by Hyundo Park

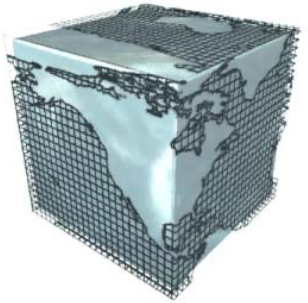
Korea University
Singapore Management University

Index

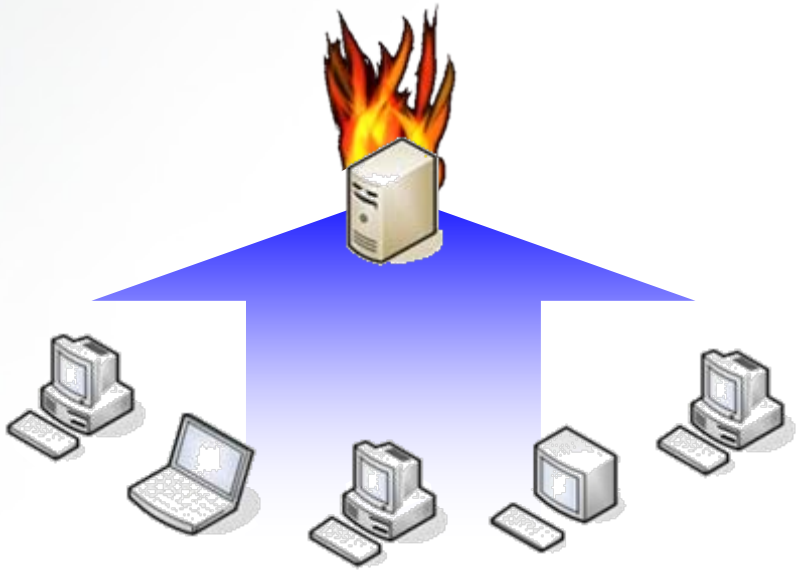


- Introduction
- Characteristics of FE and DDoS
- Motivation
- System design
- Evaluation
- Conclusion

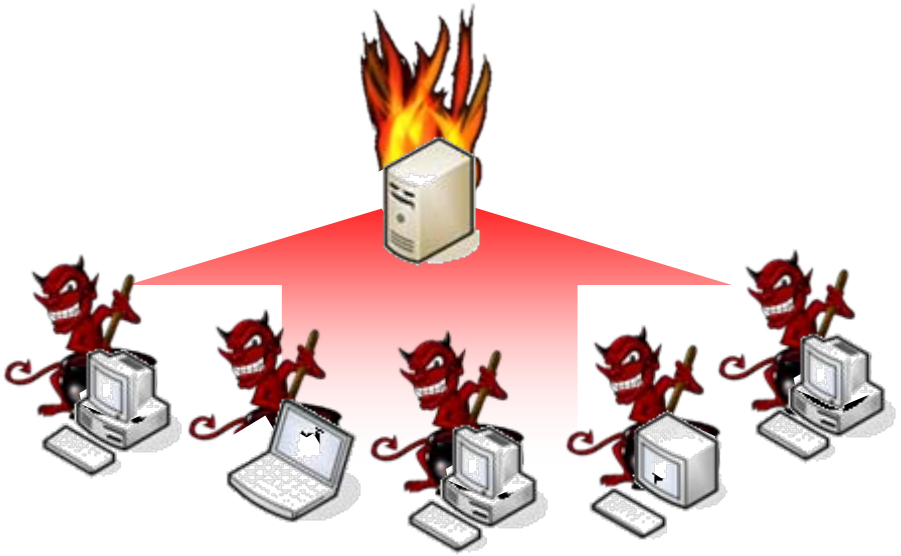
Introduction



- An exhaustion of network or server resources
  - By a Flash Event
    - Caused by legitimate users
  - By Distributed Denial of Service (DDoS) attacks
    - Caused by attackers

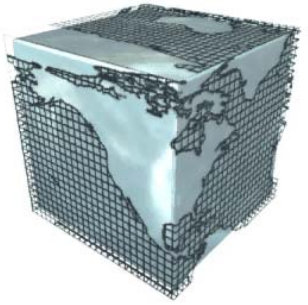


Flash Event



DDoS attack

Characteristics of FE and DDoS

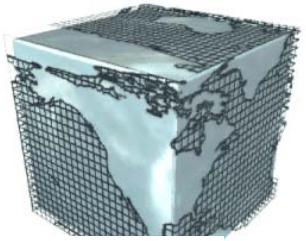


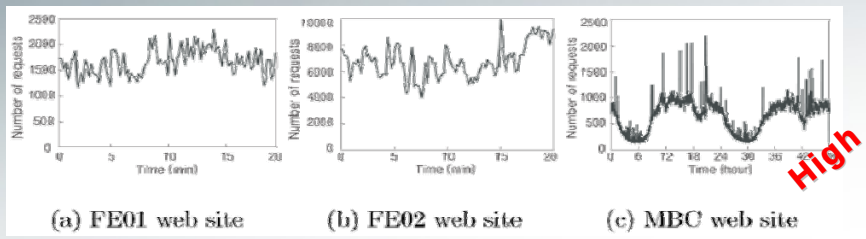
- Characteristics of FE and DDoS [1]

	FE	DDoS
Traffic volume	High	High
Distribution of clusters among clients	The number of clusters are much smaller than the number of clients	The number of clients and clusters are very similar
Cluster contribution to requests	Follows the Pareto-law (skewed / predictable)	Does not follow the Pareto-law (randomly distributed / unpredictable)

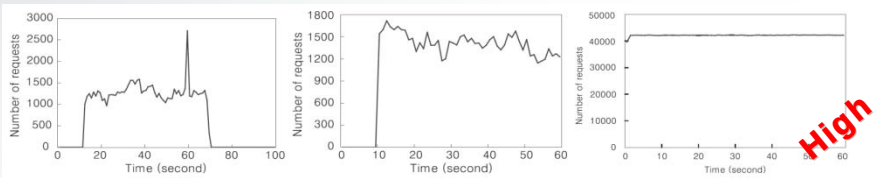
[1] J. Jung, B. Krishnamurthy and M. Rabinovich, “Flash crowds and denial of service attacks: Characterization and implications for CDNs and web sites”, in World Wide Web, May 2002.

Simulation and Analysis of Real Traffic



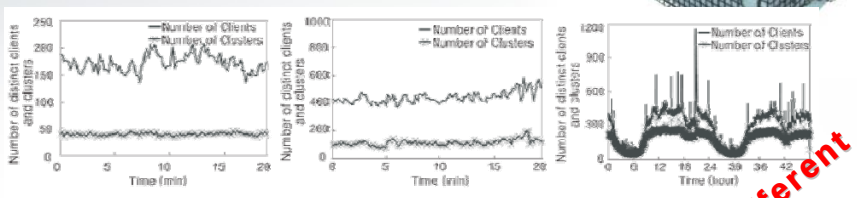


(a) FE01 web site (b) FE02 web site (c) MBC web site

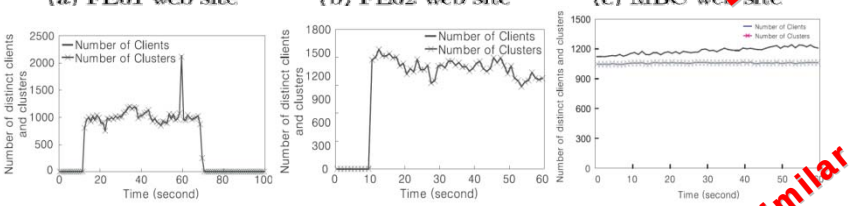


(a) DoS01 (b) DoS02 (c) Non source-spoofed DDoS

Traffic volumes

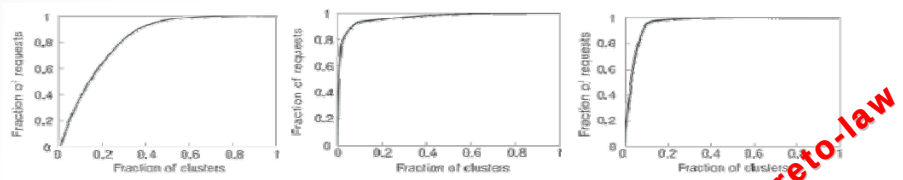


(a) FE01 web site (b) FE02 web site (c) MBC web site

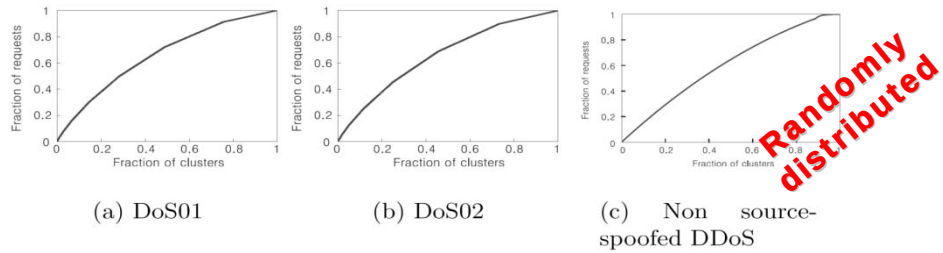


(a) DoS01 (b) DoS02 (c) Non source-spoofed DDoS

The number of clusters among clients



(a) FE01 web site (b) FE02 web site (c) MBC web site



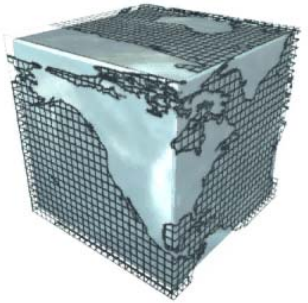
(a) DoS01 (b) DoS02 (c) Non source-spoofed DDoS

Distribution of clusters to requests

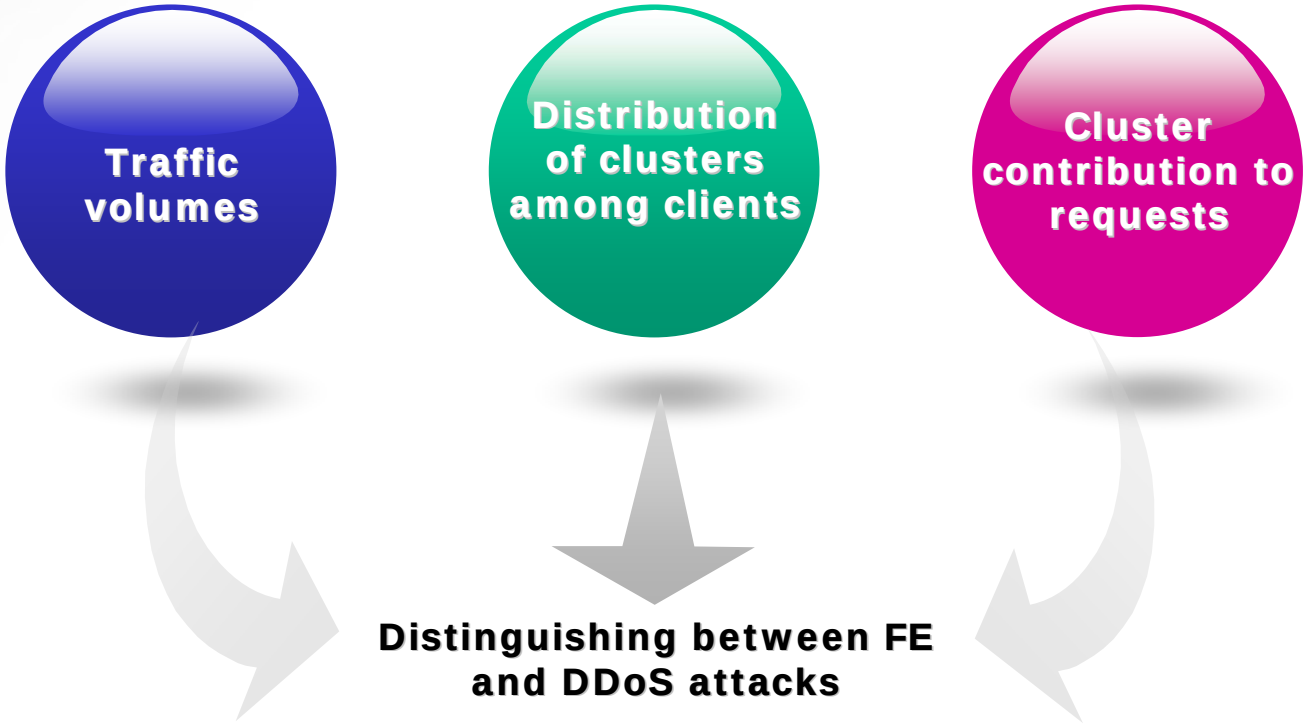
- **FE01:** Published many pictures and java scripts to decorate websites
- **FE02:** A Microsoft Windows update website
- **MBC:** The biggest private broad cast company in Korea

- **DOS01 & DoS02:** Obtained from two trans-pacific T-3 links connecting the United states and a Korean Internet gateway.
- **Non source-spoofed DDoS:** Generated a non-source-spoofed DDoS attack traces with the normal web requests as background traffic using NS-2

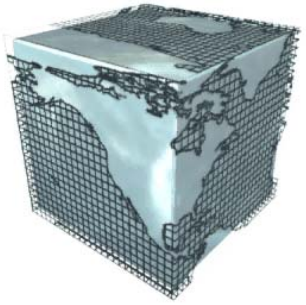
Motivation



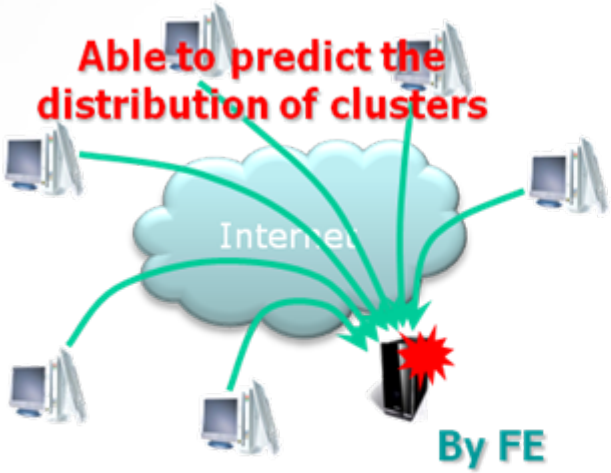
- Distinguishing between FE and DDoS attacks with their characteristics
- Using a randomness checking



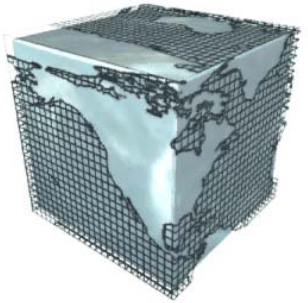
Randomness

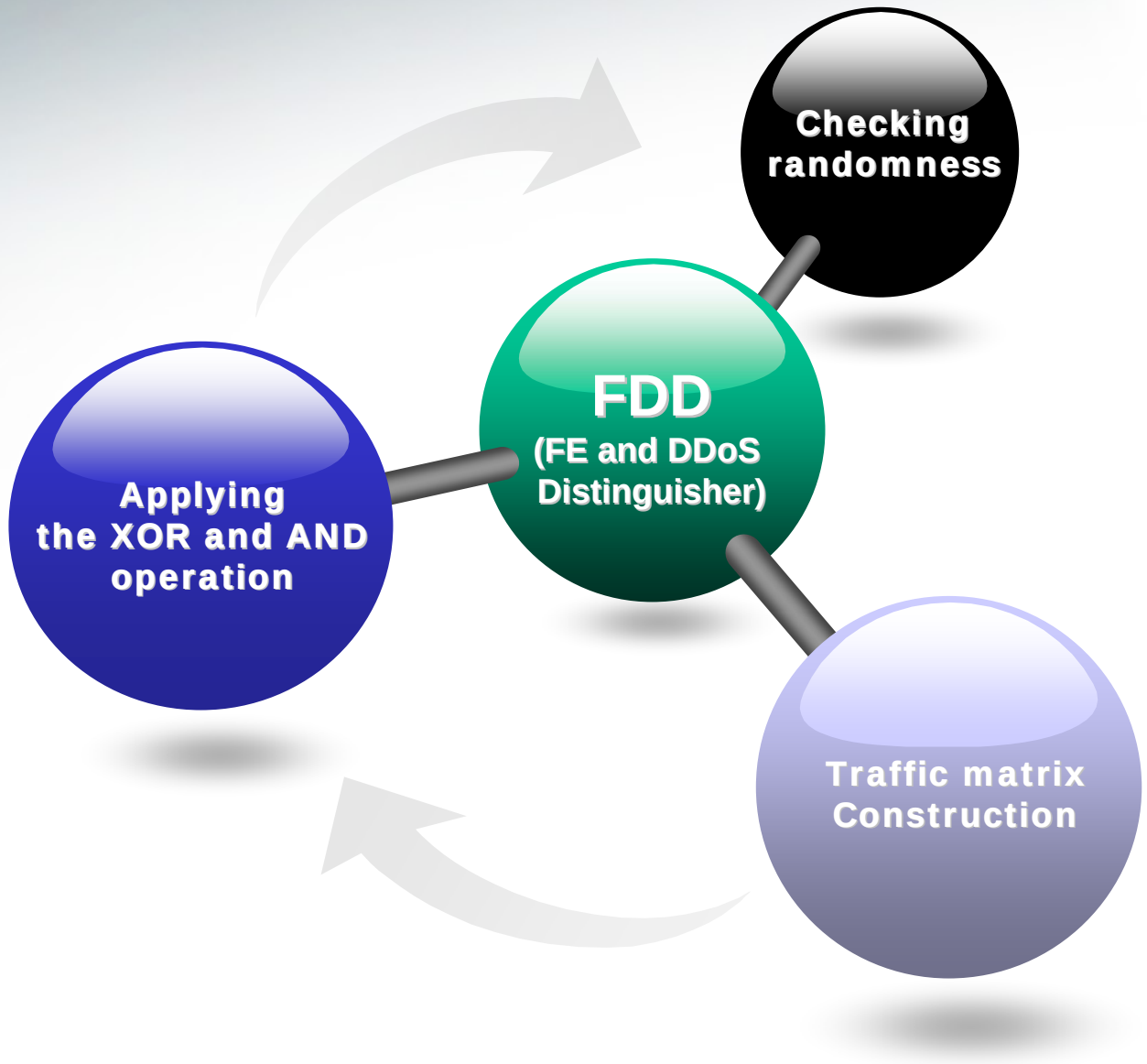


- Abnormal situations on the network by FE and DDoS
  - Able to predict the distribution of clusters among clients or not
  - The unpredictability signified a randomness.

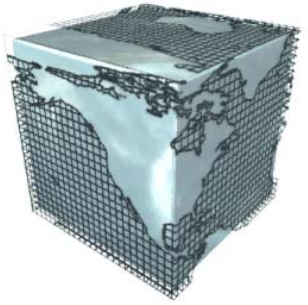


System Design

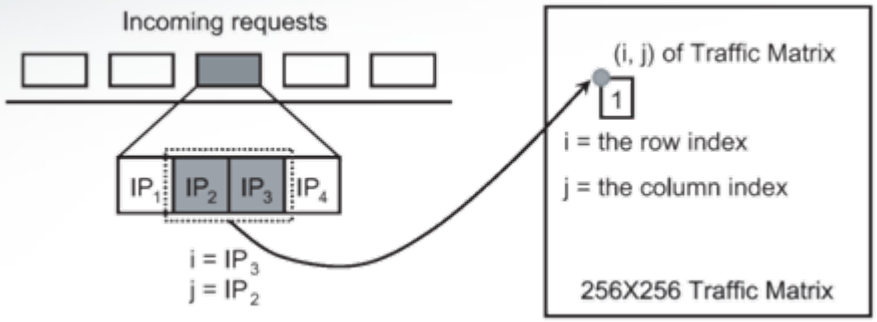




System Design
1. Traffic matrix construction



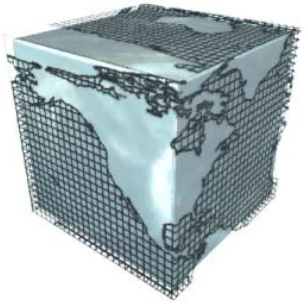
- Place of an incoming request in matrix construction



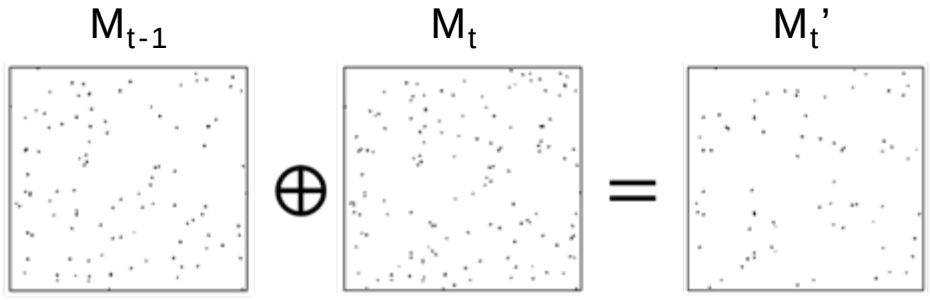
- Process of matrix construction
  - Initialized with zero in all entries
  - For each incoming request, overwritten the content of the entry with the value 1 using one bit

- Clustering clients with IP_2 and IP_3
  - There are many unused or unallocated IP addresses in the Internet. So, we do not use IP_1

Benefits of Randomness Check with Matrix



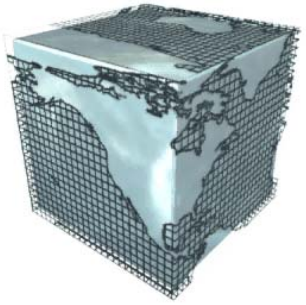
- Easy to apply on the network
  - If we define the method to construct traffic matrix and it's size
- Providing fixed threshold
  - Does not depend on the network traffic environment
- Easy to apply operations, such as XOR, AND and others, between continuative matrix
  - The XOR operation deletes normal traffic
  - The AND operation remains normal traffic



Delete normal traffics at the continuity time units

System Design

2. Applying the XOR and AND operation



- Apply XOR and AND operation between matrices of the current and the previous time units XOR and AND operation

$$R_{\mathrm{XOR}}(M_t) = R(M_t \text{ XOR } M_{t-1})$$
$$R_{\mathrm{AND}}(M_t) = R(M_t \text{ AND } M_{t-1})$$

$R(M_t)$ to denote the rank value of M_t,

  - M_t is the traffic matrix, generated at time t

- Delete or remain traffic on the matrix using the XOR and AND operation

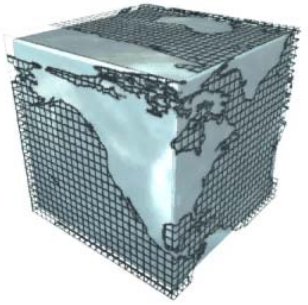
$$\begin{pmatrix}1&0&1\\1&0&0\\0&1&0\end{pmatrix}\oplus\begin{pmatrix}1&0&0\\1&1&0\\0&1&1\end{pmatrix}=\begin{pmatrix}0&0&1\\0&1&0\\0&0&1\end{pmatrix}$$

After XOR

$$\begin{pmatrix}1&0&1\\1&0&0\\0&1&0\end{pmatrix}\otimes\begin{pmatrix}1&0&0\\1&1&0\\0&1&1\end{pmatrix}=\begin{pmatrix}1&0&0\\1&0&0\\0&1&0\end{pmatrix}$$

After AND

System Design
3. Checking randomness



- Randomness check
  - Apply the Gaussian elimination
  - Check the rank value, the number of leading ones
- The probability of a rank value of a *m*x*n* random matrix

$$2^{r(n+m-r)-nm} \prod_{i=0}^{r-1} \frac{(1-2^{i-n})\,(1-2^{i-m})}{(1-2^{i-r})} \quad \text{where } r = 1, 2, \ldots, \min(m, n)$$

- Calculation of the threshold
  - Apply $\log_2$ function

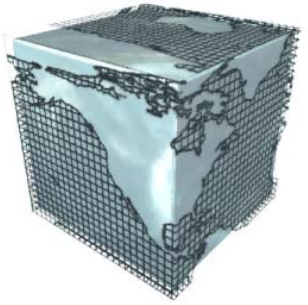
$$2^{r(n+m-r)-nm} \prod_{i=0}^{r-1} \frac{(1-2^{i-n})\,(1-2^{i-m})}{(1-2^{i-r})} = P$$

$$\log_2 \left(2^{r(n+m-r)-nm} \prod_{i=0}^{r-1} \frac{(1-2^{i-n})\,(1-2^{i-m})}{(1-2^{i-r})} \right) = \log_2 P$$

then, we can get the equation, $(m-r)^2 > \log_2 \frac{1}{P}$

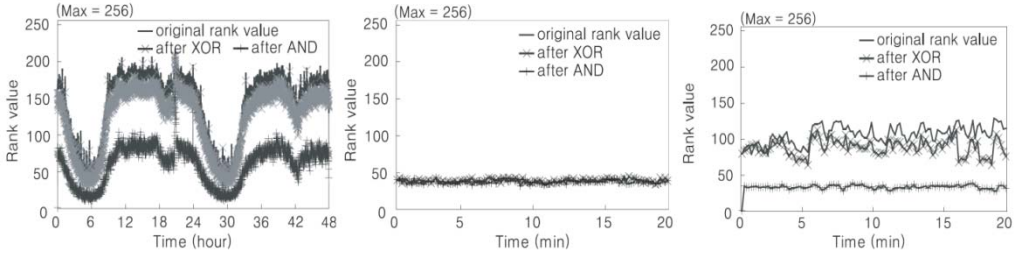
If we assume ***P*** is 0.01%(a value near to zero), we will get 252 as the biggest value to be the threshold, when the value of ***m*** is 256

Evaluation

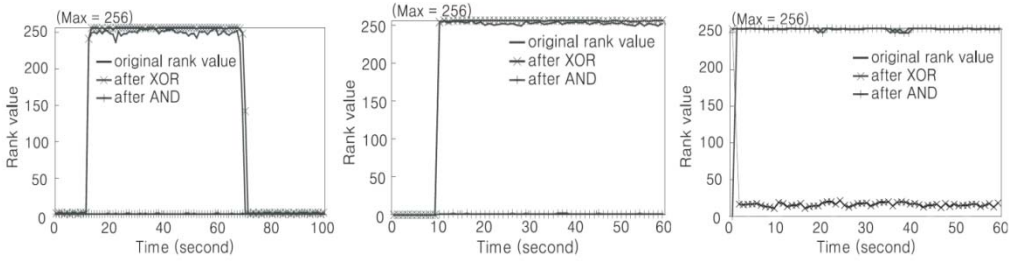


- Randomness check on FE and DDoS traces

	$R(M_t)$	$R_{\text{XOR}}(M_t)$	$R_{\text{AND}}(M_t)$
Normal	small	small	small
FE	Medium$^+$	Medium	Medium$^-$
DDoS with spoofed source IP	Large ($> T$)	Large ($> T$)	Small
DDoS without spoofed source IP	Large ($> T$)	Small	Large ($> T$)

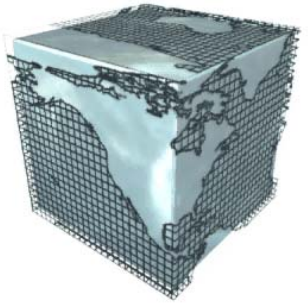


(a) MBC (b) FE01 (c) FE02



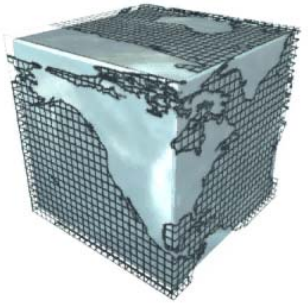
(a) DDoS01 (b) DDoS02 (c) Non source-spoofed DDoS

Conclusion



- FDD, a simple yet effective mechanism, distinguish flash event and DDoS attacks using randomness check
- Our trace-driven evaluation results show that FDD distinguishes between FE and DDoS attacks with high accuracy and low memory usage.

Question and Answer



- Thank you
- **hyundo95@korea.ac.kr**

KOREA UNIVERSITY

http://ccs.korea.ac.kr

SMU SINGAPORE MANAGEMENT UNIVERSITY

School of Information Systems

http://www.sis.smu.edu.sg