Computer Networks
컴퓨터네트워크

(Course syllabus)

Wonjun Lee, Ph.D., IEEE Fellow
Network and Security Research Lab. (NetLab)
http://netlab.korea.ac.kr
http://mobile.korea.ac.kr
Korea University

COURSE INFORMATION & POLICY

ABOUT MYSELF

Instructor: Wonjun Lee

- **Wonjun Lee, Ph.D., IEEE Fellow**

- Contact information: *wlee AT korea.ac.kr*
  - http://netlab.korea.ac.kr

Computer Networks (담당교수 : 이원준; wlee@korea.ac.kr)

- 강의 요목

This course covers the fundamentals and various issues from the broad areas of modern communication networks, including wired, mobile, and communication networks. Through various practical tasks and projects, network security skills would be fertile

- 강의 내용

✓ **Introduction to wired & wireless communication networks**
  . TCP/IP protocol suite
  . cellular communication networks
  . Wi-Fi premier

✓ (Wired) network security 2학기
  . network security applications
  . network access control and cloud security
  . transport-level security
  . IP security
  . operational security

✓ Advanced topics (Wireless communication security) 2학기
  . mobile network security
  . wireless communication network security (4G LTE, 5G)
  . security issues for LR-WPAN (BLE, ZigBee, CTC/CTI)
  . recent developments of IEEE 802.11 Wi-Fi security
  . wireless PHY-level security
  . case studies

About me

Network and Security Research Lab. (지도교수 : 이원준)

- 학력:

    (美) University of Minnesota 컴퓨터공학 박사
    (美) University of Maryland 컴퓨터공학 석사
    서울대학교 공과대학 컴퓨터공학과 석사
    서울대학교 공과대학 컴퓨터공학과 석사

- 주요경력:

    (現) 고려대학교 정보보호대학원 교수
    (現) 고려대학교 스마트보안학부 사이버국방학과 교수
    (現) 고려대학교 미래네트워크연구소(FNC) 연구소장
    (前) 고려대학교 정보통신대학 컴퓨터학과 교수
    (前) 고려대학교 WCU 미래네트워크최적화기술 사업단장
    (賞) IEEE Fellow(석학회원)
    (賞) 한국과학기술한림원(KAST) 정회원(Fellow)
    (賞) 한국공학한림원(NAEK) 정회원

- 주요 연구분야

    유무선 네트워크 프로토콜
    RF-Powered 네트워킹
    네트워크 및 무선통신 보안
    데이터센터/클라우드 네트워킹

Teaching Assistants

- 조교장:
  - **Wonwoo Jang (장원우) 박사과정**, wwjang AT korea.ac.kr
  - 조교: Seungmin Lee 이승민 연구원

- *Office: 우정정보관 5F 507A호* ***(네트워크및보안 연구실); NetLab***

스마트보안학부 네트워크/통신 과목은 3학년 1, 2학기 통년으로 구성

- **3학년 1학기:**

  - **COSE342 컴퓨터네트워크 @컴퓨터학과** (유선 네트워크, 인터넷 아키텍쳐);

- **3학년 2학기:**

  (신설) SMRT324 컴퓨터네트워크보안 @ 스마트보안학부 (네트워크 보안, 무선/모바일 통신네트워크 + 무선 보안);

  Shall be open for 스마트보안학부/사국/컴퓨터학과/데이터과학과/전전학부/자유전공학부/…

Course workload

Midterm exams 2회	(up to 30~40%)
Final exam	(up to 30~40%)
Quiz, Projects, Homework	(up to 15~30%)
Attendance, attitude, participation	(up to 10%)

- Note
  - Final exam will be "comprehensive", i.e., it covers all (including midterm exams) material taught in class
  - Quiz exams will be taken once (or twice) every month
  - **Total *3* absence → 'F' degree**
  - The weighting scheme used for grading can be changed a bit

Course policy

- Questionnaire 설문조사 is ***mandatory*** (2nd week after enrollment process is over)

1. 텀 프로젝트를 포함한 컴퓨터 네트워킹 프로그래밍 과제 1~2차례.

2. 과제 미제출 시 최저학점 부여.
   여러 차례의 숙제 있음.

3. 적어도 2~4주에 한 번씩 퀴즈 시험 실시. (미 응시 경우 최종학점 부여 시 추가 감점 있음).

4. 모든 숙제, 과제는 마감 일시까지 제출된 경우만 인정함.

5. 출석/지각 및 참여도는 최종 점수에 **<u>중요하게</u>** 반영함.

- 최종학점 관련한 문의는 일체 받지 않습니다.
- 수업유형(대면 강의 & 온라인 녹화 강의)
- 성적평가방식(대면 시험, 대면 퀴즈, term project, homework)
- 시험일정: TBA

- 더 자세한 사항은 Blackboard/e-mail을 통해 수업 관련 사항 공고.
- All the lecture notes and reference papers including reading assignments and change of schedule will be posted in Blackboard or by e-mail.

Course material (no main textbook)

- Lecture notes and textbook
- Supplementary material via class e-mail list

Class information

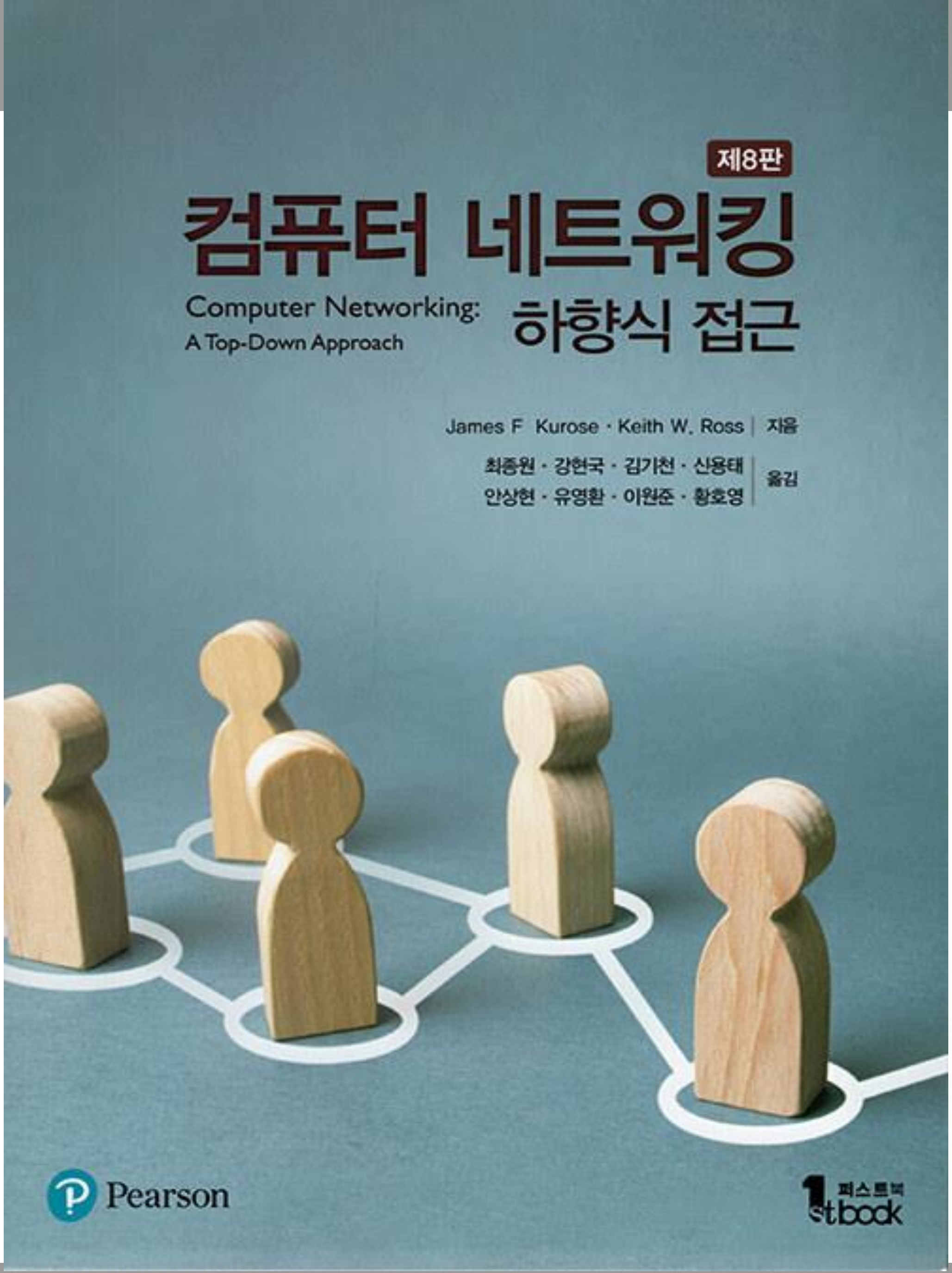
- Lecture Notes
  - Will be posted on the class website **after** the corresponding class
  - Check the web page ("Announcements") periodically. It will be each student's responsibility to check unforeseenly updated and/or changed schedule regarding make-up classes, exam date, etc.
  - ***To encourage your study priority, a full set of lecture notes will not be posted → getting behind in your reading/writing will affect every aspect of your learning efficiency***

Miscellaneous

- 재강조: 출석 및 참여도, 수업태도 등은 최종학점에 중요하게 반영됨

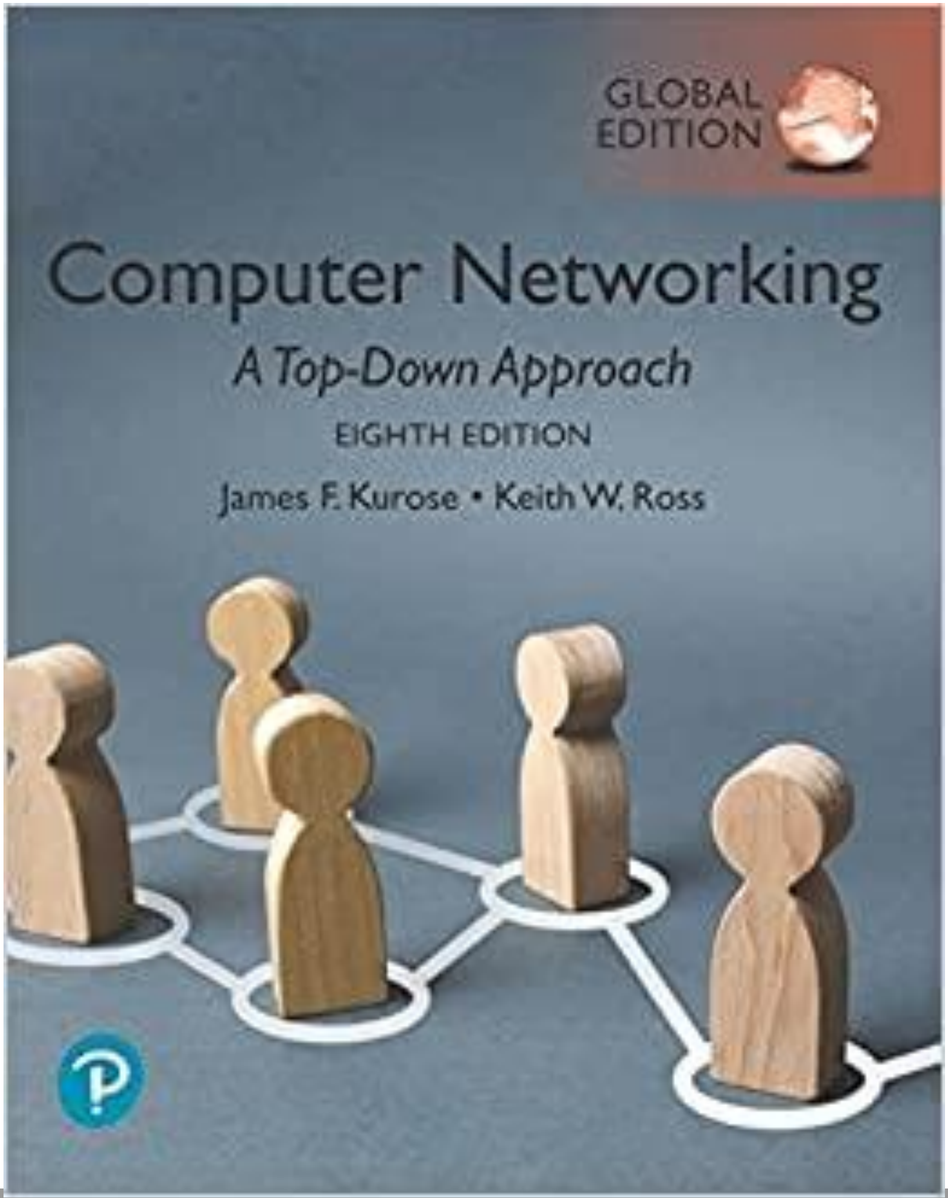
Course Material

- http://www.kyobobook.co.kr/product/detailViewKor.laf?mallGb=KOR&ejkGb=KOR&barcode=9789813350212


제8판
컴퓨터 네트워킹
Computer Networking: A Top-Down Approach
하향식 접근
James F. Kurose · Keith W. Ross | 지음
최종원 · 강현국 · 김기천 · 신용태
안상현 · 유영환 · 이원준 · 황호영 | 옮김
Pearson
퍼스트북 1st book

Computer Networking [Global Edition] 8th Edition

- by James Kurose (Author), Keith Ross (Author)



주	학습내용	교재	활동 및 설계내용
1	Introduction to layered network architectures		
2	Introduction to layered network architectures		
3	Network terminology, protocols		
4	Network performance issues		
5	Application layer overview		중간고사 1 (TBD)
6	Application layer protocols: HTTP, DNS		
7	Network programming (Socket programming fundamentals)		
8	Transport layer overview		학교 중간고사 기간
9	Transport layer reliable data transfer (rdf)		
10	TCP/UDP and congestion control		
11	Network layer overview		중간고사 2 (5/20 월; NOT finalized)
12	Network layer protocols		
13	IPv4, IPv6, QoS		
14	Internet routing algorithms		
15	Internet routing algorithms: LS and DV		
16	Course wrap-up		기말고사 (6/12 수)

사국 박사과정

이인섭(3기)

이동근(7기)

윤승민(7기)

UniQGAN: Towards Improved Modulation Classification with Adversarial Robustness Using Scalable Generator Design, IEEE Trans. On Dependable and Secure Computing (TDSC), 2023

UniQGAN: Towards Improved Modulation Classification with Adversarial Robustness Using Scalable Generator Design

Insup Lee, *Student Member, IEEE*, and Wonjun Lee, *Fellow, IEEE*

Abstract—Automatic modulation classification (AMC) has been envisioned as a significant element for security issues at the physical layer due to its indispensable role in accurate communications. Recent attention to deep learning has impacted the AMC, which exhibits exceptional performance without manual feature engineering. To guarantee the accuracy and robustness of deep learning-based AMC, data augmentation is a critical issue. While existing studies have used several deep generative models to handle the data insufficiency, these studies face three challenges including low scalability, lengthy training time, and limited accuracy improvement. To this end, this paper presents UniQGAN, a novel unified generative architecture that models I/Q constellation diagrams from various signal-to-noise ratios (SNRs) using a single model. The proposed method enables the generation of high-quality data with a scalable generator, while requiring reduced training time. At the core of UniQGAN are *multi-conditions embedding* and *multi-domains classification* techniques that leverage both SNR and modulation type during the optimization process to enable unified modeling. Using abundant high-quality training data, UniQGAN accelerates the enhanced AMC with high performance and adversarial robustness. Experimental results demonstrate that the data generation by UniQGAN achieves superiority in terms of scalability, training time, and accuracy.

Index Terms—Automatic modulation classification, data augmentation, adversarial robustness, deep learning, GAN

1 Introduction

Automatic modulation classification (AMC) enables legitimate communications by synchronizing modulation schemes between a transmitter and a receiver. It makes AMC essential in ensuring accurate communications and further communication security [2]. Although AMC has started to draw attention in the military domain (e.g., electronic warfare), AMC is also adopted in civilian scenar-
ios ysical layer
autl Specifically,
sinc evices com-
plic ey roles in
spe ntication to
det AMC as a
star yer threats.
Cor likelihood-
bas . However,
the nputational
con heads from
feat

ering issue
is ed to be a
key whose most
dist nunications
ena numerous
rela C [8], [10],

[11], [12], [13], [14]. Unlike the earlier AMC methods that relied on feature-based or likelihood-based approaches, deep learning-based AMC automatically extracts hidden features from received signals without manual feature engineering. There have been many examples for AMC using Recurrent Neural Network (RNN) [10], Long Short Term Memory (LSTM) [11], and Convolutional Neural Network (CNN) [8], [12], [13], [14]. RNN and LSTM perform well on I/Q signals due to their superior ability to process time-series signals. Especially, CNN shows excellent accuracy even with speed improvements [15] on I/Q constellation diagrams, which are typical image data that represent signals. In this paper, we focus on the case that employs the CNN-based AMC for classifying the I/Q diagrams.

The most critical factor affecting classification performance is availability of sufficient high-quality training data. Note that abundant training data is required also for robustness against adversarial attacks [16]. Neural networks are inherently vulnerable to adversarial examples; even a minor perturbation can cause misclassification [17], which motivates studies on adversarial attacks for deep learning-based AMC [18], [19], [20]. Since deep learning-based AMC has deployed in various fields, it would pose fatal impacts if the dependability of the deep learning-based AMC violated. As shown in Fig.1, if adversarial attacks occurred on deep learning-based AMC, the attacks would deteriorate diverse

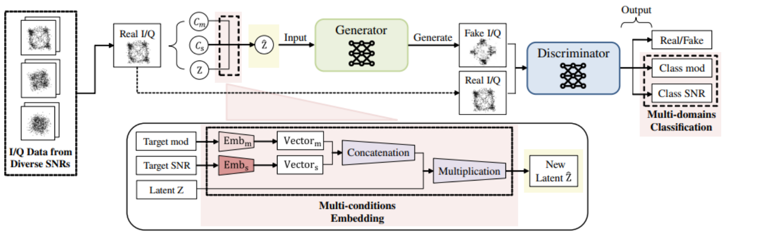


Fig. 6. UniQGAN Architecture. Its key components consist of *multi-conditions embedding* and *multi-domains classification*. In multi-conditions embedding, after concatenating the independently embedded vectors Vector_m and Vector_s, we multiply them with the latent $\mathbb{Z}$ to create a new latent $\hat{\mathbb{Z}}$. Then, we extend the capability of ACGAN's auxiliary classifier to two domains (modulation type and SNR) in multi-domains classification. As a result, both conditions c_m and c_s are successfully reflected in the optimization process of UniQGAN, allowing for the scalable architecture to be trained using a single model over diverse SNRs.

the trained generator can produce constellation diagrams for a given SNR. To prepare the diagrams at various SNRs, it is necessary to train and manage generators as many as the number of SNRs, which sparks our research.

5 UniQGAN Design

We propose UniQGAN, a scalable GAN design to generate constellation diagrams at various SNRs with a single generator. This section discusses design objectives, suggested

In addition, we quantify the changes in AMC accuracy caused by data augmentation and reflect them in determining UniQGAN's weights (Section 5.3).

5.2 UniQGAN Architecture

As illustrated in Fig.5, the architecture of UniQGAN deviates from ACGAN in that the generator and discriminator consider modulation type and SNR simultaneously. In this section, we describe the main parts of UniQGAN and several techniques to achieve faster convergence with reduced

TABLE 2
Accuracy on RadioML2018.01a Benchmark Augmented by Different GANs

Augmentation Method	SNR (dB)							Low SNRs (-2∼4)	All SNRs (-2∼10)
	-2	0	2	4	6	8	10	Average	Average
Original (No augmentation)	0.234	0.325	0.555	0.841	0.956	0.976	0.985	0.489	0.696
cGAN	0.253	0.336	0.530	0.824	0.946	0.966	0.976	0.486	0.690
ACGAN	0.250	0.340	0.518	0.847	0.950	0.970	0.978	0.489	0.693
UniQGAN* (One-hot encoding)	0.267	**0.352**	0.573	0.851	0.958	0.976	0.988	0.511	0.709
UniQGAN (Multi-conditions embedding)	**0.269**	0.349	**0.592**	**0.866**	**0.961**	**0.983**	**0.989**	**0.519**	**0.716**

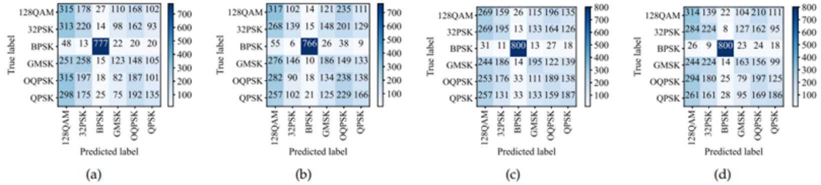


Fig. 8. Confusion matrix of 0 dB for (a) Original, (b) cGAN, (c) ACGAN, and (d) UniQGAN.

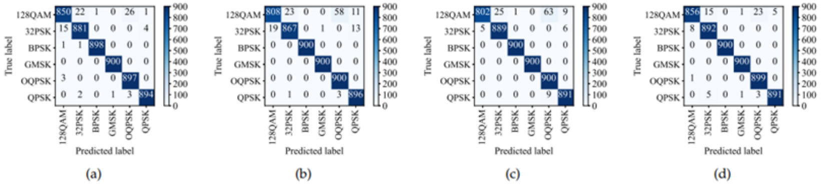


Fig. 9. Confusion matrix of 10 dB for (a) Original, (b) cGAN, (c) ACGAN, and (d) UniQGAN.

Net-track: Generic Web Tracking Detection Using Packet Metadata, WWW (Web Conf.) 2023, May, 2023, Austin, USA

THE WEB CONFERENCE ACM

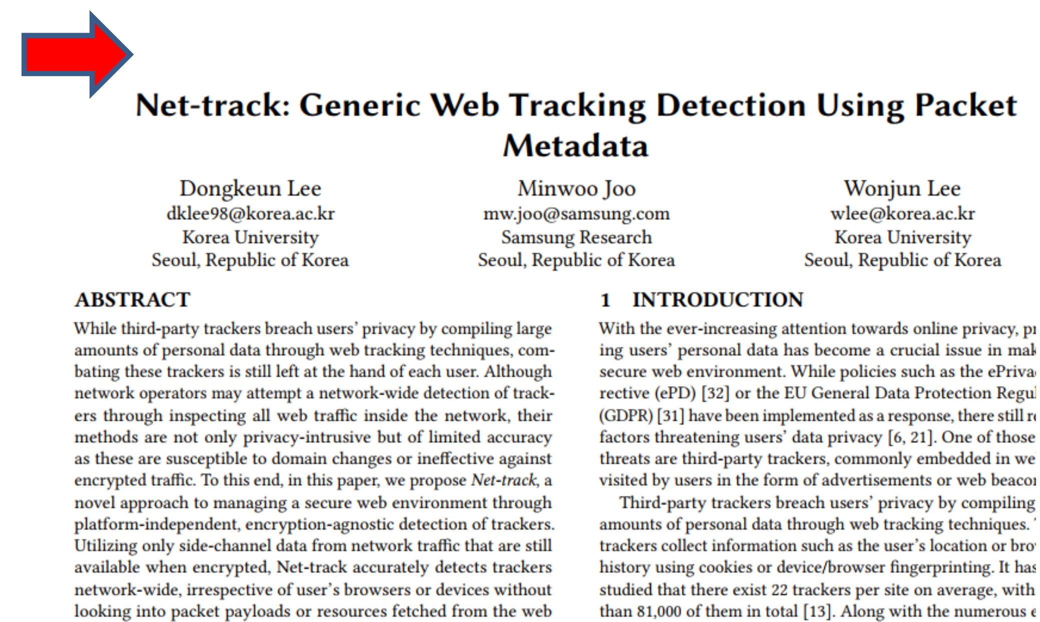
Calls▾ Special Days▾ Satellite Events▾ Program▾ Attendees▾ Important Dates About▾

WELCOME TO THE WEB CONFERENCE 2023 IN AUSTIN, TEXAS, USA

APRIL 30 - MAY 4, 2023

AT&T Hotel and Conference Center at The University of Texas at Austin

REGISTRATION



Net-track: Generic Web Tracking Detection Using Packet Metadata

Dongkeun Lee
dklee98@korea.ac.kr
Korea University
Seoul, Republic of Korea

Minwoo Joo
mw.joo@samsung.com
Samsung Research
Seoul, Republic of Korea

Wonjun Lee
wlee@korea.ac.kr
Korea University
Seoul, Republic of Korea

ABSTRACT

While third-party trackers breach users' privacy by compiling large amounts of personal data through web tracking techniques, combating these trackers is still left at the hand of each user. Although network operators may attempt a network-wide detection of trackers through inspecting all web traffic inside the network, their methods are not only privacy-intrusive but of limited accuracy as these are susceptible to domain changes or ineffective against encrypted traffic. To this end, in this paper, we propose *Net-track*, a novel approach to managing a secure web environment through platform-independent, encryption-agnostic detection of trackers. Utilizing only side-channel data from network traffic that are still available when encrypted, Net-track accurately detects trackers network-wide, irrespective of user's browsers or devices without looking into packet payloads or resources fetched from the web

1 INTRODUCTION

With the ever-increasing attention towards online privacy, pr
ing users' personal data has become a crucial issue in mak
secure web environment. While policies such as the ePriva
rective (ePD) [32] or the EU General Data Protection Regul
(GDPR) [31] have been implemented as a response, there still r
factors threatening users' data privacy [6, 21]. One of those
threats are third-party trackers, commonly embedded in we
visited by users in the form of advertisements or web beaco

Third-party trackers breach users' privacy by compiling
amounts of personal data through web tracking techniques.
trackers collect information such as the user's location or bro
history using cookies or device/browser fingerprinting. It has
studied that there exist 22 trackers per site on average, with
than 81,000 of them in total [13]. Along with the numerous e

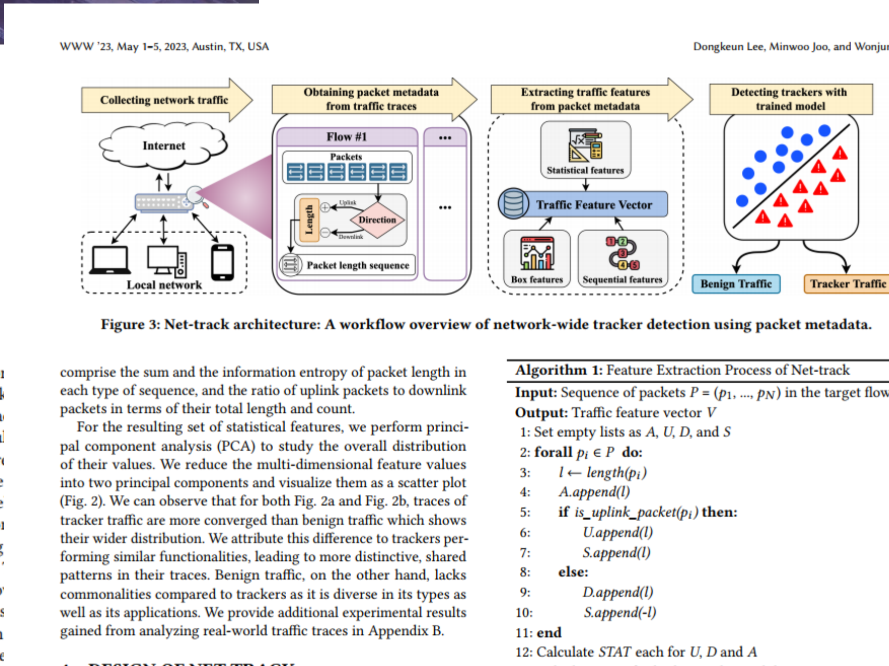


Figure 3: Net-track architecture: A workflow overview of network-wide tracker detection using packet metadata.

comprise the sum and the information entropy of packet length in each type of sequence, and the ratio of uplink packets to downlink packets in terms of their total length and count.

For the resulting set of statistical features, we perform principal component analysis (PCA) to study the overall distribution of their values. We reduce the multi-dimensional feature values into two principal components and visualize them as a scatter plot (Fig. 2). We can observe that for both Fig. 2a and Fig. 2b, traces of tracker traffic are more converged than benign traffic which shows their wider distribution. We attribute this difference to trackers performing similar functionalities, leading to more distinctive, shared patterns in their traces. Benign traffic, on the other hand, lacks commonalities compared to trackers as it is diverse in its types as well as its applications. We provide additional experimental results gained from analyzing real-world traffic traces in Appendix B.

Algorithm 1: Feature Extraction Process of Net-track

```
Input: Sequence of packets $P = (p_1, ..., p_N)$ in the target flow
Output: Traffic feature vector $V$
Set empty lists as $A$, $U$, $D$, and $S$
forall $p_i \in P$ do:
    $l \leftarrow length(p_i)$
    $A.append(l)$
    if $is\_uplink\_packet(p_i)$ then:
        $U.append(l)$
        $S.append(l)$
    else:
        $D.append(l)$
        $S.append(-l)$
end
Calculate $STAT$ each for $U$, $D$ and $A$
```

Computer Networks
컴퓨터네트워크

(Ch 1. Introduction)

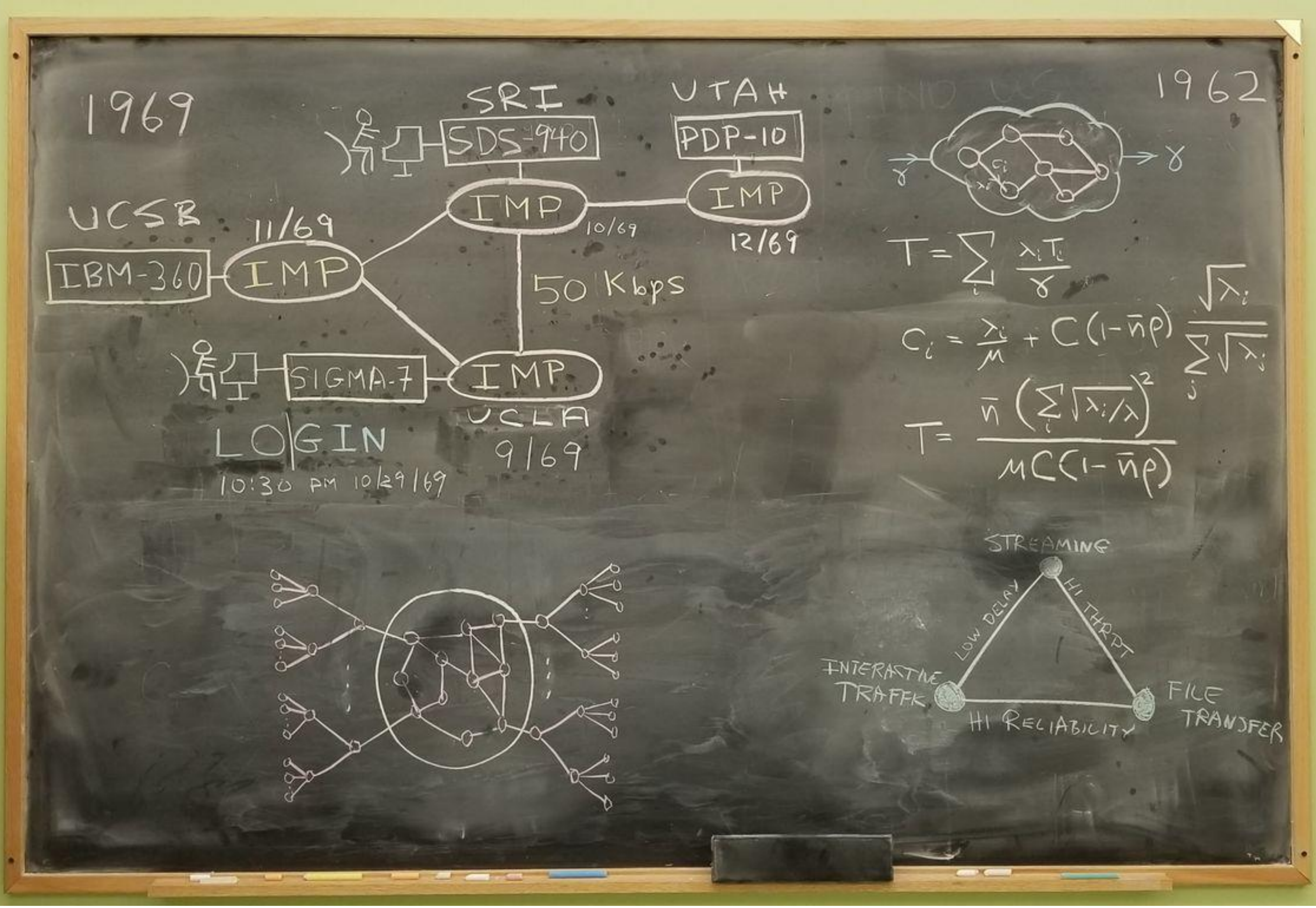
Wonjun Lee, Ph.D., IEEE Fellow

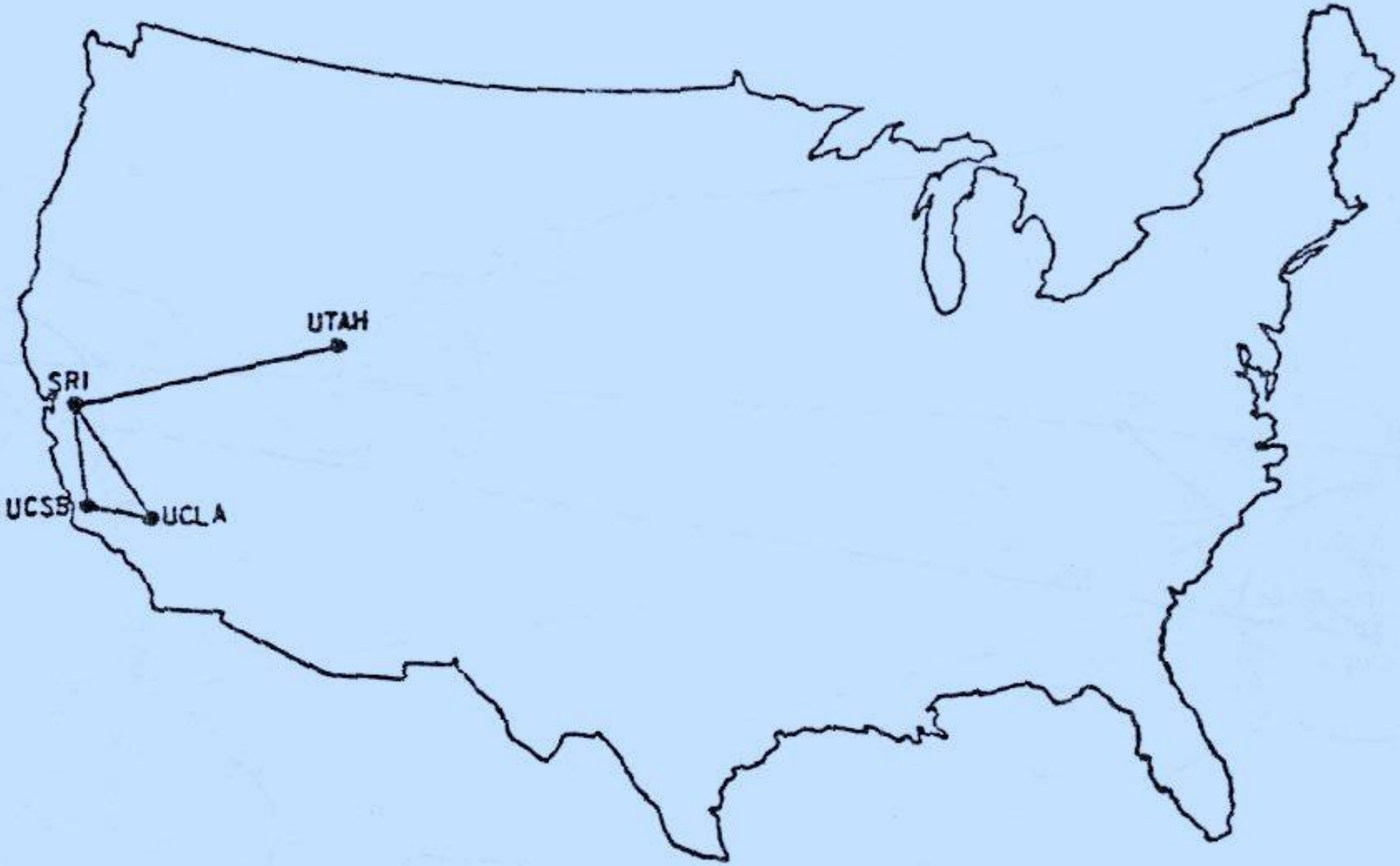
Network and Security Research Lab. (NetLab)

http://netlab.korea.ac.kr

http://mobile.korea.ac.kr

Korea University


1969
SRI
SDS-940
UTAH
PDP-10
IMP
IMP
10/69
12/69
UCSB
11/69
IBM-360
IMP
50 Kbps
SIGMA-7
IMP
UCLA
9/69
LOGIN
10:30 PM 10/29/69
1962
γ
C_i
γ
$T = \sum_i \frac{\lambda_i T_i}{\gamma}$
$C_i = \frac{\lambda_i}{\mu} + C(1-\bar{n}\rho)\frac{\sqrt{\lambda_i}}{\sum_j \sqrt{\lambda_j}}$
$T = \frac{\bar{n}\left(\sum_i \sqrt{\lambda_i/\lambda}\right)^2}{\mu C(1-\bar{n}\rho)}$
STREAMING
LOW DELAY
HI THRPT
INTERACTIVE TRAFFIC
FILE TRANSFER
HI RELIABILITY



The ARPANET in December 1969