Early detection of Crossfire attacks using deep learning

Saurabh Misra, Mengxuan Tan, Mostafa Rezazad, Ngai-Man Cheung

Singapore University of Technology and Design

SINGAPORE UNIVERSITY OF TECHNOLOGY AND DESIGN

Content

The Crossfire Attack
- A brief introduction
- Detection approach

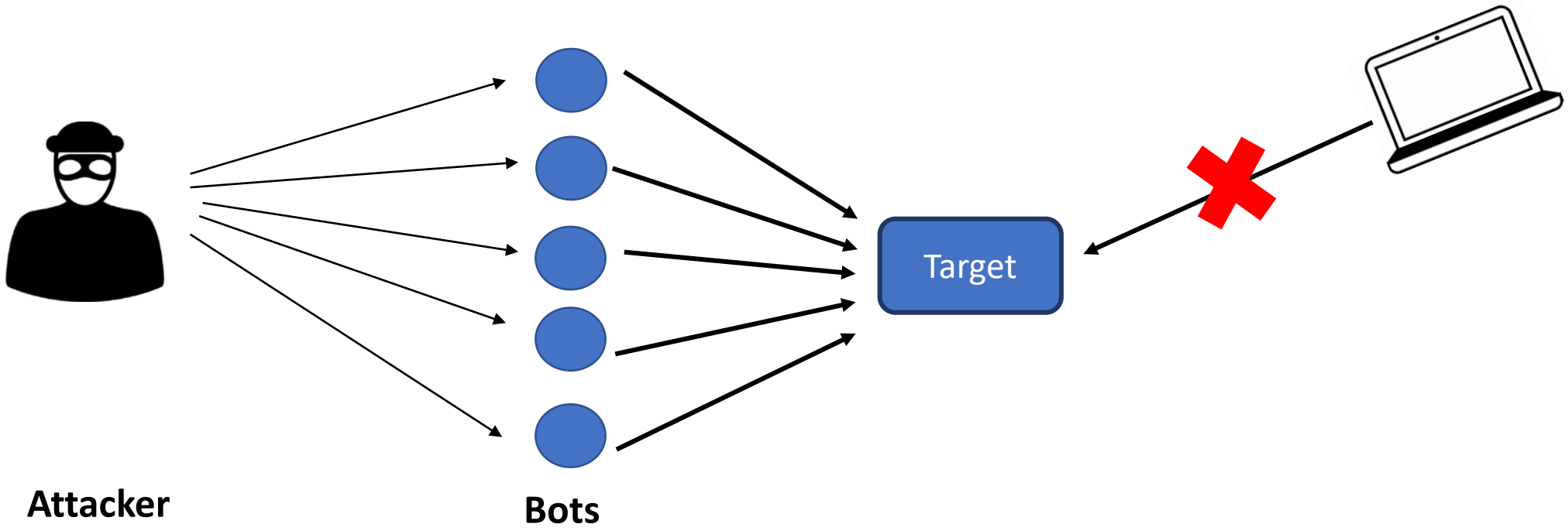
Network Data
- Simulation of data

Methods for detection
- Baseline method
- Deep Autoencoder
- Convolutional Neural Network (CNN)
- Long Short-Term Memory Network (LSTM)

Traditional DDoS Attack

Distributed Denial of Service attack (DDos)

- Attacker targets victims (i.e., web servers) **directly**
- Attacker **overwhelms** victim with network traffic
- Intended users are unable to access the servers



The Crossfire Attack

Introduction

A **sophisticated** DDoS attack

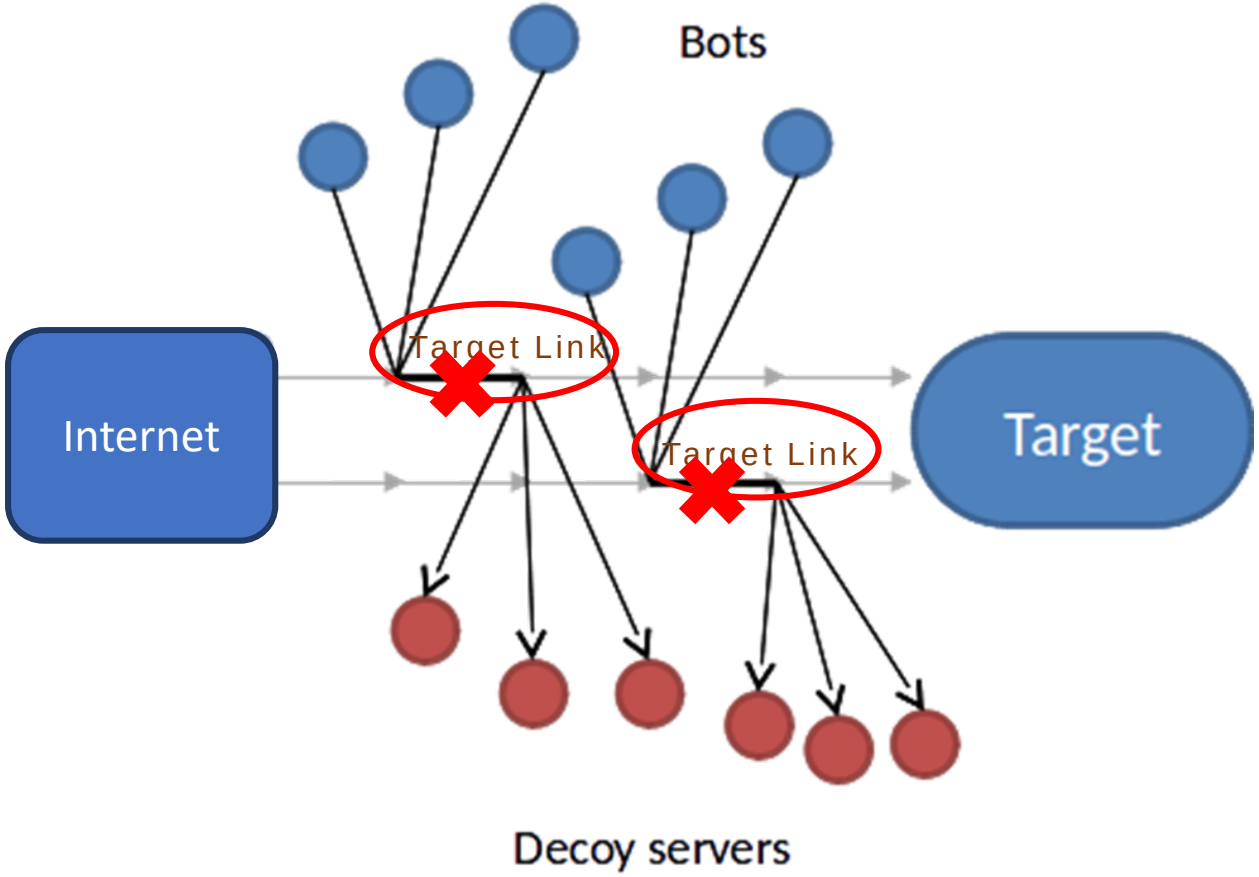
- **Disconnects** an entire area from the Internet
- Targeting a link or set of links

Distributed attack at source and destination level

- Using Botnet to generate traffic
- Traffic destined to many public servers (decoy servers) sharing the **same network link**

It is **hard** to **detect**

- Traffic is normal web traffic
- Traffic flow is very small in terms of size
- Attack can be very dynamic with changing source, destination and target link



Source: Min Suk Kang, Soo Bum Lee, Virgil D. Gligor, "The Crossfire Attack," 2013 IEEE Symposium on Security and Privacy

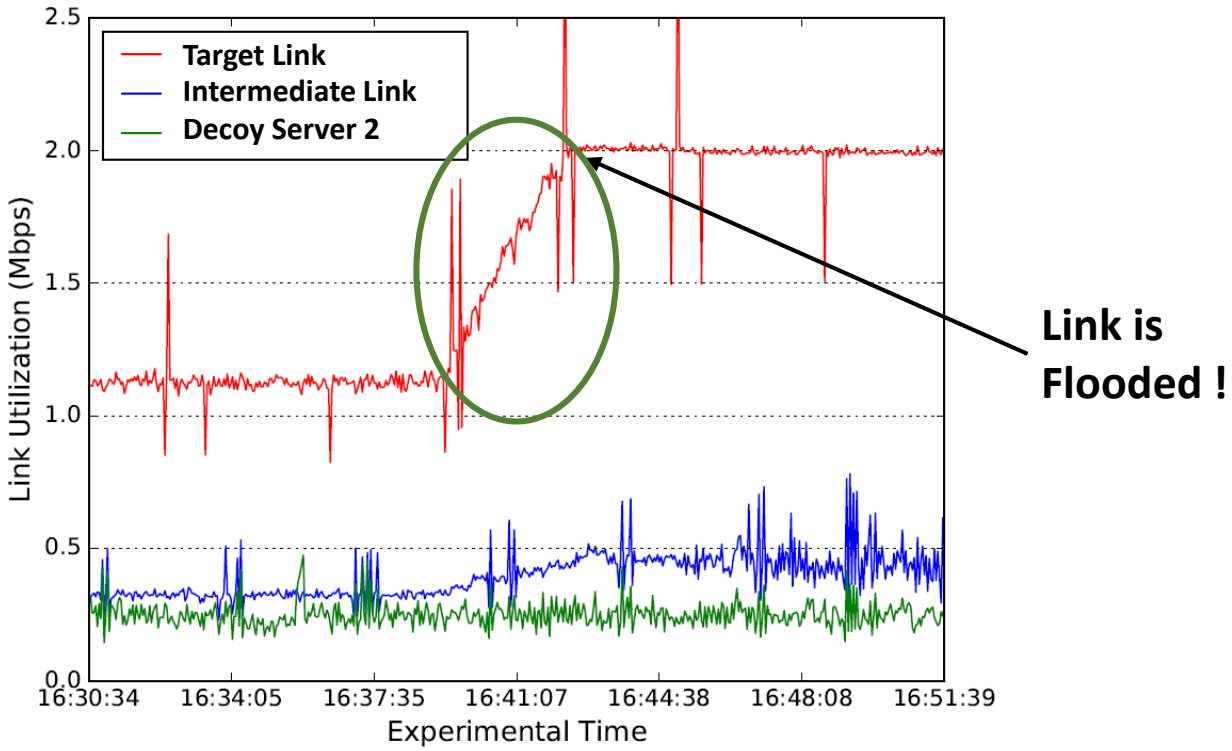
The Crossfire Attack Early Detection at the Warm-up period

Warm-up Period:

Time difference between the time of the **first bot-flow** of the attack reaches the target link and the moment the **target link is down**.

Objective:

Early detection of the the attack during the **warm-up period**.



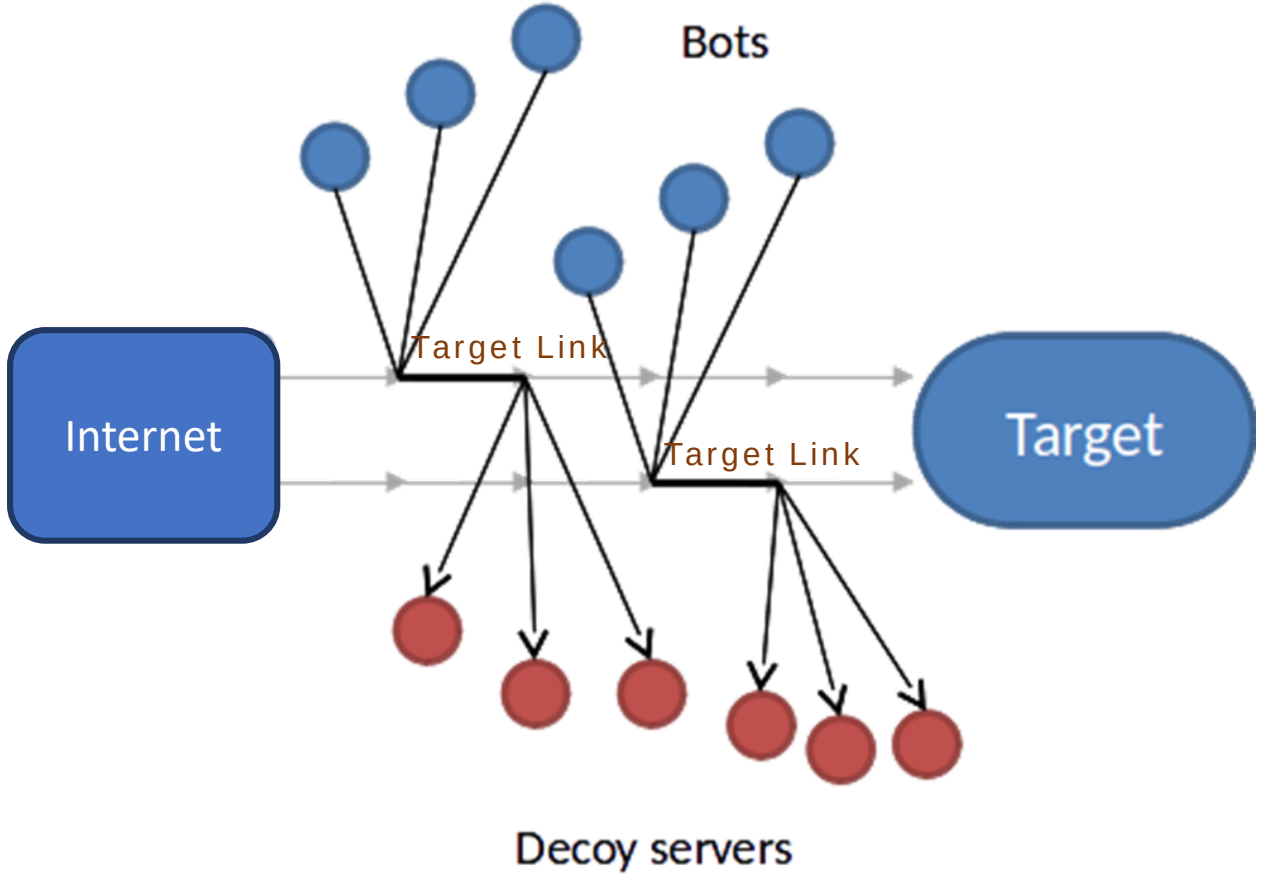
The Crossfire Attack

Stages of the attack

Stage 1: Link map construction

Stage 2: Target links selection

Stage 3: Bot coordination



Source: Min Suk Kang, Soo Bum Lee, Virgil D. Gligor, “The Crossfire Attack,” 2013 IEEE Symposium on Security and Privacy

Our Research Contribution

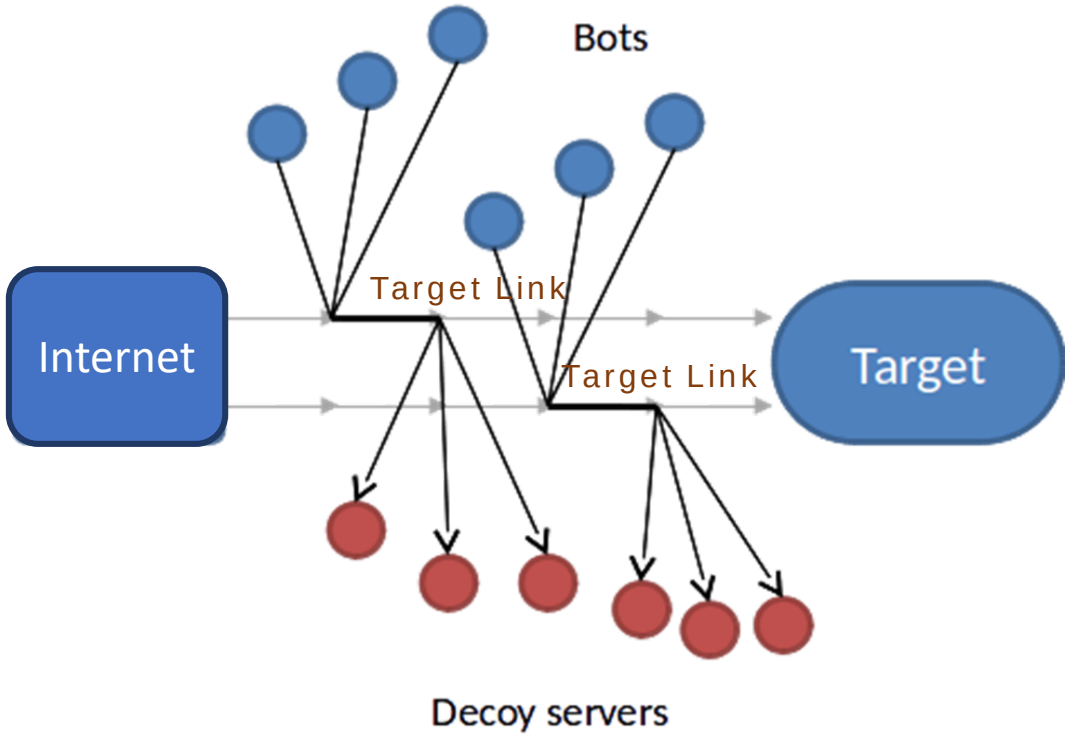
Detection Approach

- Analyse **pros and cons** of monitoring network traffic at different **locations**.
- Proposing location to monitor network traffic by providing justifications.

Methods of Detection

- Analyse **performances** of three **deep-learning models** on detecting the attack at the **proposed location.**

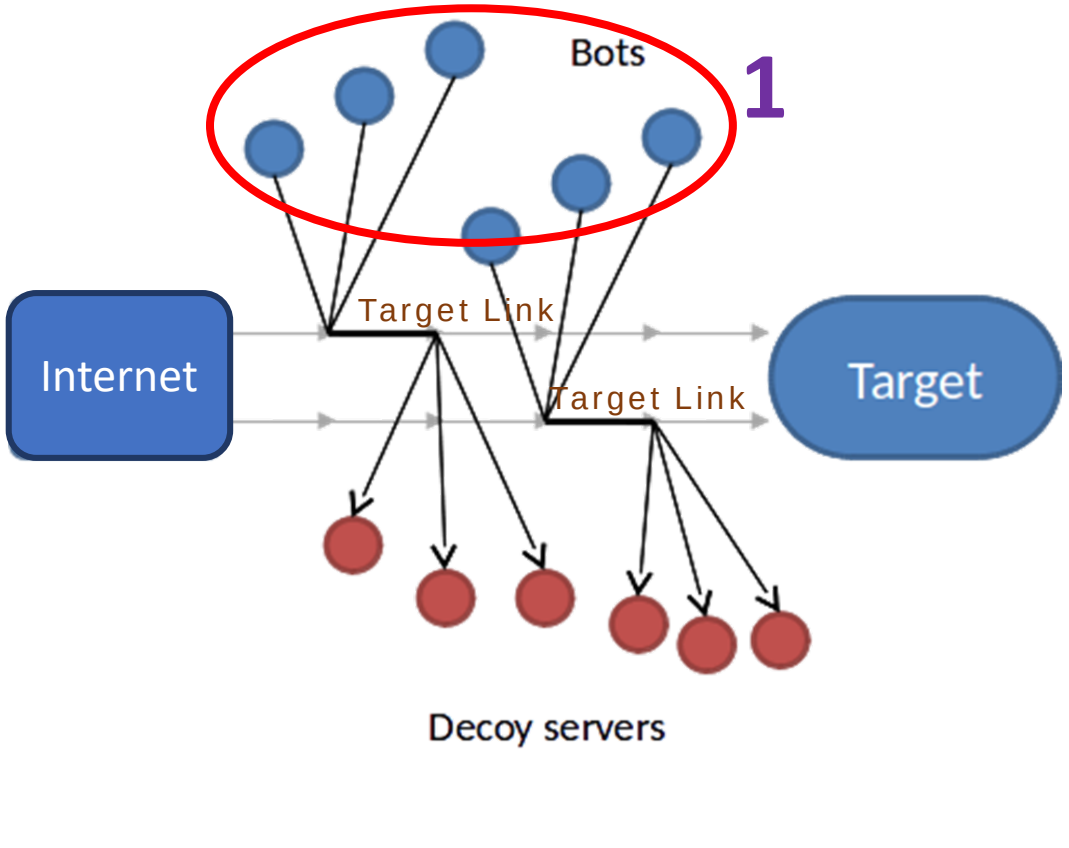
The Crossfire Attack **Detection Approach**



The Crossfire Attack Detection Approach

Advantages

- **Fastest** way to stop an attack



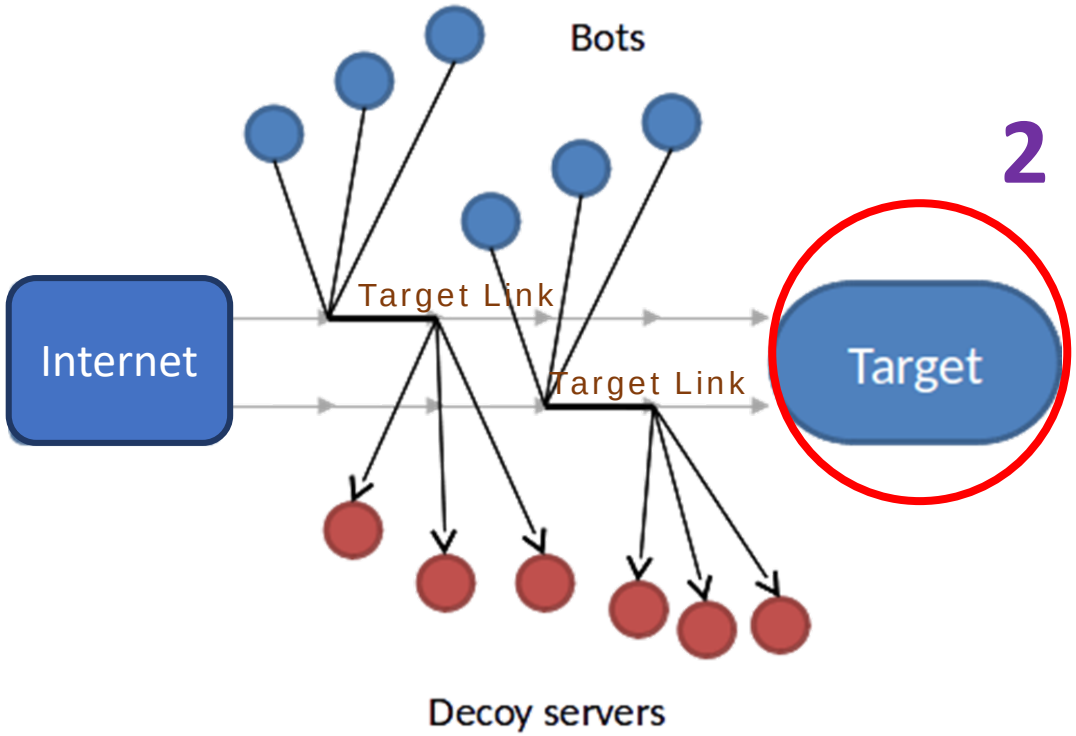
Disadvantages

- **Unknown location** of bots

The Crossfire Attack Detection Approach

Advantages

- Target areas are usually **equipped for self-defense.**



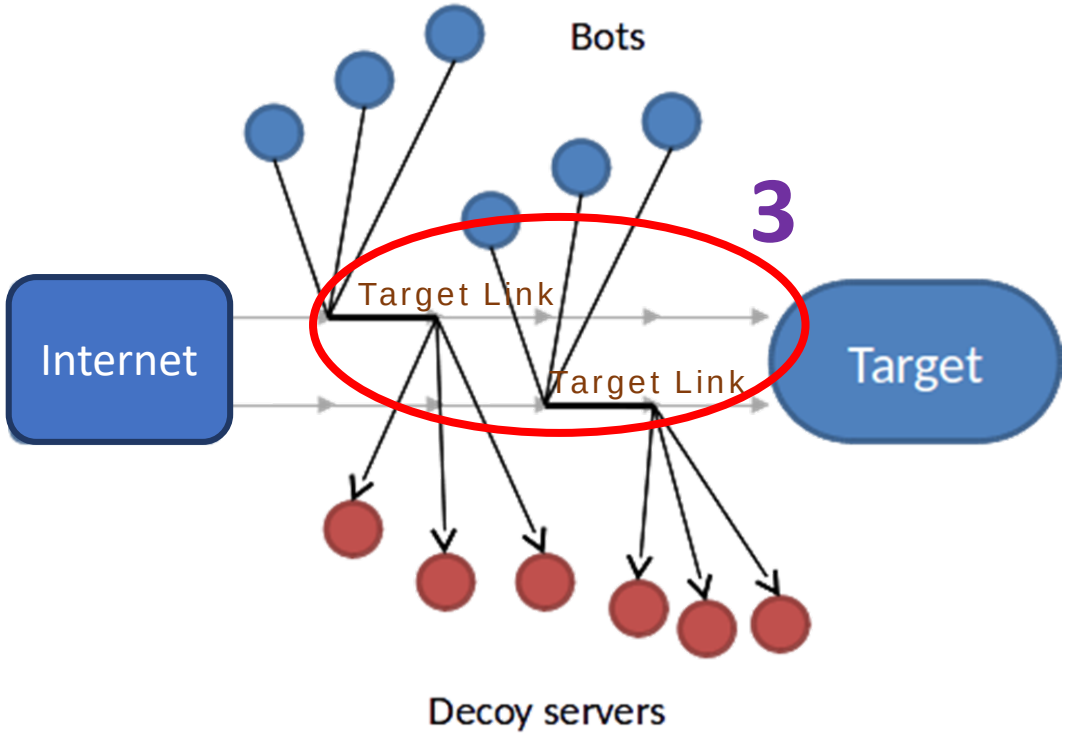
Disadvantages

- If **no decoy servers** are inside the target area, early detection is impossible.

The Crossfire Attack Detection Approach

Advantages

- A simple **threshold based detection system** could detect the trend of the incoming traffic.



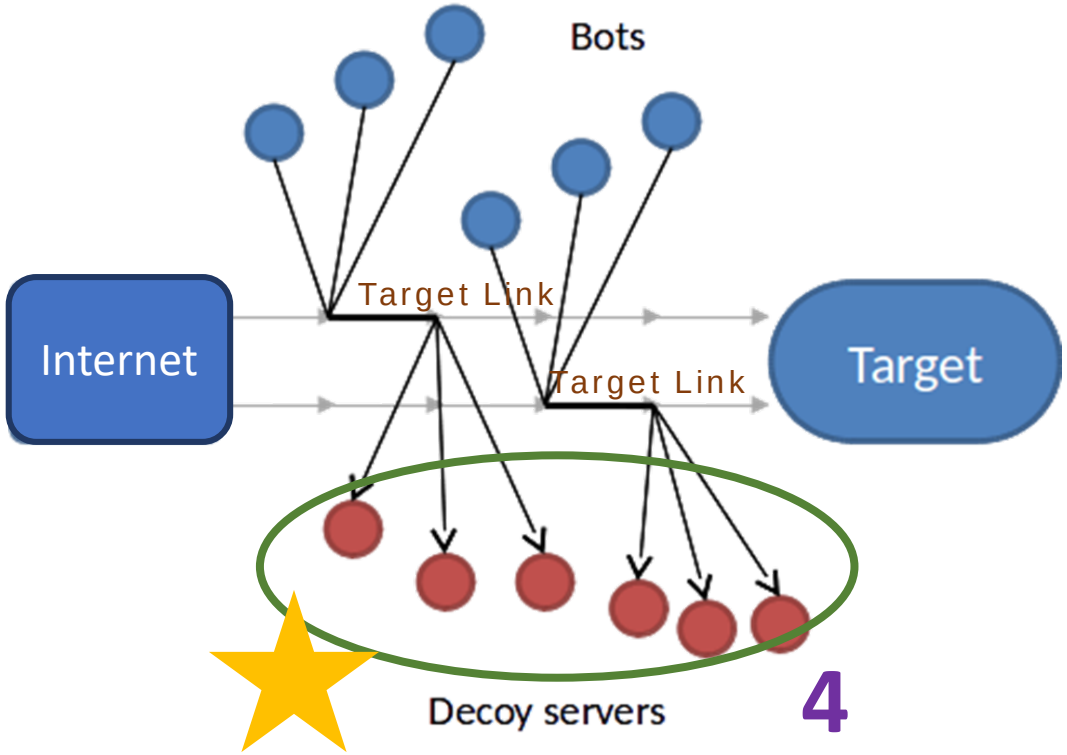
Disadvantages

- **Locations** of target links are **unknown.**
- Attacker may **switch target links** during an attack

The Crossfire Attack Detection Approach

Advantages

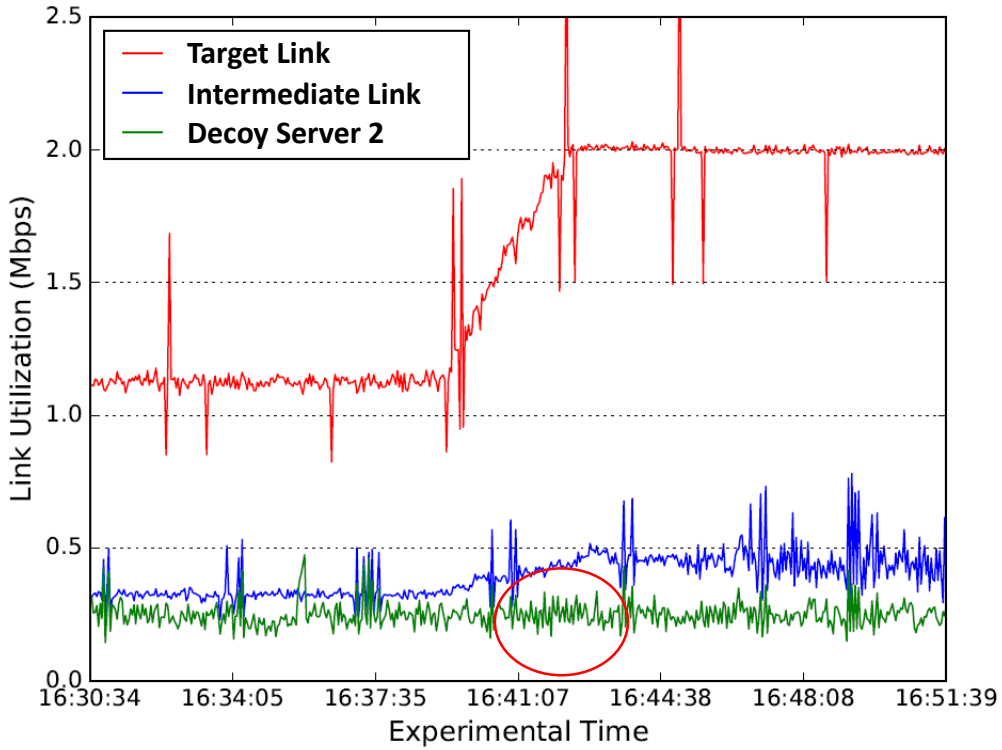
- Allow defenders to **examine the correlation** of attack traffic in the servers
- Defenders can **actively respond** to the attack



Disadvantages

- The **assumption** that the **decoy servers are not far** from the target area must be made

The Crossfire Attack **Detection Approach**



Difficulty of detection at decoy servers:

Attack traffic is almost **indistinguishable** from background traffic

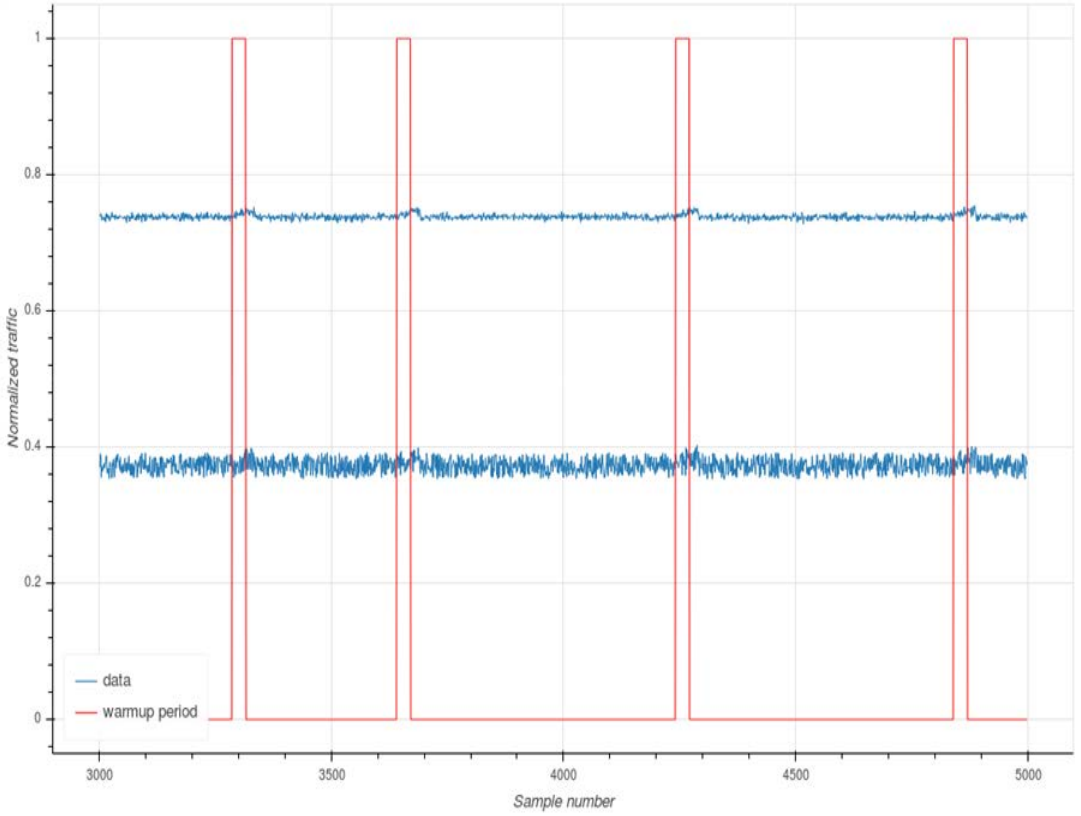
Network Data Data Simulation

Features of data

- The data is the link utilization **of 80 decoy servers.**

Distribution of data

- Background traffic is modelled by a Gaussian distribution
- When an attack happens, the link utilization slowly increases due to new attack traffic. This is called as the warmup phase of the attack.
- We attempt to detect the attack during this warmup period.



Detection Method

Random Forest (Baseline)

Deep-autoencoders

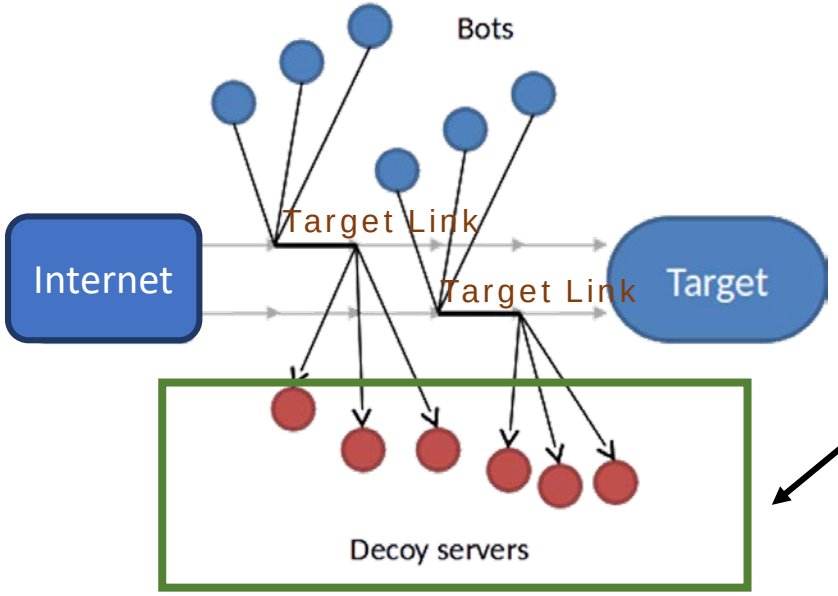
Convolutional Neural Network (CNN)

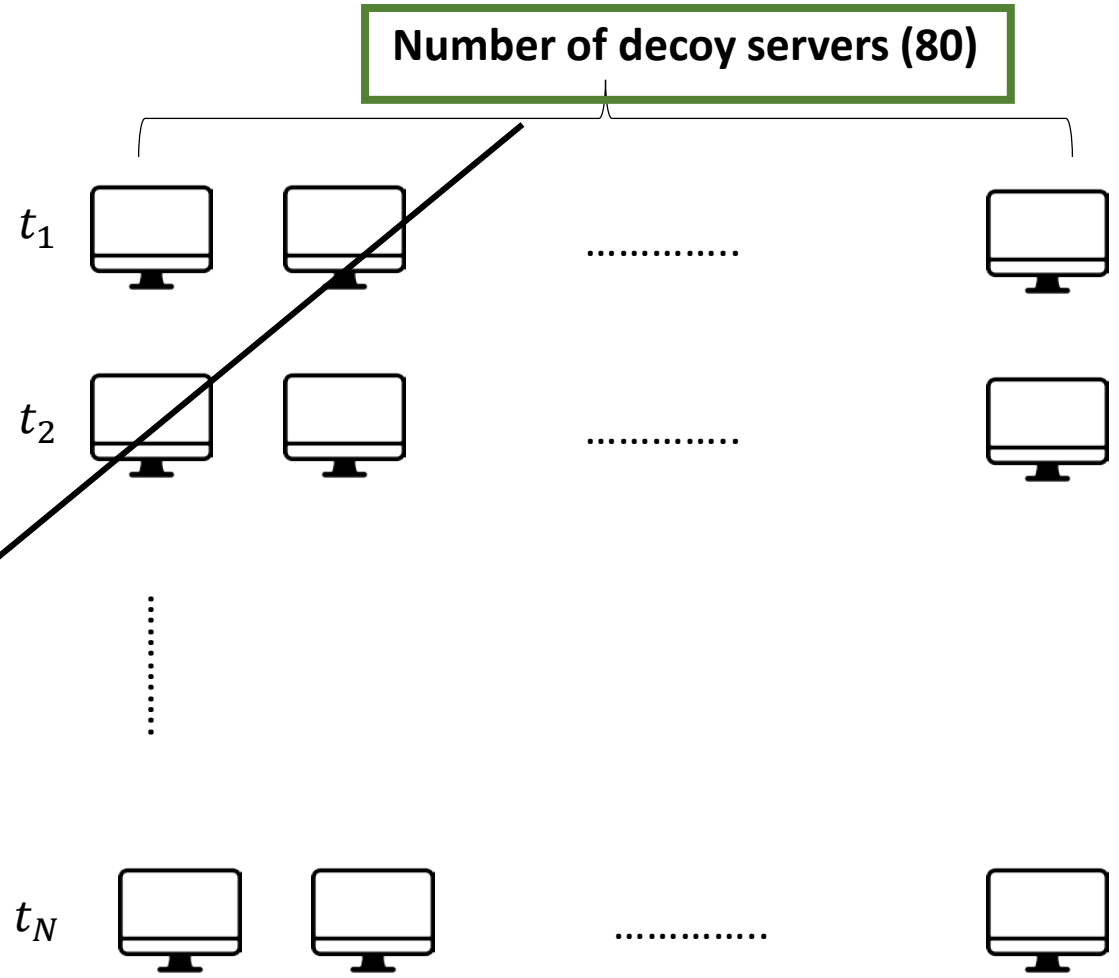
Long Short-Term Memory (LSTM)

Detection Method **Random Forest**

Data

- Each sample consists of **80 variables** representing network traffic value at each of the **80 decoy servers** at one time step.





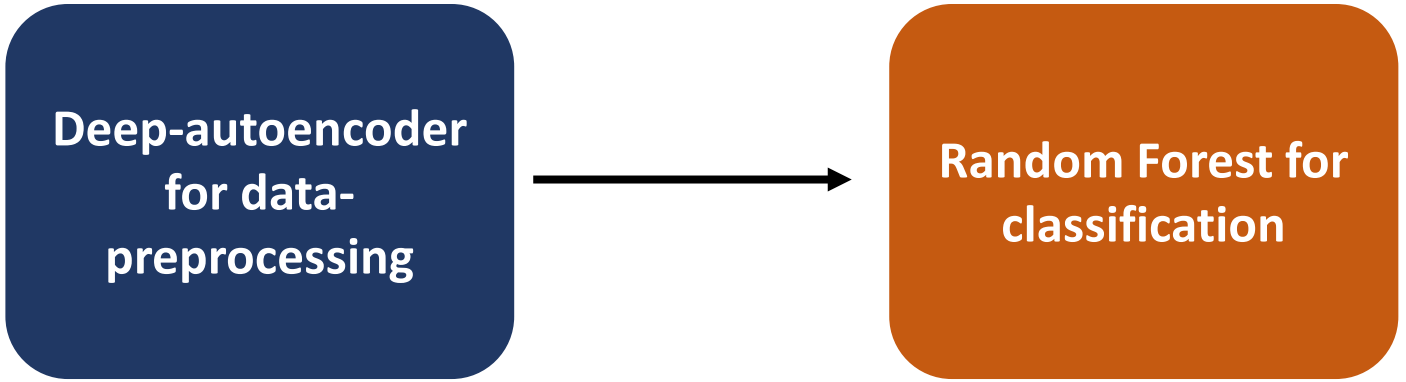
Detection Method **Baseline Performance**

	Threshold	Precision	Recall	F1
RF (Baseline)	0.38	0.81	0.66	**0.73**

Detection Method Deep Autoencoders

Method

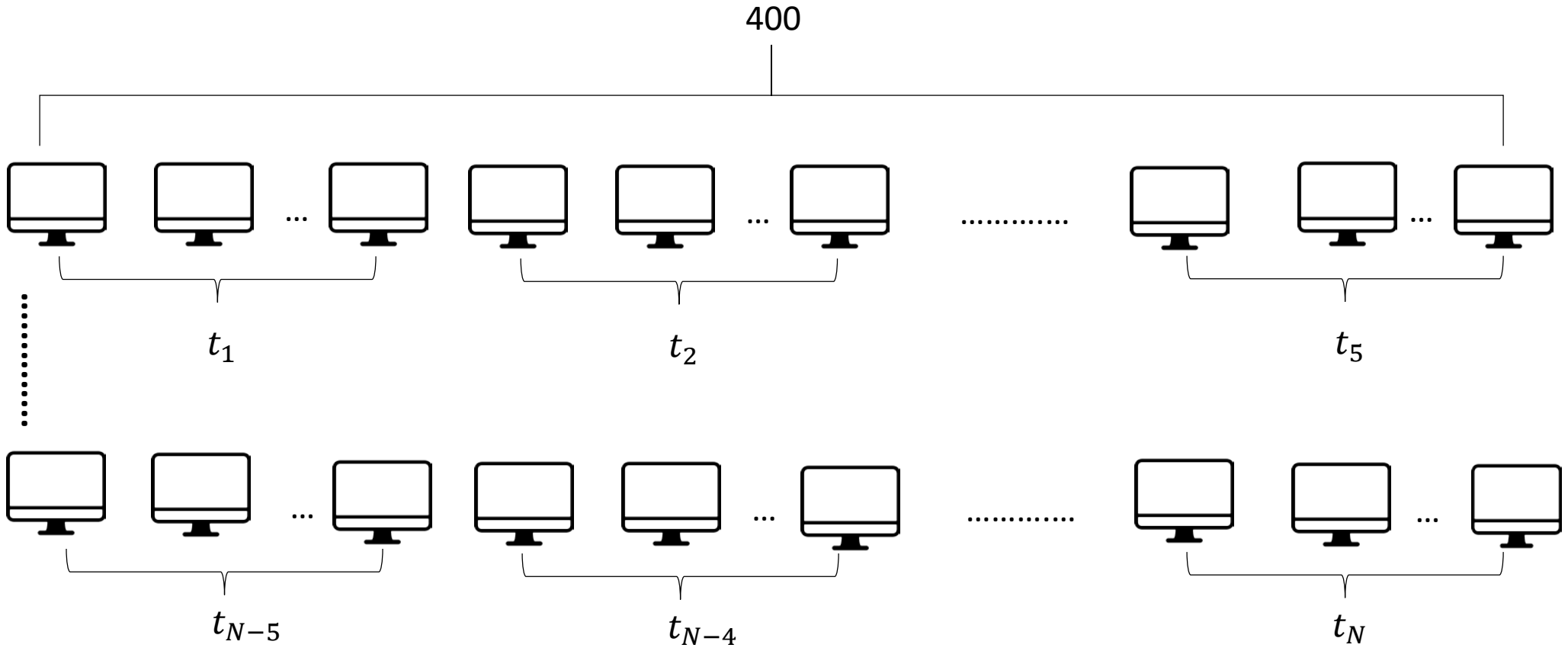
- Auto-encoder to extract intrinsic features from data
- Exploit spatiotemporal information from the data.
- Random Forest for classification of the extracted data



Detection Method **Deep Autoencoders**

Data

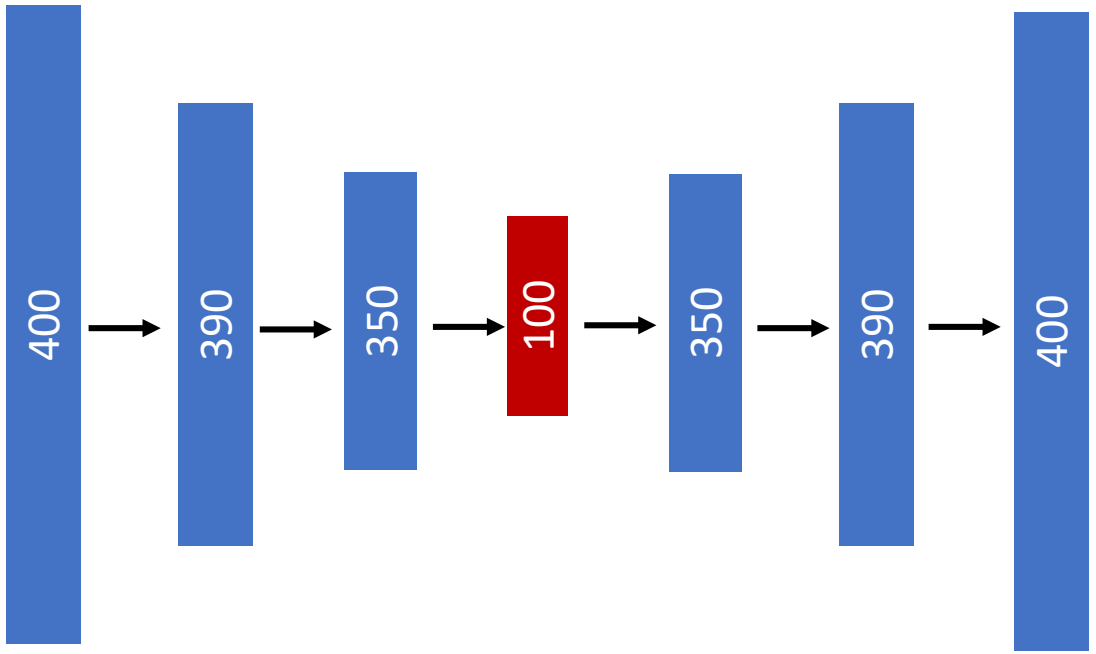
Spatio-temporal data (Windows of 5 time-steps)



Detection Method Deep Autoencoders

Autoencoder structure

400-390-350-**100**-350-390-400



Detection Method **Deep Autoencoders performance**

	Threshold	Precision	Recall	F1
RF (Baseline)	0.38	0.81	0.66	0.73
Autoencoder	0.35	0.71	0.63	**0.66**

Detection Method CNN Intuition

The Temporal Filter

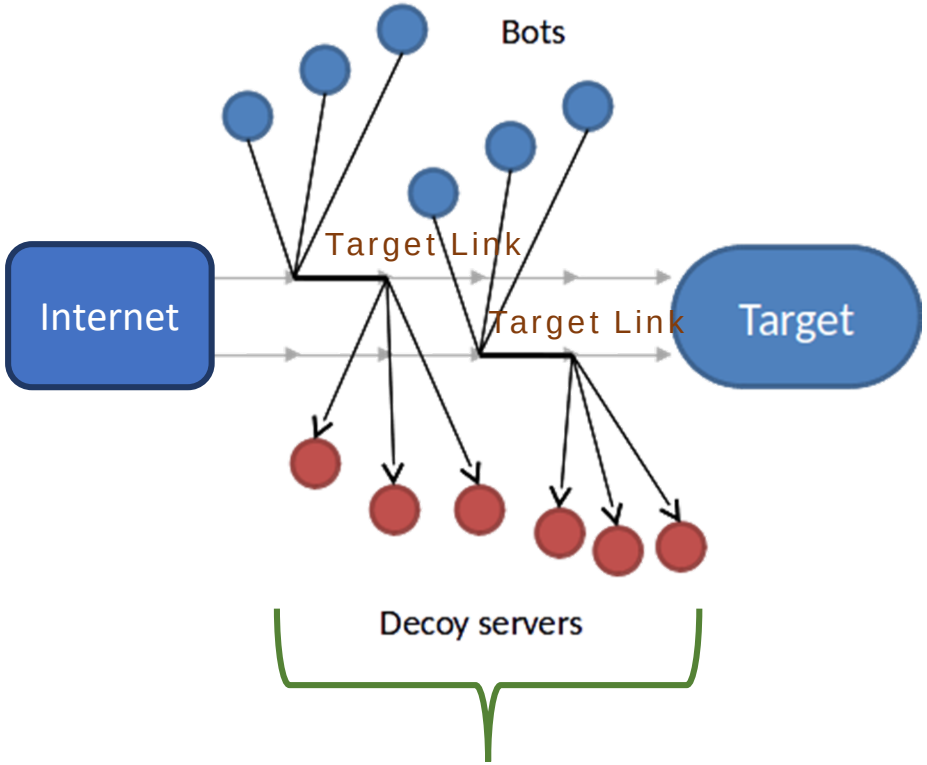
Learns the pattern for the attack **only in the time axis independent** of the **servers**.

The Spatial Filter

Discover the correlation between different servers as they are under attack at the same time.

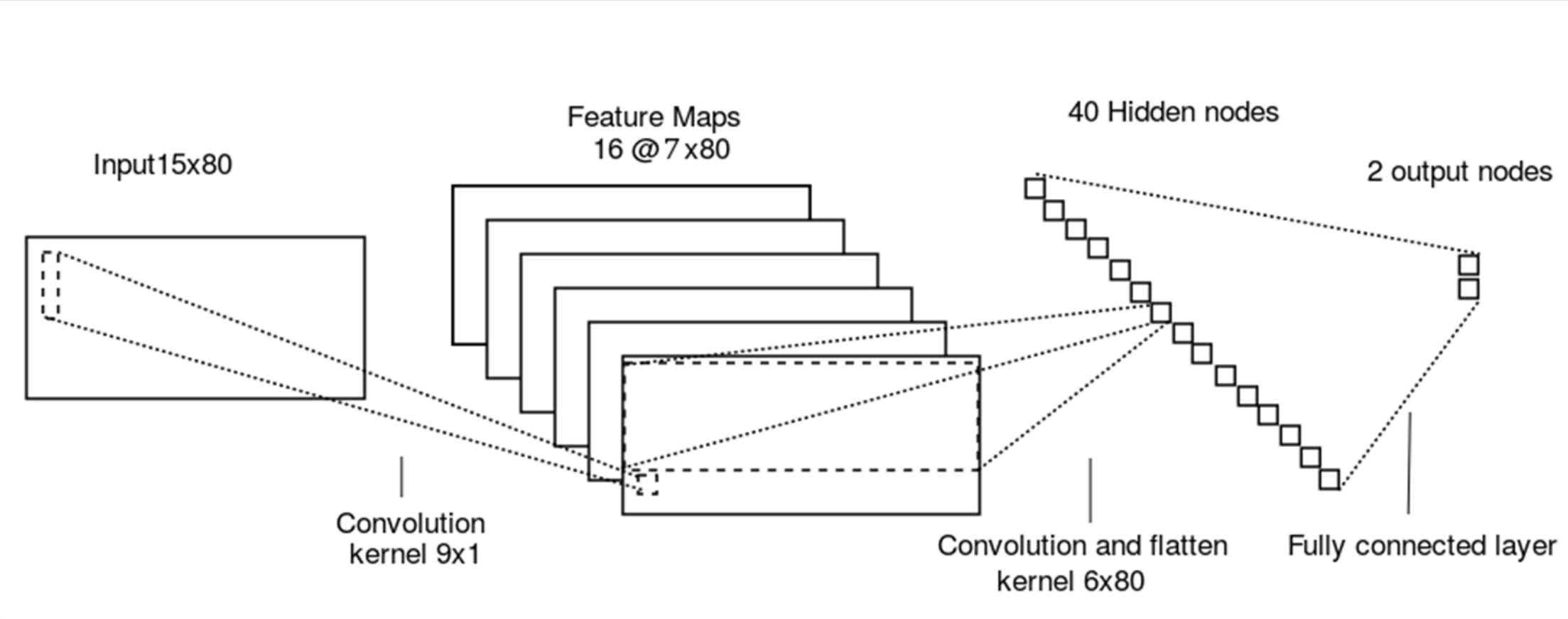
Fully Connected layer

Binary Output:
Attack or not?



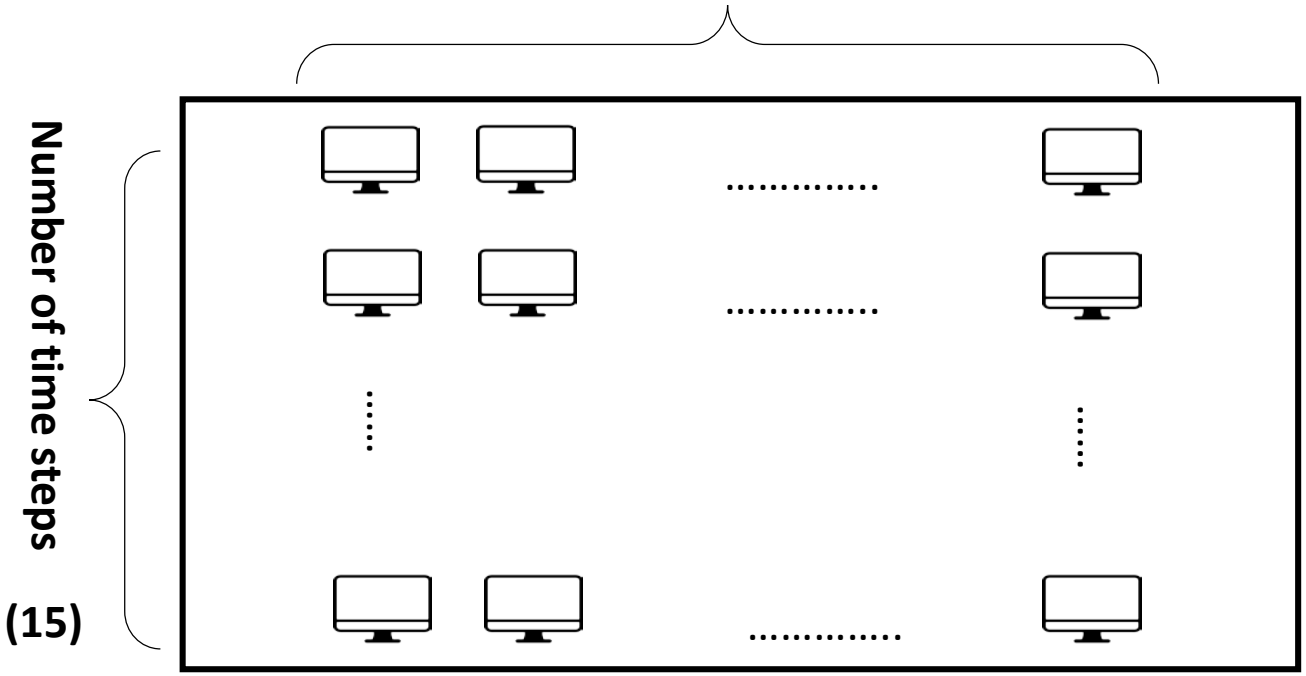
Spatial Dimension

Detection Method CNN Structure

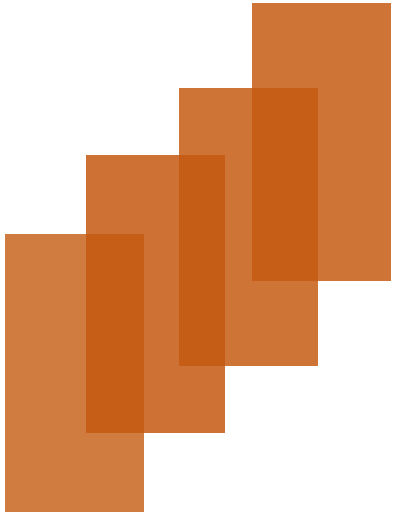


Detection Method 1st convolution step

Input Data:
15 X 80 windows

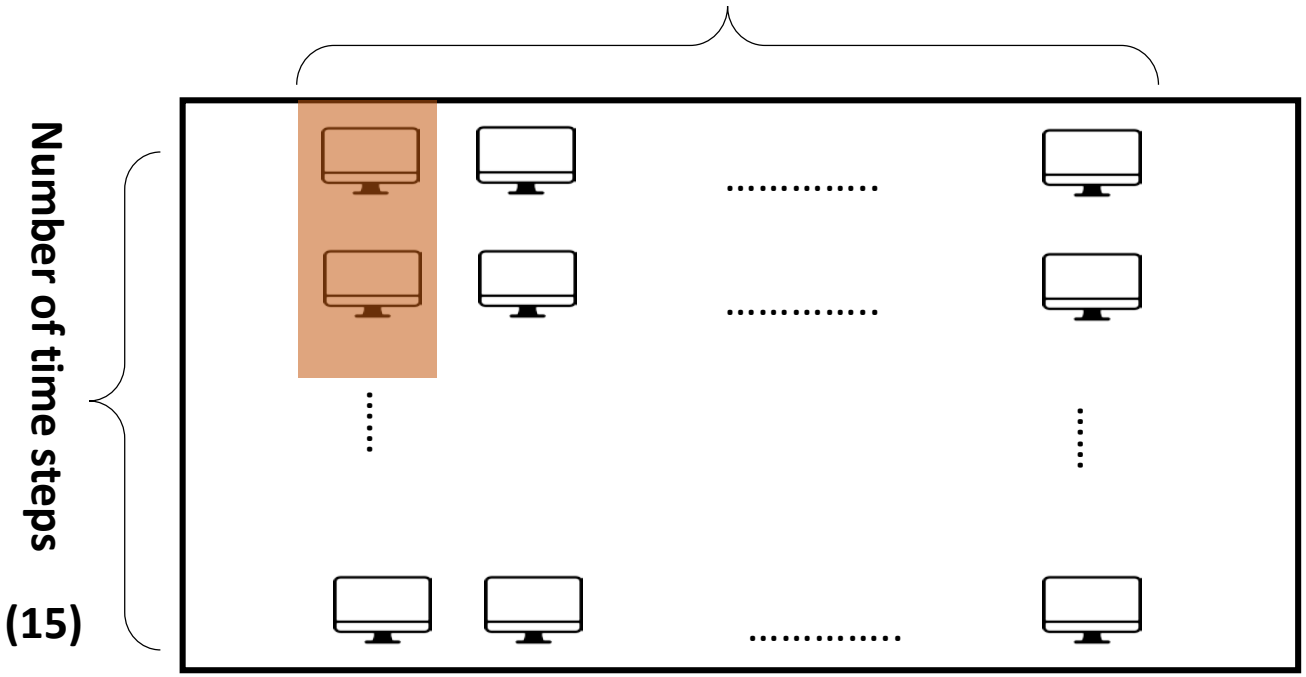


Temporal filters:
16 @ 9x1 filters



Detection Method 1st convolution step

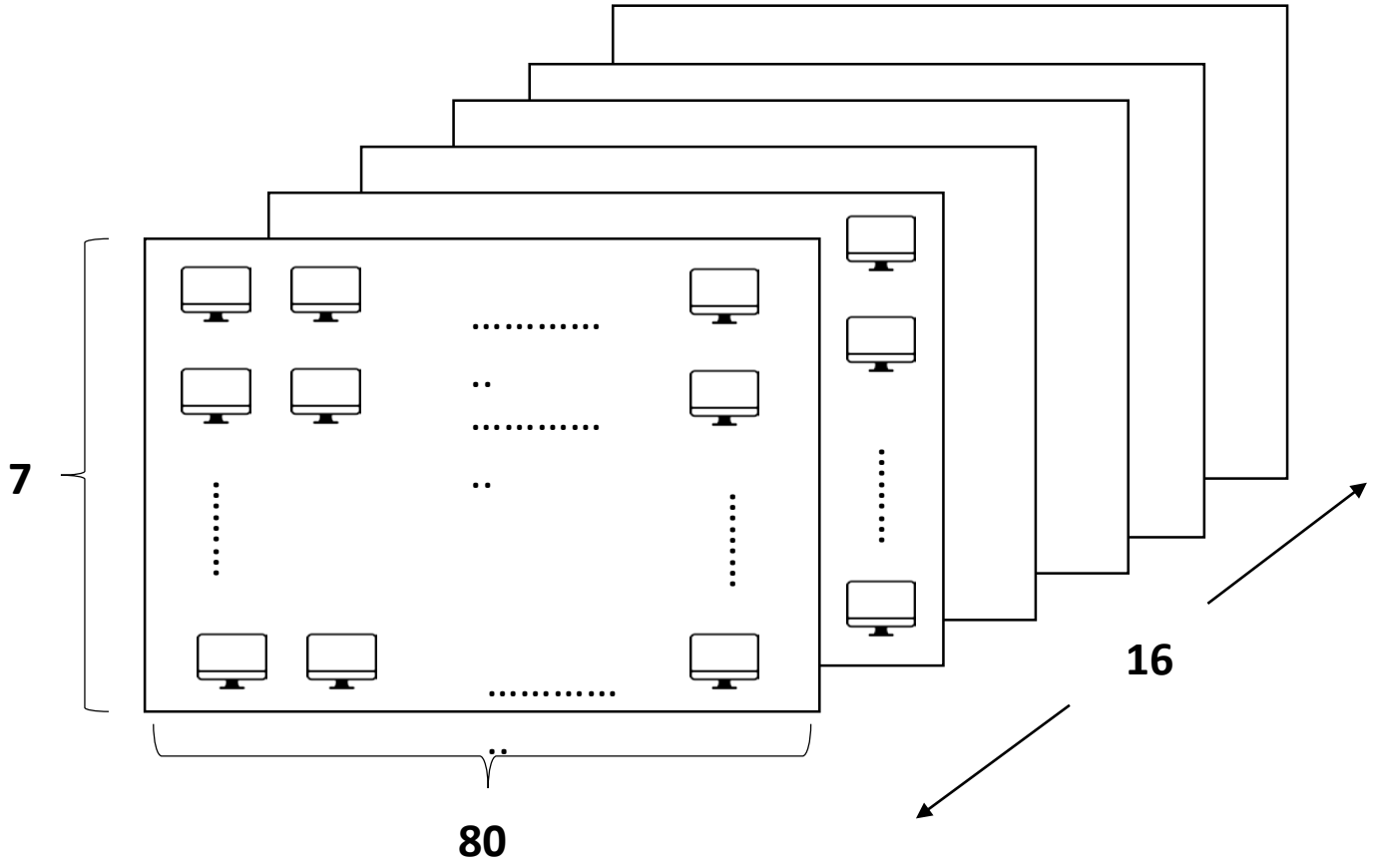
Input Data:
15 X 80 windows



Temporal filters:
16 @ 9x1 filters

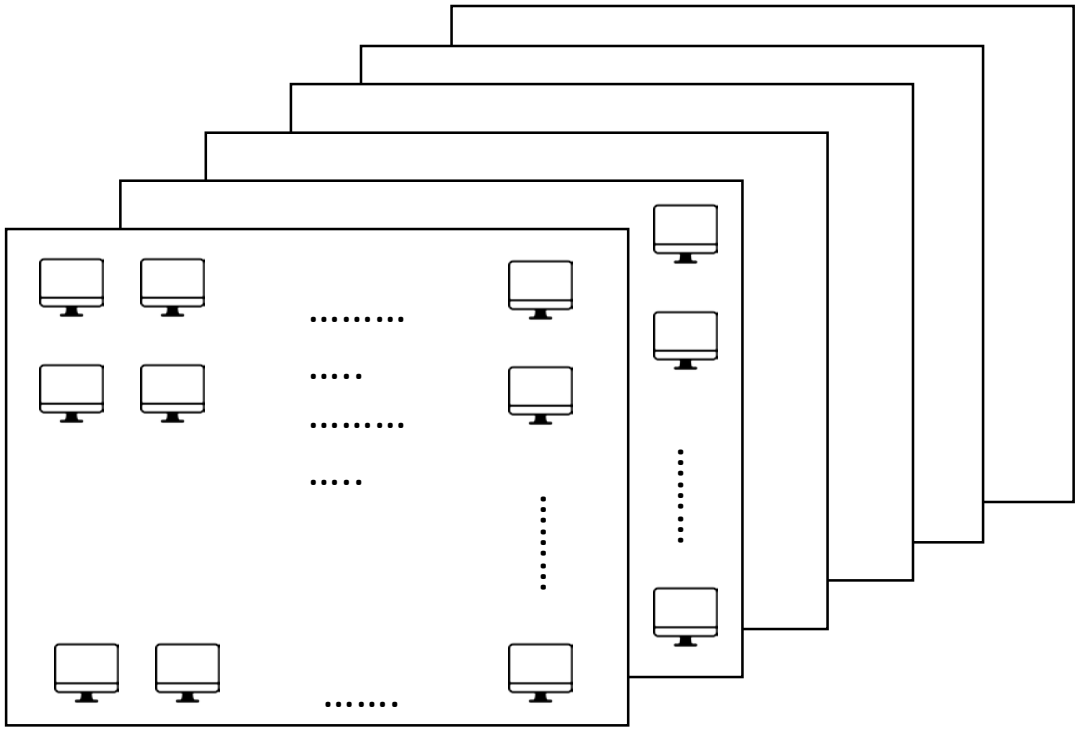
Detection Method 1st convolution step

Output of first convolution step:
16 Feature Maps of size **7 x 80**

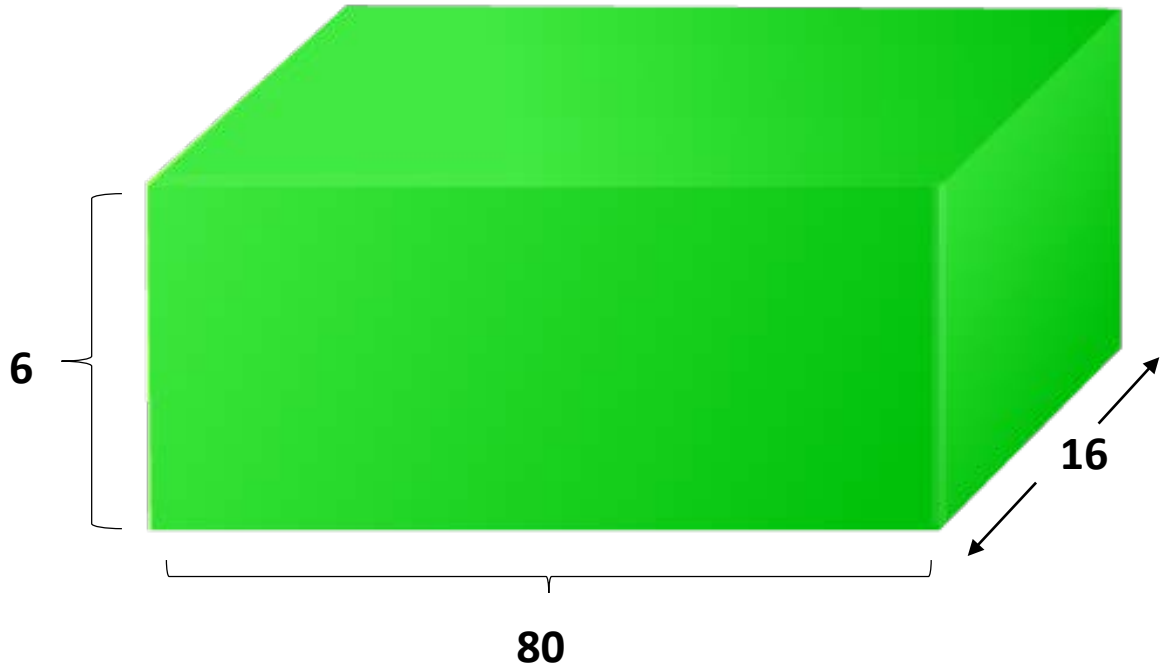


Detection Method 2nd convolution step

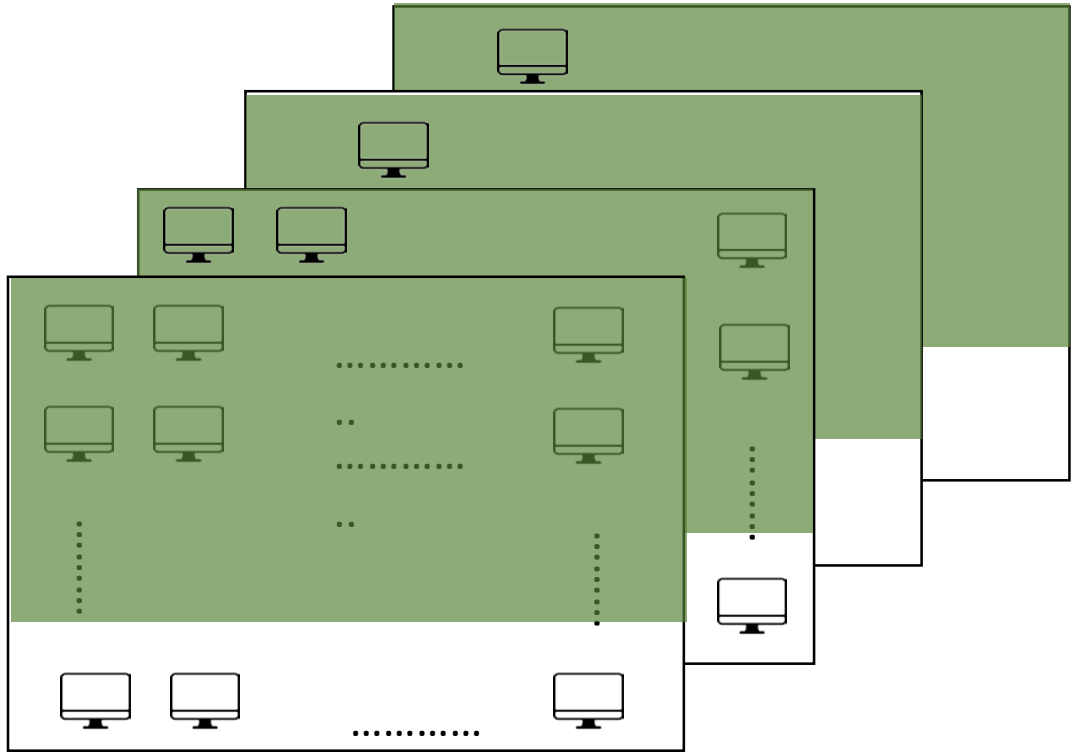
Input Data:
16 feature maps



Spatial filters:
20 @ 6x80x16 filters

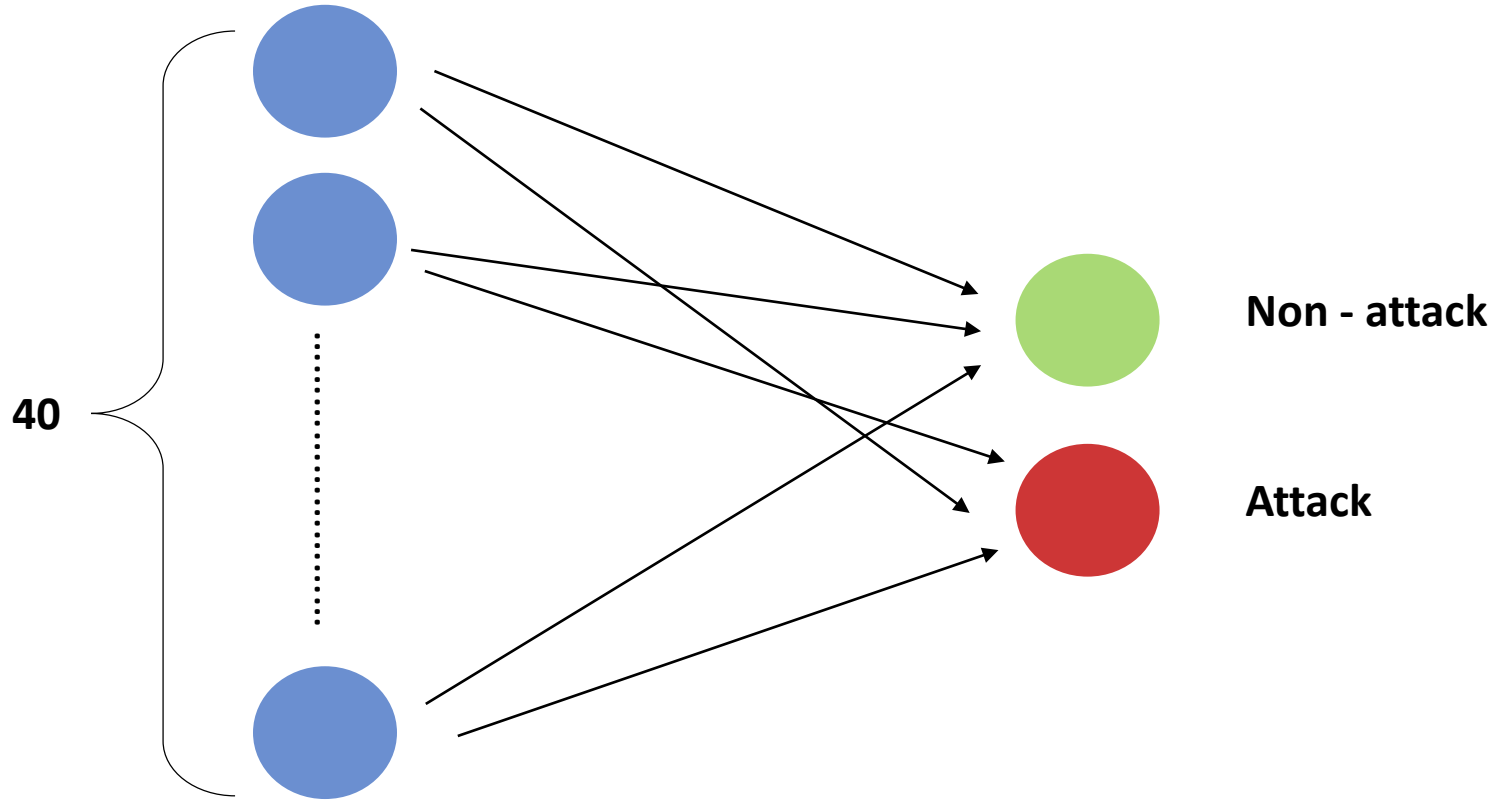


Detection Method 2nd convolution step



X 20

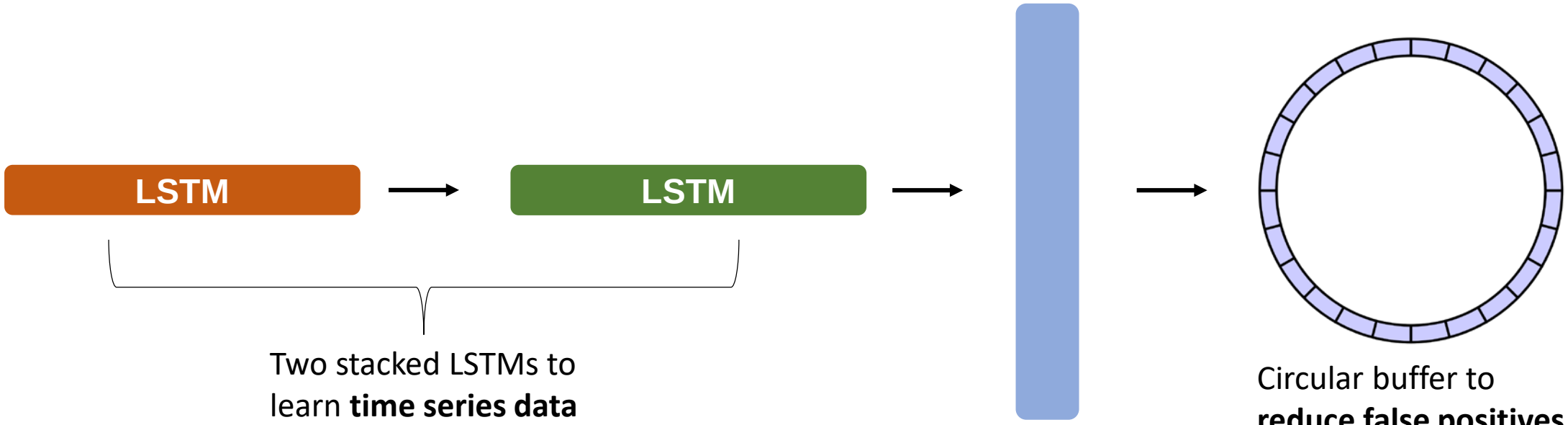
Detection Method Last convolution step



Detection Method CNN Performance

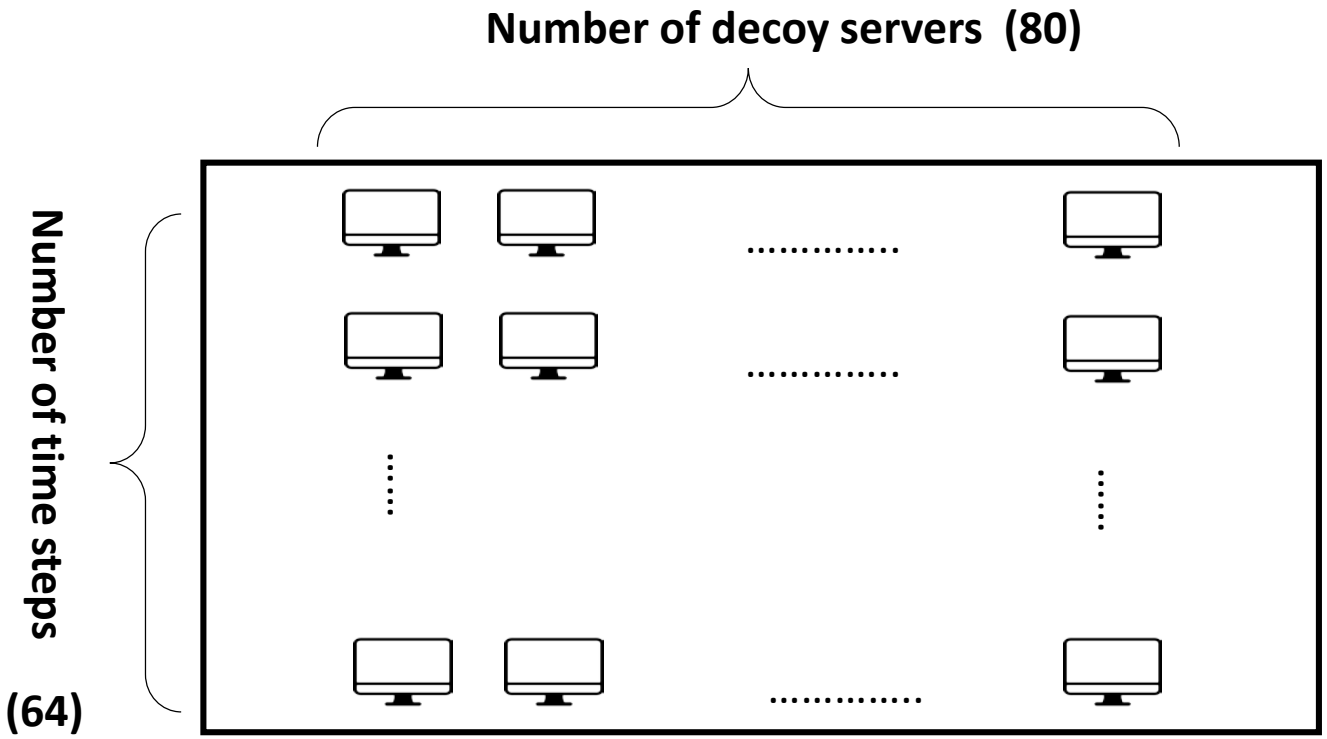
	Threshold	Precision	Recall	F1
RF (Baseline)	0.38	0.81	0.66	0.73
Autoencoder	0.35	0.71	0.63	0.66
CNN	0.50	0.74	0.97	**0.84**

Detection Method LSTM intuition

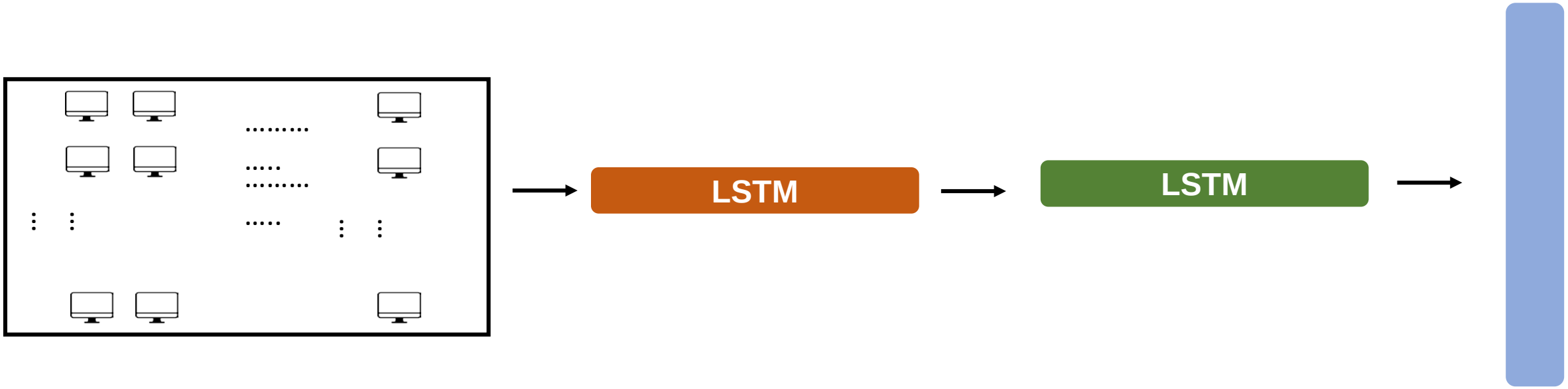


Detection Method LSTM

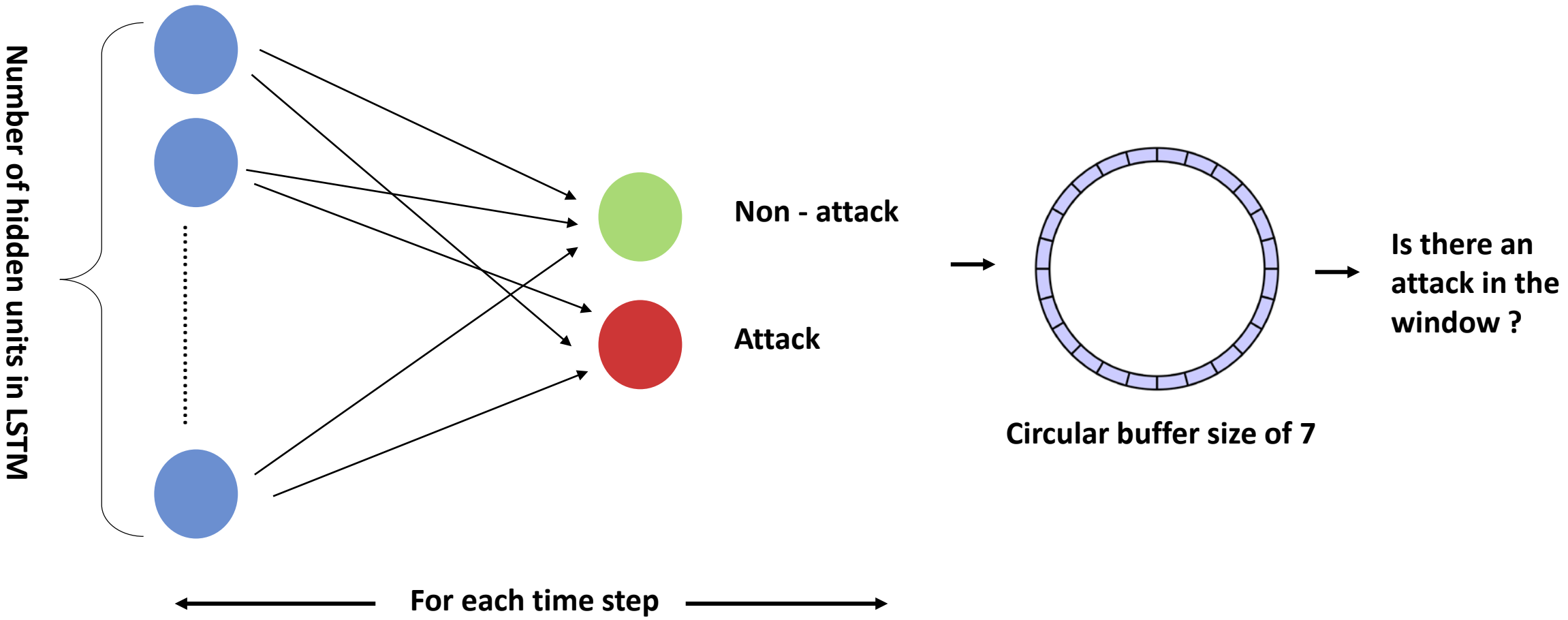
Input Data:
64 X 80 windows



Detection Method LSTM



Detection Method LSTM



Detection Method LSTM Performance

	Threshold	Precision	Recall	F1
RF (Baseline)	0.38	0.81	0.66	0.73
Autoencoder	0.35	0.71	0.63	0.66
CNN	0.50	0.74	0.97	0.84
LSTM	0.50	1.00	0.998	**0.999**

Conclusion

Research Focus

- Proposing location for detection
- Develop deep-learning models for attack detection

Performance of models

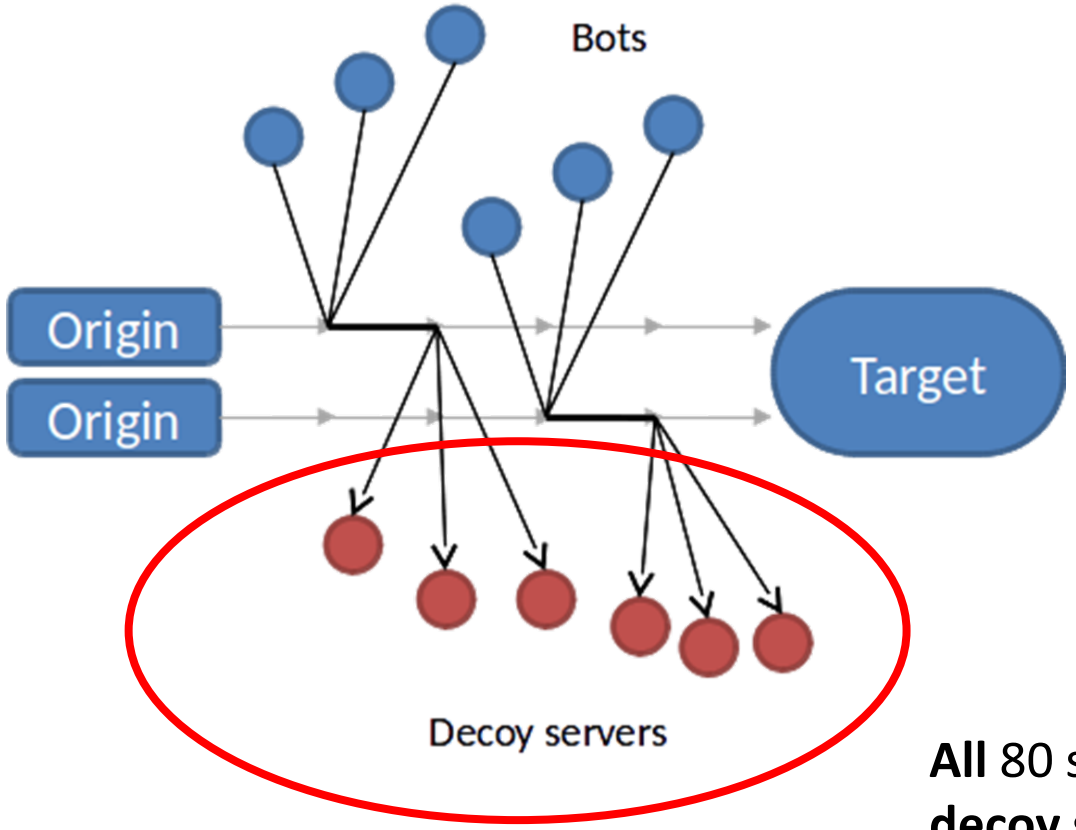
- Long Short-Term Memory Network (LSTM) has the best performance

Future work

- Simulate actual Crossfire Attack on testbeds
- Test models

Detection Method **Simulating more realistic attack condition**

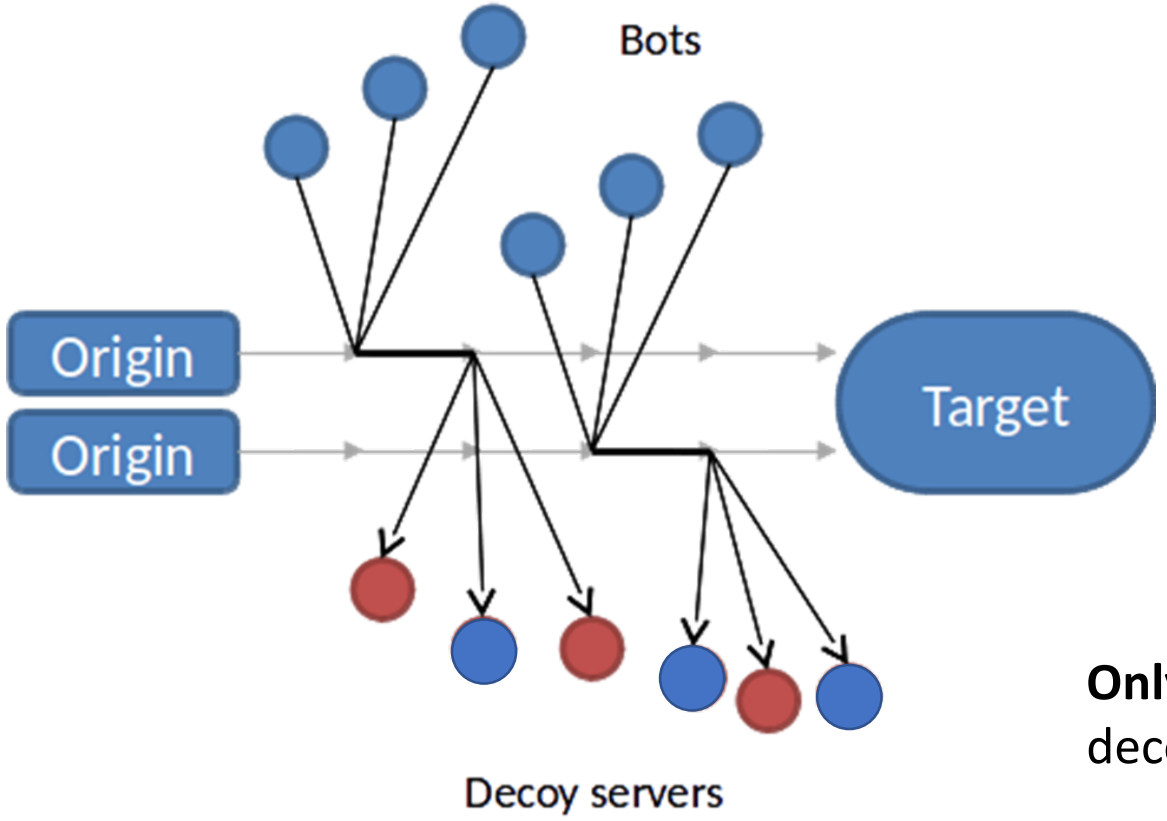
Current Assumption



All 80 servers are **decoy servers**

Detection Method **Simulating more realistic attack condition**

Simulating actual attack scenario



Only 70 servers are decoy servers

Detection Method Performance of new attack condition

Convolutional Neural Network (CNN)

Servers under attack	Threshold	Precision	Recall	F1
80/80	0.50	0.74	0.97	0.84
70/80	0.50	0.759	0.78	**0.773**

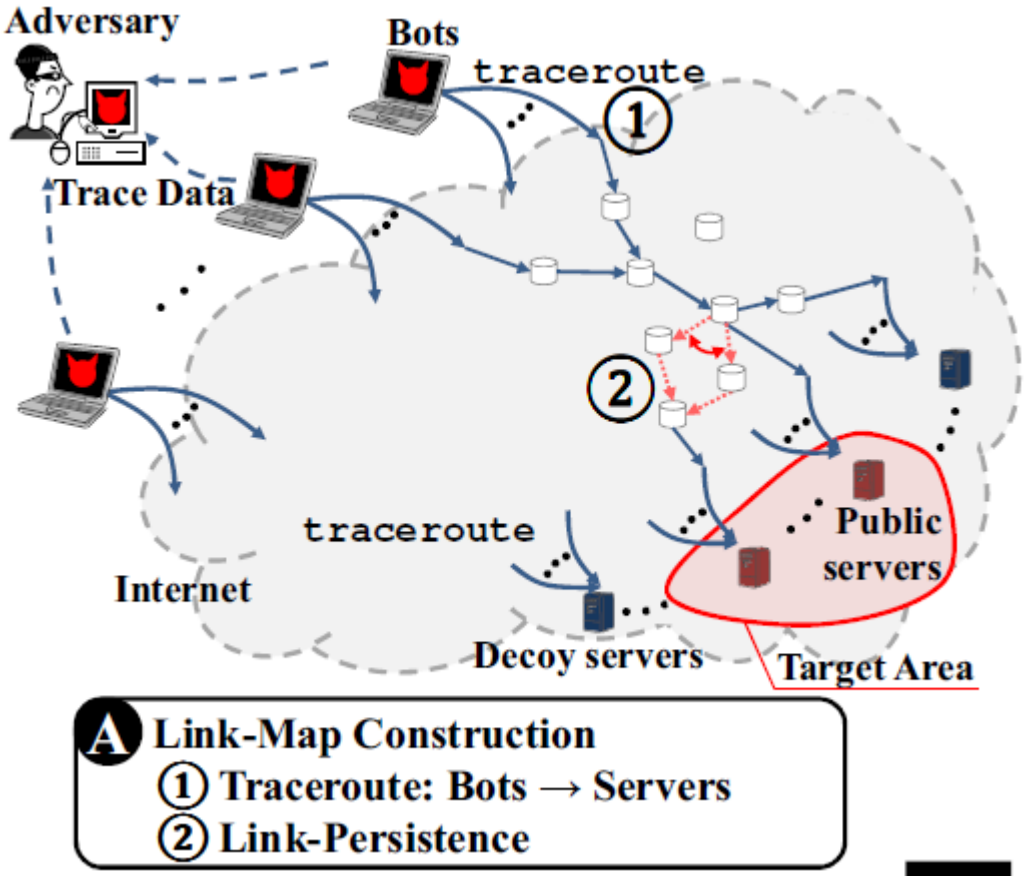
Long Short-Term Memory Network (LSTM)

Servers under attack	Threshold	Precision	Recall	F1
80/80	0.50	1.00	0.998	0.999
70/80	0.50	0.995	0.964	**0.979**

The Crossfire Attack Stages of the attack

Stage 1: Link map construction

The attacker determines the **topology** of the network and creates a **link map**.

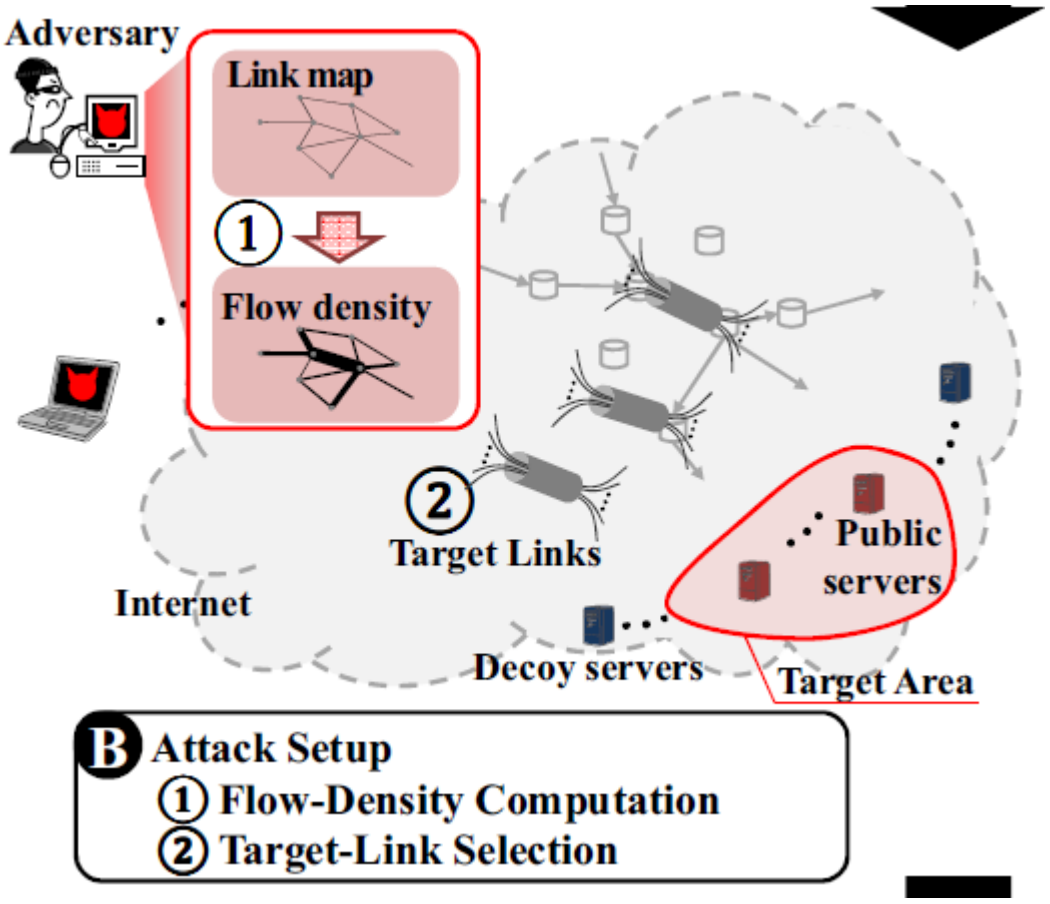


Source: Min Suk Kang, Soo Bum Lee, Virgil D. Gligor, "The Crossfire Attack," 2013 IEEE Symposium on Security and Privacy

The Crossfire Attack Stages of the attack

Stage 2: Target links selection

The attacker selects the set of **target links** after evaluating their stability and utilization

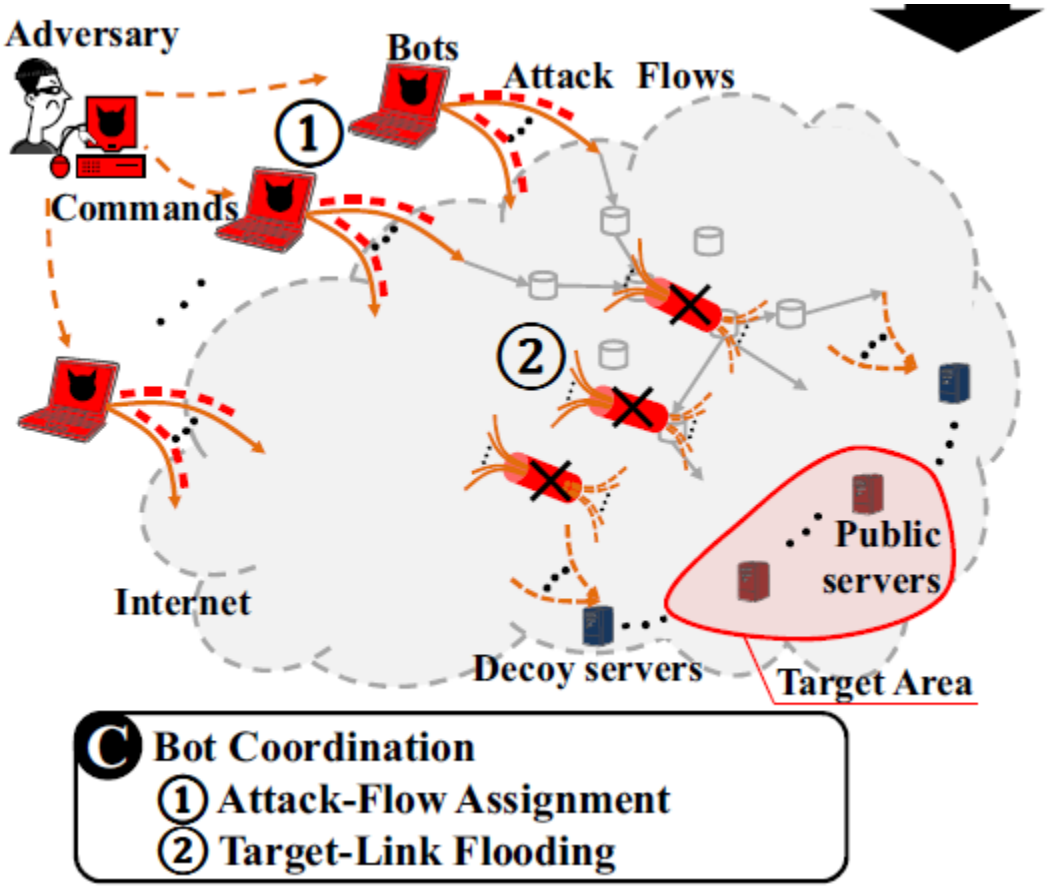


Source: Min Suk Kang, Soo Bum Lee, Virgil D. Gligor, “The Crossfire Attack,” 2013 IEEE Symposium on Security and Privacy

The Crossfire Attack Stages of the attack

Stage 3: Bot coordination

The attacker **coordinates the bot** to generate **low-rate traffic** to the decoy servers which **aggregate** at the target links.



Source: Min Suk Kang, Soo Bum Lee, Virgil D. Gligor, “The Crossfire Attack,” 2013 IEEE Symposium on Security and Privacy