
TECHNICAL REPORT

Editors
Shlomi Dolev and Oded Margalit

Technical Report #20-01

July 12, 2020

The BGU-Negev Hi-Tech Faculty Startup Accelerator,
Department of Computer Science,
Ben-Gurion University, Beer Sheva, Israel
2020 INTERNATIONAL SYMPOSIUM ON CYBER SECURITY CRYPTOGRAPHY AND MACHINE LEARNING

JULY 2-3, 2020
BEN-GURION UNIVERSITY
ALON BUILDING FOR HI-TECH

PROF. SHLOMI DOLEV
DR. SACHIN LODHA
GENERAL CHAIRS
# Table of Contents

PhD Student Research Track .................................................................................................................. 1

Introduction .......................................................................................................................................... 2

Policy Pruning and Shrinking Algorithm for Deep Reinforcement Learning ........................................... 3  
*Dor Livne, Kobi Cohen*

Solving Network Security Problems Using Autonomous Systems Embedding ........................................ 7  
*Tal Shapira*

Machine Learning by Actigraph Data for Detection of Postpartum Depression ........................................ 27  
*Roy Hershinfkel, Alexander Binun, Julie Cwikel, Shlomi Dolev*

Prioritized Multi-Criteria k-Shortest Path Problem ................................................................................. 35  
*Manish Kumar, Shlomi Dolev*

Toward Provable One-Way Functions .................................................................................................... 47  
*Hagar Dolev, Shlomi Dolev*

Video synthesis of an exemplary patient exercise as part of a physiotherapeutic treatment .................... 51  
*Itai Dror, Ofer Hadar*
Entrepreneurship Pitch Track

Introduction

FertilEyesTM Algorithm and IoT nitrate sensor to optimize agriculture yields and protect the environment.  
-Shlomi Arnon

AntisepTech Empowering the People – Preventing infections.  
-Barak Katz

-Ziyu Wang

Drones' Cryptanalysis - Detecting Spying Drones.  
-Ben Nassi, Adi Shamir and Yuval Elovici

Leveraging deep learning to automate device connectivity to any platform.  
-Enis Abo Alhasan and Othman Alshekh

Body movement tagging engine.  
-Yoram Segal and Ofer Hadar

Stick ‘n Grip: A revolutionary robot gripper for the e-commerce industry.  
-Amir Shapiro
PhD Student Research Track

Chair: Oded Margalit
Conferences are one of the best ways to get to know the state-of-the-art status of a research area. The PhD session of CSCML 2020 was an intimate (7 presentations) group of researchers that talked about their work. I loved to see the variety of topic: from basic computer science research like k-Shortest path, via detecting malicious power-shell code, to postpartum depression.

The COVID-19 pandemic which made the whole CSCML conference virtual, didn't hurt the PhD session too much – we still enjoyed an interesting discussion.

I hope we'll have the conference face-2-face next year, but in any case, I strongly recommend all researchers in Cyber-Security, Machine Learning and Cryptology to submit their work (if relevant) and participate in the PhD track next year – it is a great way to learn about other’s work and receive feedback on your own.

Looking forward to CSCML 2021.

Regards,

Prof. Oded Margalit,

Computer Science department BGU

and Security Innovation Center Citi
Policy Pruning and Shrinking Algorithm for Deep Reinforcement Learning

Dor Livne and Kobi Cohen
Ben-Gurion University of the Negev, Beer Sheva 8410501 Israel
dorliv@bgu.ac.il, yakovsec@bgu.ac.il

Abstract
The recent success of deep neural networks (DNNs) for function approximation in reinforcement learning has triggered the development of Deep Reinforcement Learning (DRL) algorithms in various fields, such as robotics, computer games, natural language processing, computer vision, sensing systems, and wireless networking. Unfortunately, DNNs suffer from high computational cost and memory consumption, which limits the use of DRL algorithms in systems with limited hardware resources. In recent years, pruning algorithms have demonstrated considerable success in reducing the redundancy of DNNs in classification tasks. However, existing algorithms suffer from a significant performance reduction problem of pruning in the DRL domain, and establish a working algorithm, named Policy Pruning and Shrinking (PoPS), to train DRL models with strong performance while achieving a compact representation of the DNN. The framework is based on a novel iterative policy pruning and shrinking method that leverages the power of transfer learning when training the DRL model. Strong performance is demonstrated using the popular Mountain Car environment.\footnote{The full version of the paper was accepted for publication in the IEEE Journal of Selected Topics in Signal Processing [1]. In this conference version we present new experimental evaluations}.

Student Paper
Policy Pruning and Shrinking Algorithm for Deep Reinforcement Learning

Dor Livne and Kobi Cohen
Ben-Gurion University of the Negev, Beer Sheva 8410501 Israel
dorliv@bgu.ac.il, yakovsee@bgu.ac.il

Abstract

The recent success of deep neural networks (DNNs) for function approximation in reinforcement learning has triggered the development of Deep Reinforcement Learning (DRL) algorithms in various fields, such as robotics, computer games, natural language processing, computer vision, sensing systems, and wireless networking. Unfortunately, DNNs suffer from high computational cost and memory consumption, which limits the use of DRL algorithms in systems with limited hardware resources. In recent years, pruning algorithms have demonstrated considerable success in reducing the redundancy of DNNs in classification tasks. However, existing algorithms suffer from a significant performance reduction in the DRL domain. In this paper, we present the first effective solution to the performance reduction problem of pruning in the DRL domain, and establish a working algorithm, named Policy Pruning and Shrinking (PoPS), to train DRL models with strong performance while achieving a compact representation of the DNN. The framework is based on a novel iterative policy pruning and shrinking method that leverages the power of transfer learning when training the DRL model. Strong performance is demonstrated using the popular Mountain Car environment.

keywords—Deep reinforcement learning, deep neural network, pruning algorithms.

I. INTRODUCTION

The superior performance of DRL algorithms in decision making tasks [2] has triggered the need to make them practically appealing when using cheap hardware devices. For example, industrialization of artificially intelligent engines in controlled manufacturing processes often requires small and cheap sensing devices to detect and respond to events. Another example is automatizing users in wireless communication and Internet of Things (IoT) systems which often consist of low power, computationally limited and battery constrained nodes.

This issue has been recognized by the industry, and there are more and more players in the market that develop chips for low-power devices that support computationally intensive deep learning algorithms with low-power consumption. Prominent examples are Qualcomm Artificial Intelligence Engine, Intel’s EyeQ family of system-on-chip (SoC) devices, Intel’s Myriad 2 family, NXP’s ADAS chip, and more. Along with these industrial developments, establishing fundamental algorithmic methods to reduce the size of DRL models is crucial for making them practically appealing for a wide range of applications that use systems with limited hardware resources. This challenge has triggered a new and fascinating research direction: How to train DRL models with strong performance while achieving compact representations of the DNNs? In this paper we address this issue. In the DRL domain, the goal of an agent is to learn a policy, which is a mapping from a state to an action. Thus, the objective value at each state-action pair is not given as in supervised learning but need to be learned online by exploring actions. Therefore, the agent faces the well-known exploration versus exploitation dilemma. On the one hand, the agent should explore all actions in order to figure out their influence on the objective function. On the other hand, it should exploit the information gathered so far to choose the best actions. Existing pruning techniques do not operate well in the DRL domain since the ground truth is not given. Therefore, they must explore the state space in order to recuperate from the pruning procedure by interacting with the environment. This leads to a significant instability in the pruning procedure and increases the performance loss. As a result, when implementing pruning in the DRL domain, our algorithm must guard against losing a significant information regarding the optimal policy. Once the algorithm has this ability, it can detect redundancy in the DRL model, and train a regenerated shrunk dense model with strong performance.

II. RELATED WORK

The recent success of DRL algorithms has triggered the need to make them practically appealing when using cheap hardware devices. This is particularly relevant for DRL algorithms in sensing and inference systems (see [3], [7]–[9] and references therein), IoT, and wireless communication networks [10]–[12], that often require to operate using low power, computationally...
limited and battery constrained devices. DNNs are typically over-parameterized, i.e., there is a significant redundancy in deep learning models [13]. This redundancy leads to a waste of both computation and memory usage, which limits their use in resource-constrained devices. Therefore, in recent years, various methods have been developed to find efficient compact representations of DNNs. In [4], the authors developed a pruning method followed by vector quantization and Huffman coding [14] to compress neural networks. Other pruning methods for supervised learning tasks can be found in [20]–[22].

Pruning methods for supervised learning tasks can be found in [20]–[22]. In this paper, we first develop the method for pruning DRL models.

III. SYSTEM MODEL AND PROBLEM STATEMENT

Consider a system consisting of an agent who interacts with an environment. Let \( S \) be the state space that the system can reach, and \( s_t \in S \) be the system state at time \( t \). Let \( A \) be the action space that the agent can take. At each time (say \( t \)), the agent takes action \( a_t \in A \), receives reward \( r_{t+1} \), and the system transits to state \( s_{t+1} \), which is observed (or partially observed) by the agent. Let

\[
R = \sum_{t=1}^{T} \gamma^{t-1} r_t
\]

be the accumulated discounted reward, where \( 0 \leq \gamma \leq 1 \) is a discount factor, and \( T \) is the time horizon of the control problem. The agent’s objective is to find a policy \( \pi : S \rightarrow A \) that maximizes the expected accumulated discounted reward:

\[
\max_{\pi} \mathbb{E}[R(\pi)]
\]

where \( \mathbb{E}[R(\pi)] \) denotes the expected accumulated discounted reward when the model performs policy \( \pi \). Q-learning uses a DNN (referred to as Deep Q-network or DQN) to map from the observed state to a Q-value for each action. The action that maximizes the Q-value is selected (according to \( \epsilon \)-greedy distribution). Denote the DQN network by \( Q \). Then, the updates to the Q-values satisfy the following equation:

\[
Q_{t+1}(s_t, a_t) = Q_t(s_t, a_t) + \alpha \left[ r_{t+1} + \gamma \max_{a_{t+1}} Q_t(s_{t+1}, a_{t+1}) - Q_t(s_t, a_t) \right]
\]

where the subscript \( t \) denotes the time index, and

\[
r_{t+1} + \gamma \max_{a_{t+1}} Q_t(s_{t+1}, a_{t+1})
\]

is the learned value obtained by getting reward \( r_{t+1} \) after taking action \( a_t \) in state \( s_t \), moving to the next state \( s_{t+1} \), and then taking action \( a_{t+1} \) that maximizes the future Q-value seen at the next state. Our goal is to develop a fundamental method to train DRL models with strong performance in terms of solving (2) while achieving compact representations of the DNNs.

IV. ALGORITHM DESCRIPTION AND EXPERIMENTAL EVALUATIONS

We now present the Policy Pruning and Shrinking (PoPS) algorithm to train DRL models with strong performance while achieving a compact representation of the DNN. PoPS executes an iterative procedure using three main steps to achieve this goal. In the first step, PoPS leverages the power of transfer learning to capture the full information regarding the desired policy. Specifically, PoPS trains a teacher network using a large-scale DRL model to yield a policy that maximizes the objective function without pruning. In the second step, PoPS executes a novel transfer learning-based policy pruning procedure, which is controlled by the teacher, to find an efficient pruned representation of the model. The policy pruning step avoids the direct interaction with the environment when implementing pruning in the DRL domain. Since the teacher that controls the pruning process has already explored and exploited actions successfully, the fine-tuning step has the ability to remove redundancy iteratively without the need of exploring actions which are less likely to contribute significantly to the objective function. In the third step, namely the policy shrinking step, PoPS regenerates and trains a newly-constructed smaller dense model based on the redundancy measured by the policy pruning procedure. The policy pruning and policy shrinking steps are repeated until the algorithm can no longer detect any redundancy. For a detailed description of the algorithm see [1]. We used the Mountain car environment from the gym library [5] to evaluate the performance. The objective is to drive the car to the top of the hill (as illustrated in Fig. 1). For this, the DRL agent must learn to drive backwards to have enough momentum to climb to the top of the hill. The state space contains the velocity and position of the car. At each time step, the agent can push the car backwards or forward. The agent gets a reward of -1 for each time step spent not at the top of the hill. The episode ends when the car reaches the top of the hill or after 200 time steps. A policy that solves the environment is a policy that achieves more than -110 points in average over 100 episodes. The DRL architecture that was used in this experiment was a DQN with 3 feed-forward fully connected layers with 256, 256, and 128 neurons, respectively, summing up to a total of roughly 100K parameters. We present the performance of PoPS algorithm in Table I. PoPS generated a compact representation of the DRL model that solves the environment with a size of less than 0.3% of the initial DQN representation size, which significantly outperformed existing algorithms, namely, Magnitude-Base Gradual Pruning (MBGP) [4] and Knowledge Distillation-Based Pruning (KDBP) [6] as presented in Table II.
Fig. 1. An illustration of the Mountain car environment.

<table>
<thead>
<tr>
<th>Iteration</th>
<th># non-zero parameters (percentage of initial size)</th>
<th>Average score</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>100K (100%)</td>
<td>&gt; -110</td>
</tr>
<tr>
<td>1</td>
<td>8K (8%)</td>
<td>&gt; -110</td>
</tr>
<tr>
<td>2</td>
<td>5.9K (5.9%)</td>
<td>&gt; -110</td>
</tr>
<tr>
<td>3</td>
<td>4.1K (4.15%)</td>
<td>&gt; -110</td>
</tr>
<tr>
<td>4</td>
<td>2.3K (2.2%)</td>
<td>&gt; -110</td>
</tr>
<tr>
<td>5</td>
<td>1K (11%)</td>
<td>&gt; -110</td>
</tr>
<tr>
<td>6</td>
<td>529 (0.53%)</td>
<td>&gt; -110</td>
</tr>
<tr>
<td>7 (output)</td>
<td>279 (0.28%)</td>
<td>-104.74</td>
</tr>
</tbody>
</table>

### TABLE II

<table>
<thead>
<tr>
<th># non-zero parameters (percentage of initial size)</th>
<th>Average score under MBGP</th>
<th>Average score under KDBP</th>
</tr>
</thead>
<tbody>
<tr>
<td>100K (100%)</td>
<td>&gt; -110</td>
<td>&gt; -110</td>
</tr>
<tr>
<td>60K (60%)</td>
<td>&gt; -110</td>
<td>&gt; -110</td>
</tr>
<tr>
<td>50K (50%)</td>
<td>&gt; -110</td>
<td>&gt; -110</td>
</tr>
<tr>
<td>40K (40%)</td>
<td>&gt; -110</td>
<td>&gt; -110</td>
</tr>
<tr>
<td>30K (30%)</td>
<td>&gt; -110</td>
<td>&gt; -110</td>
</tr>
<tr>
<td>20K (20%)</td>
<td>&gt; -110</td>
<td>&gt; -110</td>
</tr>
<tr>
<td>10K (10%)</td>
<td>-125</td>
<td>-116</td>
</tr>
<tr>
<td>2.5K (2.5%)</td>
<td>&lt; -190</td>
<td>-170</td>
</tr>
<tr>
<td>2.1K (2.1%)</td>
<td>&lt; -190</td>
<td>&lt; -190</td>
</tr>
</tbody>
</table>

### REFERENCES


Solving Network Security Problems Using Autonomous Systems Embedding

School of Electrical Engineering

TAL SHAPIRA, PH.D CANDIDATE
UNDER THE SUPERVISION OF PROF. YUVAL SHAVITT
Outline

- Introduction
- ToR Classification
- IP Hijack
- Motivation
- Datasets
- Method
  - BGP2VEC
  - Classification
- Experiments and Results
- Summary
Autonomous System (AS): a collection of physical networks glued together using IP, have a unified administrative routing policy, and has been assigned a number (ASN - 32 bits).

- ISP Internal networks: Verizon – 701, 702, 703 …, Leve3: 3356, 3549 …
- Campus networks: University of Delaware – 2, MIT - 3
- Corporate networks: Intel - 4983
- Content provider: Google - 15169, 16591 …, Facebook - 32934, 63293 …

Border Gateway Protocol (BGP) coordinates the Inter-AS routing in the Internet

- BGP routing's update messages list the entire AS path to reach an IP address prefix (AP)
The commercial agreements between two connected ASes are broadly classified into three types of relationship (ToR):

- **Provider-to-customer (P2C)** - the customer AS pays the provider AS for transit traffic from and to the rest of the Internet.
- **Peer-to-peer (P2P)** - two ASes freely exchange traffic between themselves and their customers, but do not exchange traffic from or to their providers or other peers, and
- **Siblings (S2S)** - two ASes that belong to the same administrative domain
  - Ex: Verizon – 701, 702
Prefix hijacking in a nutshell - another AS originates the prefix

More than 40% of the network operators reported that their organization had been a victim of a hijack in the past

What’s to stop someone else?

- BGP does not verify that the AS is authorized
- Registries of prefix ownership are inaccurate

How to?

- Sub-prefix hijack (e.g. 1.1.1.1/22 instead of 1.1.1.1/24)
- Path shortening (BGP chooses path based on cost and length)
- Add a legitimate AS at the end of the path (and therefore it’s hard to tell that the AS path is bogus)
Why ToR Classification?

- The Internet topology alone does not imply reachability among ASs.

- Use cases
  - Routing management and engineering
    - Inference the possible routes selected by BGP in case of a link failure
  - Routing security
    - IP hijack detection (e.g. based on the ‘Valley-Free’ routing)

- ToR information is mostly not public
  - The commercial agreements between two connected ASes are usually classified

---

1. [Dolev et al. 2006] “Internet Resiliency to Attacks and Failures Under BGP Policy Routing”
2. [Gao 2001] “On inferring autonomous system relationships in the Internet”
ToR Classification - Previous Approaches

- Algorithms based on:
  - Routing data:
    - RouteViews BGP announcements (RV)
    - AS level Routes generations from traceroutes (DIMES)
  - Routing Policies - IRR (Internet Routing Registry)
  - BGP communities (an attribute in update messages)

- Heuristic assumptions based on graph characteristics:
  - AS degree
  - VF paths maximization problem
  - Reachability or customer cone
  - Based on the core existence assumption
  - Based on K-shell

1. [Giotsas et al. 2013] “Inferring multilateral peering” (IXP)
2. [Gao 2001] “On inferring autonomous system relationships in the Internet” (Gao)
3. [Subramanian et al. 2002] “Characterizing the Internet hierarchy from multiple vantage points” (SARK)
4. [Dimitropoulos et al. 2007] “AS Relationships: Inference and Validation” (CAIDA 07)
5. [Shavitt et al. 2009] “Near-Deterministic Inference of AS Relationships” (ND-ToR)
6. [Luckie et al. 2013] “AS relationships, customer cones, and validation” (CAIDA 13, AS-Rank)
IP Hijack Detection - Previous Approaches

- Prevention solutions (or reactive solutions):
  - Based on cryptographic authentications – RPKI¹ and BGPsec²
  - Operators are reluctant to deploy them due to technical and financial costs

- Detection solutions - based on the type of information:
  - Control-plane approaches³ (passive solutions) – based on a distributed set of BGP monitors and route collectors
  - Data-plane approaches⁴ - only relies on real-time data plane information that is obtained from multiple sensors that deploy active probing (pings/traceroutes)
  - Hybrid approaches⁵

- Most of the previous detection solutions rely on:
  - Features engineering + ML algorithm⁶
  - Heuristic assumptions (e.g. VF)

3. [Sermpezis et al. 2018] “ARTEMIS: Neutralizing BGP Hijacking within a Minute”
‘Valley Free’ Routing

Routing rules:
- Provider accepts everything
- Peer only if it is for its customers

Path Properties:
- Up then down
- No up-down-up, at most 1 P2P step

[Gao 2001] “On inferring autonomous system relationships in the Internet”
Motivation

- Using an **assumption-free** method for **ToR classification and IP hijack Detection**:
  - An inherent problem of the existing algorithms is their use of heuristics assumptions, causing unbounded errors that are spread over all inferred relationships
  - There are complex cases, such as non-valley-free routing
- Our method is based **only on** BGP announcements (or AS-level routes)
- We introduce the first end-to-end **deep learning** approach
- Our goal is to use a **generic approach** based on ASN embedding
  - We aim to learn the dense representations of ASNs from BGP routes
  - Apply machine/deep learning techniques based on the representations
Datasets

- Route Views\(^1\) BGP announcements (RV)
  - 3,600,000 BGP paths
  - 62,525 Ases
  - 113,400 undirected AS links
- CAIDA AS Relationships Dataset\(^2\)
  - Serial 1 - based on AS-Rank\(^3\)
  - Serial 2 - additional 264,534 P2P, inferred from BGP communities\(^4\)
  - Not contains siblings – “an accurate S2S inference is almost impossible without using IRR databases”\(^5\)
- Labeled BGP routes:
  - consists of approximately 2,648,900 standard routes (‘GREEN’) and 47,800 hijacked routes (‘RED’)
  - The labeling was generated by combinations of VF algorithms\(^6\) and manual work

1. University of Oregon, Route Views Project, [http://www.routeviews.org](http://www.routeviews.org), March 2018
3. [Luckie et al. 2013] “AS relationships, customer cones, and validation” (CAIDA 13, AS-Rank)
4. [Giotsas et al. 2013] “Inferring multilateral peering” (IXP)
5. [Dimitropoulos et al. 2007] “AS Relationships: Inference and Validation” (CAIDA 07)

Table 1: Number of labeled ToRs in the dataset.

<table>
<thead>
<tr>
<th></th>
<th>CAIDA AS ToRs serial-2</th>
</tr>
</thead>
<tbody>
<tr>
<td>P2P</td>
<td>608,486</td>
</tr>
<tr>
<td>P2C</td>
<td>118,405</td>
</tr>
<tr>
<td>C2P</td>
<td>118,405</td>
</tr>
</tbody>
</table>
Method

- An end-to-end deep learning approach:
  - First stage – *BGP2Vec* – ASN Embedding
  - Second stage –
    - ASN/ToR classification using **Artificial Neural Networks**
    - IP hijack detection using **LSTM networks**
BGP2VEC – ASN Embedding

- Based on Word Embedding (Word2Vec¹), broadly used in NLP
- Embedding = represent discrete variables as continuous vectors
- An ASN is characterized by its context, i.e., neighboring ASNs
- \( V = 62,525, N = 32 \)

An example with \( V = 4 \):

\[
\begin{array}{c|cccc}
\text{index} & 2 & 0 & 0 & 1 & 0 \\
\text{one-hot vector} & 1 & 0 & 0 & 1 & 0 \\
\text{weight matrix} & 5.1 & -3 & 0.1 & 3.2 & 1.3 \\
\text{embedding} & -1 & 7.5 & -2 & 3.4 & 0.5 \\
\end{array}
\]

\[
\begin{array}{c|cccc}
\text{index} & 1.2 & 27 & 0.4 & -1 & 2.8 \\
\end{array}
\]

1. [Mikolov et al. 2013] “Distributed representations of words and phrases and their compositionality” (Word2Vec)
### Exploration of ASN Embedding

<table>
<thead>
<tr>
<th>Neighbour</th>
<th>ASN</th>
<th>Owner</th>
<th>Cosine Similarity</th>
<th>Degree</th>
<th>Distance from Tier-1</th>
<th>AS Class</th>
<th>Country</th>
<th>ToR</th>
<th>Grade</th>
</tr>
</thead>
<tbody>
<tr>
<td>-</td>
<td>3356</td>
<td>Level3</td>
<td>1</td>
<td>5635</td>
<td>0</td>
<td>NSP</td>
<td>USA</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>1st</td>
<td>3549</td>
<td>Level3</td>
<td>0.897</td>
<td>2334</td>
<td>0</td>
<td>NSP</td>
<td>USA</td>
<td>S2S</td>
<td>5</td>
</tr>
<tr>
<td>2nd</td>
<td>1299</td>
<td>Telia</td>
<td>0.850</td>
<td>1747</td>
<td>0</td>
<td>NSP</td>
<td>Sweden</td>
<td>P2P</td>
<td>4</td>
</tr>
<tr>
<td>3rd</td>
<td>701</td>
<td>Verizon</td>
<td>0.849</td>
<td>1216</td>
<td>0</td>
<td>NSP</td>
<td>USA</td>
<td>P2P</td>
<td>3</td>
</tr>
<tr>
<td>4th</td>
<td>286</td>
<td>KPN</td>
<td>0.844</td>
<td>267</td>
<td>0</td>
<td>NSP</td>
<td>Netherlands</td>
<td>P2P</td>
<td>2</td>
</tr>
<tr>
<td>5th</td>
<td>6071</td>
<td>Unisys</td>
<td>0.845</td>
<td>4</td>
<td>1</td>
<td>-</td>
<td>USA</td>
<td>P2C</td>
<td>0</td>
</tr>
</tbody>
</table>

(a) AS3356: Level3, Tier 1 and siblings similarity example; Total similarity grade: 14.

<table>
<thead>
<tr>
<th>Neighbour</th>
<th>ASN</th>
<th>Owner</th>
<th>Cosine Similarity</th>
<th>Degree</th>
<th>Distance from Tier-1</th>
<th>AS Class</th>
<th>Country</th>
<th>ToR</th>
<th>Grade</th>
</tr>
</thead>
<tbody>
<tr>
<td>-</td>
<td>378</td>
<td>MACHBA</td>
<td>1</td>
<td>4</td>
<td>2</td>
<td>Research</td>
<td>Israel</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>1st</td>
<td>3268</td>
<td>CyNet</td>
<td>0.929</td>
<td>3</td>
<td>2</td>
<td>Research</td>
<td>Cyprus</td>
<td>None</td>
<td>5</td>
</tr>
<tr>
<td>2nd</td>
<td>1930</td>
<td>FCT</td>
<td>0.927</td>
<td>10</td>
<td>2</td>
<td>Research</td>
<td>Portugal</td>
<td>None</td>
<td>4</td>
</tr>
<tr>
<td>3rd</td>
<td>40981</td>
<td>University of Montenegro</td>
<td>0.925</td>
<td>2</td>
<td>2</td>
<td>Research</td>
<td>Montenegro</td>
<td>None</td>
<td>3</td>
</tr>
<tr>
<td>4th</td>
<td>57961</td>
<td>RASH</td>
<td>0.911</td>
<td>3</td>
<td>2</td>
<td>Research</td>
<td>Albania</td>
<td>None</td>
<td>2</td>
</tr>
<tr>
<td>5th</td>
<td>199354</td>
<td>ASREN</td>
<td>0.901</td>
<td>4</td>
<td>2</td>
<td>Research</td>
<td>Jordan</td>
<td>None</td>
<td>1</td>
</tr>
</tbody>
</table>

(c) AS378: MACHBA - Israel Inter-University Computation Center, Educational/Research similarity example; Total similarity grade: 15.

<table>
<thead>
<tr>
<th>Neighbour</th>
<th>ASN</th>
<th>Owner</th>
<th>Cosine Similarity</th>
<th>Degree</th>
<th>Distance from Tier-1</th>
<th>AS Class</th>
<th>Country</th>
<th>ToR</th>
<th>Grade</th>
</tr>
</thead>
<tbody>
<tr>
<td>-</td>
<td>15169</td>
<td>Google</td>
<td>1</td>
<td>54</td>
<td>1</td>
<td>Content</td>
<td>USA</td>
<td>S2S</td>
<td>5</td>
</tr>
<tr>
<td>1st</td>
<td>36385</td>
<td>Google</td>
<td>0.759</td>
<td>4</td>
<td>1</td>
<td>Content</td>
<td>USA</td>
<td>S2S</td>
<td>5</td>
</tr>
<tr>
<td>2nd</td>
<td>63293</td>
<td>Facebook</td>
<td>0.755</td>
<td>17</td>
<td>1</td>
<td>Content</td>
<td>USA</td>
<td>None</td>
<td>4</td>
</tr>
<tr>
<td>3rd</td>
<td>16391</td>
<td>Google</td>
<td>0.743</td>
<td>11</td>
<td>1</td>
<td>Content</td>
<td>USA</td>
<td>S2S</td>
<td>5</td>
</tr>
<tr>
<td>4th</td>
<td>133982</td>
<td>EXCITEL</td>
<td>0.739</td>
<td>6</td>
<td>2</td>
<td>Cable/DSL/ISP</td>
<td>Canada</td>
<td>S2S</td>
<td>5</td>
</tr>
<tr>
<td>5th</td>
<td>38726</td>
<td>VTC DIGICOM</td>
<td>0.736</td>
<td>10</td>
<td>1</td>
<td>NSP</td>
<td>Vietnam</td>
<td>None</td>
<td>0</td>
</tr>
</tbody>
</table>

(e) AS15169: Google, Content Provider similarity example; Total similarity grade: 12.

Figure 4: PCA visualization for Tier-1 ASes based on BGP2VEC embeddings. Each point represents an AS with a size relative to it’s degree, and with a color corresponds to the cluster achieved by applying a DB-SCAN (Black points do not belong to any cluster).
Training Neural Networks (IP Hijack)

- An LSTM Neural Network which is comprised of five layers
- Categorical cross entropy loss function
- Using the Adam gradient-based optimizer with default hyper-parameters
- We build and run our networks using Keras and Tensorflow frameworks
- We train our network based on our labeled dataset
- We use 20% of the samples as a test set
- We run our network for 10 epochs
- Inference time: 0.1 milliseconds on a single Intel CPU

Figure 2: Our LSTM architecture.
Experiments and Results - ToR

- We compare our ToR classification to best known previous results
  - Methods that are based on AS-level paths
  - Our method achieves the best performance, with an accuracy of 94.2%, 5.2% higher than the second-best algorithm (95.2% on s-2)
- Our method had found many mistakes in the CAIDA dataset
  - For the 30 misclassified ToRs with the highest prediction scores - half of our mistakes were actually correct
- We examined 25 ToRs that do not exist in our dataset: 18 correct, 3 siblings
- A large percentage of our misclassifications are attributed to siblings
- ToR classification based on our own dataset (based on ND-ToR with manual correction)
  - 95.8% accuracy, 5.6% higher than CAIDA.

Table III: A comparison of the ToR classification accuracy and recalls.

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>CAIDA AS Relationships Dataset (serial-1)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>GAO</td>
<td>38.4%</td>
<td>1.0%</td>
<td>99.1%</td>
<td>85.7%</td>
</tr>
<tr>
<td>SARK</td>
<td>81.9%</td>
<td>16.1%</td>
<td>95.4%</td>
<td>95.2%</td>
</tr>
<tr>
<td>NDToR CP-CORE</td>
<td>89.0%</td>
<td>99.9%</td>
<td>70.8%</td>
<td>71.2%</td>
</tr>
<tr>
<td>NDToR TS-CORE</td>
<td>56.2%</td>
<td>54.7%</td>
<td>33.3%</td>
<td>82.3%</td>
</tr>
<tr>
<td>NDToR Kmax-CORE</td>
<td>84.6%</td>
<td>12.3%</td>
<td>99.5%</td>
<td>99.4%</td>
</tr>
<tr>
<td>RUAN</td>
<td>78.6%</td>
<td>2.3%</td>
<td>97.8%</td>
<td>97.7%</td>
</tr>
<tr>
<td>BGP2VEC - NN</td>
<td>94.2%</td>
<td>89.0%</td>
<td>93.1%</td>
<td>98.5%</td>
</tr>
</tbody>
</table>
Experiments and Results - ToR

- We test our embeddings using different machine learning algorithms
  - K-Nearest Neighbors algorithm achieves higher accuracy than previous results
  - ToRs can be inferred using simple ML algorithms based on BGP2VEC

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>BGP2VEC - NN</td>
<td>94.2%</td>
<td>89.0%</td>
<td>93.1%</td>
<td>98.5%</td>
</tr>
<tr>
<td>BGP2VEC - LR</td>
<td>81.6%</td>
<td>93.7%</td>
<td>51.1%</td>
<td>49.0%</td>
</tr>
<tr>
<td>BGP2VEC - SVM</td>
<td>76.5%</td>
<td>89.1%</td>
<td>58.6%</td>
<td>57.7%</td>
</tr>
<tr>
<td>BGP2VEC - KNN</td>
<td>92.6%</td>
<td>94.0%</td>
<td>90.0%</td>
<td>90.1%</td>
</tr>
<tr>
<td>BGP2VEC - D-KNN</td>
<td>92.1%</td>
<td>94.0%</td>
<td>89.6%</td>
<td>89.0%</td>
</tr>
<tr>
<td>BGP2VEC - KMeans</td>
<td>61.6%</td>
<td>79.8%</td>
<td>26.6%</td>
<td>43.6%</td>
</tr>
</tbody>
</table>

Figure 3: Number of neighbours with the same ToR based on KNN with K=5 over the symmetric test set for; P2P, C2P, P2C and combined.
Experiments and Results – IP Hijack

- IP hijack detection based on ASN embedding
  - 99.99% Accuracy, 0.00% FA
- 50% of our misclassified predictions were wrong, i.e., we found errors in the labeled dataset
- We tested our algorithm on 48 past documented hijack events between 2008-2018
  - We classified correctly all the events within 2 years of our training data, or 2/3 of all the events
Summary

- A novel approach for ASN embedding using deep learning (BGP2VEC)
  - Unsupervised method
  - Based only on BGP announcements without any side-information
  - A building block for many problems

- Achieves excellent results for AS Type of Relationships (ToRs) classification (based on the CAIDA AS Relationship dataset)
  - Without any assumptions (no ‘VF’)
  - 5.2% higher accuracy than the second-best algorithm
  - ToRs can be inferred using simple ML algorithms based on BGP2VEC
  - As far as we know, we are the first to employs deep learning for this problem.

- Achieves excellent results for IP Hijack Detection
  - 99.99% Accuracy with 0.00% FA on our own proprietry dataset
  - We classified correctly 2/3 of past events
Thank you for your attention. Questions?
Machine Learning by Actigraph Data for Detection of Postpartum Depression

Alexander Binun\textsuperscript{1}, Julie Cwikel\textsuperscript{2}, Shlomi Dolev\textsuperscript{1}, Roy Hershfinkel\textsuperscript{1}

\textsuperscript{1}Dept. of Computer Science, Ben-Gurion University of the Negev
\textsuperscript{2}Spitzer Dept. of Social Work, Ben-Gurion University of the Negev

\textbf{Introduction/Abstract:} Clinical postpartum depression (PPD) is the most common complication of childbirth, affecting 10-20\% of new mothers, with higher rates among low income, immigrant, minority populations, in European countries, the USA and in Israel (Austin & Priest, 2003; Glasser, 2010; Reck et al. 2008; Stewart et al., 2003; Wisner, Chambers & Sit, 2006). In this study, we used actigraphs to detect differences in sleep, and activity, allowing us to use AI techniques to identify mothers whose activity and sleep levels suggest that they may have symptoms of PPD. Using the actigraph as a data collection platform, we used machine learning to distinguish, in the most parsimonious way, those mothers who are consistently showing signs of depression and differentiate them from mothers who are not depressed. Random Forest analysis succeeded in identifying 92.6\% of the 27 cases as either normal or depressed, based on the EPDS (Edinberg Postnatal Depression Scale). The quality of the actigraph results showed that the actigraph succeeds as a screening test: Sensitivity = 100\%, Specificity = 81.8\%. This suggests that the actigraph can be a useful adjunct to clinical observations in order to detect PPD in an early stage.

\textbf{Review of the literature:} While a high percentage (as much as 75-80\%) of new mothers experience mild, transient “baby blues”, PPD is characterized by persistent depressed mood, lack of energy, loss in interest in activities that once were pleasurable, including work and childcare, sleep disturbances and concomitant anxiety and irritability (Stewart et al., 2003). PPD is differentiated from post-partum psychosis that affects about 0.5\% of women after childbirth (Wisner, Chambers & Sit, 2006). The challenges of caring for a new infant bring with them significant hormonal and psychosocial changes, requiring alternations in new mothers' sleep-wake patterns in order to adjust to 24/7 infant care. Mothers in the early post-partum period have consistently less total sleep time (TST), poorer sleep efficiency (SE) and more wake after sleep onset (WASO) in the weeks immediately after delivery, compared to non-pregnant healthy controls (Lee, 2003; Posmontier, 2008). What we do not know is how these changes in sleep parameters correlate or predict changes in mood states.

While extensive research findings have established a reciprocal relationship between sleep and mood disturbances, it is very difficult to ascertain what comes first, the mood or the sleep disturbance. Chronic disturbed sleep is very common among those who suffer from depression (as high as 90\%), and disturbed sleep is associated with grumpy irritability over the short term and is considered a risk factor for the development of a mood disorder over time (Perlis et al., 1997; Zohar, et al. 2005).

Several recent studies explored the relationship between sleep and PPD symptoms using actigraphy. For example, Posmontier (2008) found that objective indicators of sleep quality (measured by TST, SE and WASO using wrist actigraphy) were poorer among mothers with PPD than mothers without PPD in a case-control study with repeated measures, with matched pairs in the USA. However, a Scandinavian study by Dørheim et al (2009) found that at two months post-partum, mothers with PPD retrospectively reported poorer subjective sleep quality compared to
non-depressed mothers, but the two groups did not differ significantly on objective actigraphy or sleep diary parameters measured prospectively. An additional study conducted in Australia, gave further evidence that subjective evaluations of sleep quality are more important in determining post-partum mood that objective measures (Bei et al., 2010). This longitudinal study evaluated objective (actigraphy measures for 7 days) and subjective assessments of mood and sleep quality in the last trimester of pregnancy and two weeks post-partum among both nulliparous and multiparous.

A further American study of 25 healthy, primiparous mothers only, wore wrist actigraphs for one week during the third trimester, and again at 2nd, 6th, 10th and 14th weeks post-partum, while completing sleep logs and surveys and reporting on mood at the end of each actigraph week (Park, Meltzer-Brody, & Stickgold, 2013). Again, subjective sleep assessments strongly predicted PPD scores on the Edinburgh Postnatal Depression Scale (EPDS, Cox, Holden & Henshaw, 2014) at all time points. However, actigraph measures were also significantly correlated with EPDS scores, except for sleep duration. This study suggests that both subjective and actigraphy measures, especially disrupted sleep are predictive of PPD. Yet, all of these studies do not help to track when mood shifts according to disturbed sleep and how this in-depth understanding might be used to detect mothers with PPD early and thus prevent the development of severe post-partum mood and anxiety reactions.

**Methods:** Using a case control study with repeated measures (approximately 1 month, 5-6 months and 12 months post-partum), we will recruited new mothers delivering their first child here at Soroka University Hospital in Beer Sheva, Israel. Exclusion criteria for new mothers: infants designated as small for gestational weight, premature, or with any other serious birth complication, other than singleton birth, inability to speak and write Hebrew, presence of any chronic medical or major psychiatric condition among the mother (excluding perinatal mood or anxiety disorders). We recruited new mothers from our program “Mom to Mom” (Cwikel, Segal-Engelchin et al. 2018) and also by snowball recruiting. A well-known staff member from the Mom to Mom program acted as program manager and approached 45 new mothers in order to form a sample of 30 new mothers. Many mothers were reluctant to participate in the study due to concerns about the effects of the actigraph on their health and their infants. Each volunteer for the study received their actigraph as a gift for participation at the end of the study period.

Sensory wearable technology (actigraphs) offered an opportunity to monitor the health and well-being of the new mothers. By the use of actigraphs, we tracked activity (steps, sleep time, sleep quality) to record indicators of mood over time and use machine-learning techniques to identify abnormal (non-typical) behavior.

All participants were given personal instruction by the project manager on how to use the actigraph and how to upload the data from the actigraph to the study’s website.

**Measures** (all questionnaires to be administered at all three time points). We prepared questionnaires and carried out standard informed consent procedures, following the attainment of ethical approvals from the BGU ethics committee.

This paper analyzes the Time1 (one-month post-partum) data which also included standard demographic measures such as age, education, and marital status. In addition, we collected data on:

**Post-partum depression** Mothers were assessed using the EPDS to indicate PPD symptoms at all three time points (Cox, Holden & Henshaw, 2014). We used the dichotomy of 1-8 as normal (not depressed) and 9 and above as depressed as per the cut-off used in several Israeli studies e.g. (Simhi, Sarid et al. 2019).
Activity level: We will use the method developed by Korszun et al (2002), which monitored activity level and sleep patterns using actigraphy and was able to discern between fibromyalgia patients with and without concomitant depression. This compares mean daytime activity levels, nighttime activity levels, and percentage time spent asleep during the daytime and nighttime as a way to differentiate between depressed and non-depressed patients.

Standard statistical procedures will be conducted using SPSS-25. In addition, we calculated the sensitivity and specificity of the actigraphy measures.

**Calculation of Specificity and Sensitivity of the AI Designations**

<table>
<thead>
<tr>
<th>AI findings</th>
<th>Normal</th>
<th>Depressed</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Normal</td>
<td>16 a</td>
<td>2 b</td>
<td>18</td>
</tr>
<tr>
<td>Depressed</td>
<td>0 c</td>
<td>9 d</td>
<td>9</td>
</tr>
<tr>
<td>Total</td>
<td>16</td>
<td>11</td>
<td>27</td>
</tr>
</tbody>
</table>

Sensitivity = \( \frac{a}{a+c} = 100\% \)

Specificity \( \frac{d}{b+d} = 81.8\% \)

**Experimental Settings:** We conducted a series of experiments, aiming at studying correlations between the physical activities of women before/after giving birth and their emotional wellbeing. Every woman that volunteered in this experiment wore a **MI Xiaomi MiBand** device.

To save data tracked by MiBand, the latter was linked to the cellphone through the MiFit application (There is a separate MiFit version for **Android** and for **iOS**). To save accumulated data, the MiFit application was linked to the cloud account of a woman (via the **GoogleFit** application in Android or via **iOS Health** application).

The following “coarse-grained” data on each woman was saved every 15 minutes:

- The time range, denoted by \( T \)
- Calories burnt during \( T \)
- The distance walked by a woman
  - It might be zero in the night time
  - The way of moving (e.g. biking, jogging) is provided in separate XML files
  - The coordinates of movement trajectories
- The speed of movement
- The time of sleep

These metrics and the daily sums were saved throughout the entire measurement period (3 months).

In addition to the coarse-grained data, the fine-grained data represents detailed trajectories of movement (geodesic coordinates of every point) and the nature of moving (biking, jogging, walking).
30 women kindly consented to save the data every day at her cloud, throughout 3 months, and send the data to us.

**Results and Conclusions:** In unsupervised learning, we tried to identify women with similar activities without knowing the labeling of the data, by means of whether the data is from a depressed or non depressed participant, the results were not indicative enough. In the supervised learning we tried to classify a woman according to other women data and classification using a set of recorded days of the tested woman, possibly first recorded days, allowing early detection of depression. We used classifiers from the large set of sci-kit learn classifiers, among those were:

- Decision Tree classifier
- Random Forest classifier
- K-Neighborhood classifier
- AdaBoost classifier
- Support Vector Classifier (SVC)
- Multi Layered Perceptron (MLP)

The raw data obtained from recording the activities of the women included missed and inconsistent data. The only feature that we found consistent and used in the experiments is *Num Of Calories* -- the number of calories burnt by a woman over the course of some day from the recording period.

The mental status of every woman was assessed following the EPDS (Edinburgh Postnatal Depression Score, Cox et al. 2014) and was used to label the data of each woman accordingly. To classify day data we label days women with EPDS less than 9 as Normal, while day data of women with EPDS at least 9 were labeled depressed.

In the prototype we use the binary classification label *Mood:* Normal and Depressed. If the EPDS ranges from 1 to 8, the class in the training set is 0 (Normal). If the EPDS is at least 9 then the class in the training set is 1 (Depressed).

**Inconsistent data:** Though we obtained the data for 30 women, 3 of them had an incomplete datasets due to family circumstances or malfunctioning devices. They recorded at most one week (instead of the standard 3-month recording period) and their data was partially corrupted. We dropped the entries of these women from the training set leaving 27 women with complete data.

We evaluated every classifier on the dataset, choosing all women (but one) from the dataset as the training set and the remaining one as the test set.

The Random Forest classifier seemed to obtain the best results out of them on the training data.

The next table depicts the overall success rate in classifying women correctly. The success rate for every classifier was averaged over all women participating in experiments.

<table>
<thead>
<tr>
<th>Classifier</th>
<th>Success rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>Decision Tree</td>
<td>50%</td>
</tr>
<tr>
<td>K-Neighborhood</td>
<td>45%</td>
</tr>
<tr>
<td>Classifier</td>
<td>Accuracy</td>
</tr>
<tr>
<td>-------------------------</td>
<td>----------</td>
</tr>
<tr>
<td>AdaBoost</td>
<td>50 %</td>
</tr>
<tr>
<td>Gradient Boost</td>
<td>73 %</td>
</tr>
<tr>
<td>Support Vector</td>
<td>60 %</td>
</tr>
<tr>
<td>Multi-Layered Perceptron</td>
<td>54 %</td>
</tr>
<tr>
<td>Random Forest</td>
<td>85 %</td>
</tr>
</tbody>
</table>

We can see that the Random Forest outperformed all the classifiers.

The table describes the results obtained from the best classifier. We trained the Random Forest classifier on the set consisting of the features for the women with correct data, testing it on the remaining woman.

Eventually, the class of woman is calculated in the following way:

- We calculate the depression day fraction $F$ as the fraction of the days within the recording period of a woman where Depressed is suggested by the classifier.
- When $F < 0.66$ then the woman is classified as Normal. If $F$ greater than or equal to 0.66 then the woman is classified as Depressed.

The following table describes, for every woman:

- the ID of a woman,
- the EPDS level of a woman (1-18)
- whether the label was successfully classified (Hit) or erroneously (Miss). In case of Miss we append the classified label (even if it is erroneous)
- the fraction of the days within the recording period (EPDS at least 9) classified as Depressed
- the number of days a woman recorded data

The fraction of women with the correctly classified labels (HIT) is 92.6%.

This approach boost the 85% correctly classified days per a woman to yield more than 95% correct classification per woman over all the traced period. The first MISS EPDS 9 and had 62% of the days classified as depressed, both values are on the borderline, the last MISS is based on only 31 days, the short tracing period can explain the classification MISS.
Conclusions: Although the set of women was small, we still got very good classification for almost all but one of them (woman number 18 classifications were borderline). Women might want to consider using the actigraph as way to monitor and classify mood and mood changes after the delivery. This might provide a way to detect PPD at an early stage and thus intervene effectively to prevent the deterioration of mood and activity.

Bibliography


<table>
<thead>
<tr>
<th>Woman</th>
<th>EPDS</th>
<th>Coarse-grained EPDS</th>
<th>Hit/MISS:classified</th>
<th>Depression Frequency</th>
<th>Recorded days</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>4</td>
<td>Normal</td>
<td>HIT</td>
<td>0.2</td>
<td>60</td>
</tr>
<tr>
<td>2</td>
<td>8</td>
<td>Normal</td>
<td>HIT</td>
<td>0.59</td>
<td>186</td>
</tr>
<tr>
<td>3</td>
<td>6</td>
<td>Normal</td>
<td>HIT</td>
<td>0.51</td>
<td>29</td>
</tr>
<tr>
<td>4</td>
<td>11</td>
<td>Depressed</td>
<td>HIT</td>
<td>0.99</td>
<td>166</td>
</tr>
<tr>
<td>5</td>
<td>9</td>
<td>Depressed</td>
<td>HIT</td>
<td>1.00</td>
<td>27</td>
</tr>
<tr>
<td>6</td>
<td>9</td>
<td>Depressed</td>
<td>HIT</td>
<td>0.93</td>
<td>567</td>
</tr>
<tr>
<td>7</td>
<td>9</td>
<td>Depressed</td>
<td>HIT</td>
<td>1.00</td>
<td>23</td>
</tr>
<tr>
<td>8</td>
<td>6</td>
<td>Normal</td>
<td>HIT</td>
<td>0.47</td>
<td>14</td>
</tr>
<tr>
<td>9</td>
<td>3</td>
<td>Normal</td>
<td>HIT</td>
<td>0.53</td>
<td>30</td>
</tr>
<tr>
<td>10</td>
<td>6</td>
<td>Normal</td>
<td>HIT</td>
<td>0.51</td>
<td>22</td>
</tr>
<tr>
<td>11</td>
<td>6</td>
<td>Normal</td>
<td>HIT</td>
<td>0.57</td>
<td>27</td>
</tr>
<tr>
<td>12</td>
<td>10</td>
<td>Depressed</td>
<td>HIT</td>
<td>0.83</td>
<td>24</td>
</tr>
<tr>
<td>13</td>
<td>6</td>
<td>Normal</td>
<td>HIT</td>
<td>0.65</td>
<td>572</td>
</tr>
<tr>
<td>14</td>
<td>18</td>
<td>Depressed</td>
<td>HIT</td>
<td>1.00</td>
<td>8</td>
</tr>
<tr>
<td>15</td>
<td>11</td>
<td>Depressed</td>
<td>HIT</td>
<td>0.96</td>
<td>26</td>
</tr>
<tr>
<td>16</td>
<td>6</td>
<td>Normal</td>
<td>HIT</td>
<td>0.48</td>
<td>86</td>
</tr>
<tr>
<td>17</td>
<td>6</td>
<td>Normal</td>
<td>HIT</td>
<td>0.53</td>
<td>27</td>
</tr>
<tr>
<td>18</td>
<td>9</td>
<td>Depressed</td>
<td>MISS:Normal</td>
<td>0.62</td>
<td>222</td>
</tr>
<tr>
<td>19</td>
<td>13</td>
<td>Depressed</td>
<td>HIT</td>
<td>1.00</td>
<td>15</td>
</tr>
<tr>
<td>20</td>
<td>7</td>
<td>Normal</td>
<td>HIT</td>
<td>0.56</td>
<td>9</td>
</tr>
<tr>
<td>21</td>
<td>6</td>
<td>Normal</td>
<td>HIT</td>
<td>0.56</td>
<td>572</td>
</tr>
<tr>
<td>22</td>
<td>6</td>
<td>Normal</td>
<td>HIT</td>
<td>0.49</td>
<td>43</td>
</tr>
<tr>
<td>23</td>
<td>9</td>
<td>Depressed</td>
<td>HIT</td>
<td>0.93</td>
<td>567</td>
</tr>
<tr>
<td>24</td>
<td>4</td>
<td>Normal</td>
<td>HIT</td>
<td>0.00</td>
<td>86</td>
</tr>
<tr>
<td>25</td>
<td>4</td>
<td>Normal</td>
<td>HIT</td>
<td>0.00</td>
<td>15</td>
</tr>
<tr>
<td>26</td>
<td>8</td>
<td>Normal</td>
<td>HIT</td>
<td>0.59</td>
<td>30</td>
</tr>
<tr>
<td>27</td>
<td>11</td>
<td>Depressed</td>
<td>MISS:Normal</td>
<td>0.52</td>
<td>31</td>
</tr>
</tbody>
</table>


Monotonic Prioritized Multi-Criteria

\( k \)-Shortest Path Problem

(Preliminary Version, PhD Track Technical Report)

Shlomi Dolev, Manish Kumar

Department of Computer Science,
Ben-Gurion University of the Negev, Be’er Sheva, Israel
{dolev@cs/manishk@post}.bgu.ac.il

Abstract. The Shortest Path Problem, in real-life applications, has to deal with multiple criteria. Finding all Pareto–optimal solutions for the multi-criteria single-source shortest–path problem with non-negative edge lengths may yield an exponential (number of paths) solution. In the first part of this report, we discuss the results in specific settings of the multi-criteria shortest path problem, which is based on prioritized multi-criteria and \( k \)-shortest path. In the second part of this report, we show a polynomial-time algorithm (for \( k = 2 \)) deciding if, given a graph \( G \) and a pair of vertices \((s, t)\), there exists prioritized multi-criteria 2-shortest vertex/edge-disjoint paths from \( s \) to \( t \) such that the two disjoint paths are shortest.

Keywords: Multi-Criteria, \( k \)-Shortest Paths, Disjoint Shortest Paths, Path Selection

1 Introduction and Related Work

We study a generalization of the shortest path problem in which multiple paths should be computed with consideration to multiple criteria such as cost, delay, and energy consumed edge. The application of these paths is mainly in the transportation networks, communication networks where we need to consider many criteria while computing the shortest path in the transportation network, and routing in the communication networks.

Shortest Path Routing algorithms mainly compute the shortest simple path between two nodes, source \( s \) and destination \( t \). In our system setting nodes and edges, both can have positive cost only, thus no loops exist in the shortest paths. In practice, while computing the shortest path routing algorithm, in general, the graph source node always picks the shortest path for routing from source \( s \) and destination \( t \).

Route latency can be computed by finding multiple (almost) shortest paths in the graph from source \( s \) and destination \( t \). Finding multiple paths is possible by generalizing the Dijkstra algorithm to find more than one path. In the literature, finding multiple

* This research was (partially) funded by the Office of the Israel Innovation Authority of the Israel Ministry of Economy under Genesis generic research project, the Rita Altura trust chair in computer science, and by the Lynne and William Frankel Center for Computer Science.
shortest path problems is referred to as \(k\)-shortest path problem. There are two main variations of the \(k - 1\) shortest path routing problem. The first is to not only find the shortest path but also \(k - 1\) other paths in non-decreasing shortest length (two shortest paths can have the same length) and paths are allowed to visit the same node more than once, which allows a loop. In other variations, paths are not allowed to visit an already visited node. Paths are required to be simple and loopless. The \(k\)-shortest path routing has applications in many areas such as Geographical path planning, Multiple object tracking, and transportation networks.

While finding multi-criteria \(k\)-shortest path, some nodes and edges can be traversed by more than one path which may yield accumulated load (and delay) on the shared node/edge. Delay can be avoided by choosing non-overlapping \(k\)-shortest paths, which is called \(k\)-shortest disjoint paths. These paths can be categorized further in two types: multi-criteria node-disjoint paths and multi-criteria edge-disjoint paths. These disjoint paths are distinct paths in the graph from source \(s\) and destination \(t\) which has a wide range of applications other than routing, such as multi-commodity flow.

**Multi-Criteria Shortest Path**

Many real-life problems can be represented as a network, such as transportation networks, biological networks, and communication networks. In these networks, finding the shortest path resolves many issues such as routing, the distance between two molecules. In general, for finding the shortest path, we consider the criteria (objective) of edge weight (cost), which is called the Shortest Path Problem (SPP) with single criterion. A Multi-Criteria Shortest Path Problem consists of more than one objective while computing the shortest path between source and destination.

In the literature, many existing results are available on MCSPP. The first result on MCSPP was analyzed by Hansen [1], which was focused on a Bi-criteria Shortest Path Problem. Hansen proved that a family of problems exists, for which, any path between a given pair of nodes is a non-dominated path. Hence, any algorithm for solving MCSPP is exponential in the worst-case analysis. Thus, no polynomial-time algorithm can guarantee to determine all non-dominated paths in polynomial time. Martins and Santose [2] modified Hansen’s algorithm [1] and analyzed the vertex labeling algorithm for MCSPP. Climaco et al. [3] worked on path ranking algorithms by using the \(k\)-shortest path routine to solve the MCSPP.

Others consider the case of Bi-Criteria, introducing edges that have cost and delay criteria. The goal is to find an \(s-t\) path that minimizes the cost while having a delay of at most \(T\) (threshold). This scenario is known as Restricted or Constrained Shortest Path Problem. Restricted Shortest Path (RSP) is often used in QoS (quality of service) routing, where the goal is to route a package along the cheapest possible path while also satisfying some quality constraint for the user. RSP is known to be NP-Hard [4]. In result, many fully polynomial-time approximation scheme (FPTAS) [5–10] were designed.

For the problem on general graphs, Hassin [6] presented as FPTAS with a time complexity of \(O(mn(n/\epsilon) \log(n/\epsilon))\), where \(\epsilon\) is the approximation factor. Lorenz and Raz [7] presented a faster FPTAS with a time complexity of \(O(mn(\log \log n + 1/\epsilon))\).
Xue et al. [10] used an extended dynamic programming scheme and achieved faster time complexity of $O(mn(\log \log n + 1/\epsilon))$. Goel et al. [5] presented a $O(mn/\epsilon)$ time algorithm which returns a path a cost no larger than optimum, but delay up to $(1 + \epsilon)T$, where $T$ is a threshold. In an another work by Warburton [8] and Ergun et al. [11] presented FPTAS for acyclic graphs. Ergun et al. [11] used scaling and rounding technique similar to Hassin [6] and improved the running time of $O(mn/\epsilon)$ for acyclic graph.

Bernstein [9] presented a new approach for the restricted shortest path problem in undirected graphs that allowed to break through a long-standing $O(mn)$ barrier and achieve a near-linear running time. Technically, it is $O(m(\frac{1}{K})^{O(\sqrt{\log(n) \log \log(n)})})$ which is $o(mn^3)$ for any fixed $\delta$. A major drawback of the algorithm is: Randomized algorithms, work only for undirected graphs, and $(1+\epsilon)$ approximation in both criteria cost and delay. This algorithm compute paths with delays of at most $(1 + \epsilon)T$ and cost within $(1 + \epsilon)$ of the shortest path with threshold $T$. Xue et al. [12] introduced $K$-approximation algorithm and an FPTAS without enforcing any constraints ($K$). For the case of $K \geq 2$, $K$-approximation algorithm takes $O(Km + n \log n)$ time and FPTAS takes $O(m(n/\epsilon)^{K-1})$ time.

Chen and Nahrstedt [13] introduced the decision version of the MCSPP, which computes a path that satisfies both delay and cost criteria. They proposed a polynomial-time heuristic algorithm based on scaling and rounding of the delay parameter so that the delay parameter of each edge is approximated by a bounded integer. If cost is within the cost criteria and delay is within $(1 - \epsilon)$ times the delay criteria then the heuristic guarantees to find a feasible path in $O((m+n \log n)/\epsilon)$ time. Yuan et al. [14] presented limited granularity heuristic and limited path heuristic algorithm for solving the Multi-Constrained Problem in $O(m(n/\epsilon)^{K-1})$ time, where constraint (criteria) $K \geq 2$.

Korkmaz and Krunz [15] proposed a randomized heuristic for MCSPP. Using simulation they showed that their heuristic provides better performance than other algorithms. For $K \geq 2$ their algorithm take $O(Km + Kn \log n)$ time. Mishra et al. [16] introduced maximum flow-based heuristic. First constructed a class of examples for which the flow-based heuristic computes the path with delays bigger than the optimal solution and then presented an FPTAS, which compute a $(1 + \epsilon)$-approximation with a running time bounded by a polynomial in $1/\epsilon$ and the input size of the instance. In this this paper simulation results confirms the advantage of FPTAS over flow-based heuristic.

The method of adapting to classical algorithms for solving multi-objective shortest path problems are discussed in [17], where a comparison of the effectiveness of solving selected multi-objective shortest path problems defined as mathematical programming problems and multi-weighted graph problems is discussed.

$k$-Shortest Path Problem

The problem of finding the shortest paths in an edge-weighted graph is an important and well-studied problem in computer science. Dijkstra’s sequential algorithm [18] computes the shortest path to a given destination vertex from every other vertex in $O(m + n \log n)$ time. The $k$ shortest paths (KSP) asks to compute a set of top-$k$ shortest
simple paths from vertex \( s \) to vertex \( t \) in a digraph. In 1971, Yen [19] proposed the first algorithm with the theoretical complexity of \( O(kn(m + n \log n)) \) for a digraph with \( n \) vertices and \( m \) edges. The KSP problem has numerous applications in various kinds of networks such as road and transportation networks, communications networks, social networks, etc.

The best-known algorithm for the \( k \)-shortest path problem was proposed by Eppstein [28] which runs in \( O(m + n \log n + kn) \) time. In the initialization phase, the algorithm uses a shortest path tree to build a data structure that contains information about all \( s-t \) paths and how they interrelate with each other, in time \( O(m + n) \). The running time for the initialization can be reduced from \( O(m + n \log n) \) to \( O(m + n) \) if shortest path tree can be computed in time \( O(m + n) \). In the enumeration phase, a path graph is constructed. The path graph is a min-heap where every path starting from the common root corresponds to an \( s-t \) path in the original graph. If we want the output paths to be sorted by the length in increasing order then the enumeration phase requires \( O(k \log k) \) time. Frederickson’s heap selection algorithm [29] can be used to enumerate the paths after the initialization phase in \( O(k) \) time each.

In the case of undirected graphs Katoh et al. [20] presented an \( O(k(m + n \log n)) \) time algorithm. Moreover, for unweighted directed graphs, Roditty et al. [23] presented an \( O(km\sqrt{n}) \) randomized algorithm. In his paper Roditty et al. [23] raised an interesting point that finding \( k \) simple shortest paths between two given vertices in a weighted graph seems to be easier than all pairs shortest path problem. Gotthilf et al. [24] improved Yen’s upper bound. They observed that \( k \)-shortest path can be computed by solving \( O(k) \) all pairs shortest path (APSP) instances.

Feng [25] introduced a node classification algorithm for finding \( k \)-shortest paths, which takes \( O(kn(m + n \log n)) \) time. Kurz et al. [27] introduced a sidetrack-based algorithm with the reuse of shortest path tree, Frederickson’s heap selection algorithm and a priority queue for shortest path tree compute \( k \)-shortest paths in \( O(kn(m + n \log n)) \) time.

Summary of existing algorithms for \( k \)-shortest simple path problem available in Table 1.

Furthermore, another by Hershberg et al. [30] discusses algorithm and implementation of \( k \)-shortest simple path in a directed graph. This algorithms is based on the re-
placement paths of Hershberger and Suri [31], achieved a $\Theta(n)$ speedup over the naive algorithm for replacement paths. The implementation of Hershberg’s algorithm [30] achieved a speedup over Yen’s algorithm [19].

**Disjoint Path Problem**

The disjoint paths problem and its variations are fundamental and extensively studied in graph theory. Many algorithms are proposed in [32–34] for finding edge-disjoint paths. In the problem, given a graph (or a directed graph) $G = (V,E)$ and $k$ vertex pairs $(s_1, t_1), \ldots, (s_k, t_k)$, we find $k$ pairwise vertex-disjoint paths $P_1, \ldots, P_k$ where $P_i$ is a path from $s_i$ to $t_i$ for $i = 1, 2, \ldots, k$ (if path exist). If $k$ is a part of the input of the problem, this is NP-hard problem, and it remains NP-hard even if the input graph is planar. The undirected version of the problem can be solved in polynomial time when $k = 2$ [35–37], while the directed version is NP-hard even when $k = 2$ [38].

**k-Disjoint Shortest Path Problem**

The $k$-shortest disjoint path problem on a graph with $k$ source-destination pairs $(s_i, t_i)$ looks for $k$ pairwise node/edge disjoint shortest $s_i - t_i$ paths. The output is prioritized: the first path should be shortest, the second one should be shortest conditioned by that property of the first path and by disjointness, and so on. $k$-Shortest Disjoint Path Problem is known to be NP-complete if $k$ is part of the input.

This problem was first considered by Eilam-Tzoreff [39]. Eilam-Tzoreff provided a polynomial-time algorithm for $k= 2$, based on a dynamic programming approach for the weighted undirected vertex-disjoint case. This algorithm has running time of $O(|V|^6)$. Later, Akhmedov [40] improved the algorithm of Eilam-Tzoreff whose running time is $O(|V|^6)$ for unit-length case of 2-Disjoint Shortest Path and $O(|V|^7)$ for the weighted case of 2-Disjoint Shortest Path. In both cases Akhmedov [40] considered the undirected vertex disjoint shortest path.

2 Finding Prioritized Multi-Criteria $k$-Shortest Paths in Polynomial Time

Reducing Multi-criteria Weight to Single Weight

Next we present a scheme that converts an existing (single criteria) $k$-shortest algorithm to prioritized multi-criteria $k$-shortest algorithm. The idea is to combine the different weights into a single weight, such that the most significant part of the new single weight, is the weight of the most important criteria. Say, using the first most important $k_1$ bits, that suffice to accumulate the sum of weights of the most prioritized criteria. The second most important weight resides in the next $k_2$ bits of the edge weight, and so on and so forth. We illustrate the conversion using the following example.

In the example we showed the reduction of multi-criteria weight to single weight using an example. In Fig.1 each edge holds a vector of criteria and sum of weights. In
Fig. 2 each edge holds a vector of criteria in binary form and sum of weights in the colored binary form where each color represents the weight of each criterion. In Fig. 3, we computed the only shortest path between node $A$ and $E$ and the total length of path represented in a colored binary number, in that also each color represents the sum of the weight of each individual criteria. The summarized calculations are in Table 2.

### 2.1 Prioritized Multi-Criteria $k$-Shortest Simple Paths

The multi-criteria shortest path problem has a rich history, several approximation and heuristic-based algorithms have been proposed to solve it. Instead of considering the approximation or heuristic approach, we are interested in problem families for which a polynomial solution exists. For example, (1) if one criterion is that no edge on the path should weigh more than a given threshold ($T$), then when computing the shortest multi-criteria algorithm, do not consider this edge. (2) another family of multi-criteria is prioritized multi-criteria where one would like to optimize the first criteria, and within all solutions that optimize the first criteria, find the optimal solution for the second criteria, and so on. (3) a combination of the two multi-criteria above.

Thus, as explained above, to ensemble the weights of the monotonic prioritized criteria into one weight, we use the most important part of an edge ensemble weight for the most important criteria, and the least important part of an edge ensemble weight for the least important criteria, and similarly for criteria in between.

To make sure that the portion of edges weight dedicated to criteria does not overlap, we assign each portion a span of bits in the ensemble weight of an edge to suffice
Table 2. Reduction of Multi-criteria Weight to Single Weight, where $a_i$ is sum of $w_i+1$ weights over all edges, $a_1 = 20$, $a_2 = 14$, $\max_a = 20$, for which value of $\max_a$ is ($2^5 > \max_a \geq 2^3 > 14$), so choose $2^5$ due to 20. In fact, according to $a_2$ only four bits suffice for the description of the $w_2$ to maximal value in a shortest (in fact any simple) path, as $14 < 2^4$.

<table>
<thead>
<tr>
<th></th>
<th>Edge 1</th>
<th>Edge 2</th>
<th>Edge 3</th>
<th>Edge 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>$w_1$</td>
<td>3</td>
<td>4</td>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>$w_2$</td>
<td>4</td>
<td>3</td>
<td>6</td>
<td>7</td>
</tr>
<tr>
<td>$w_3$</td>
<td>5</td>
<td>2</td>
<td>5</td>
<td>2</td>
</tr>
<tr>
<td>$w_1 = w_1 \cdot 2^9$</td>
<td>1536</td>
<td>2048</td>
<td>512</td>
<td>2048</td>
</tr>
<tr>
<td>$w_2 = w_2 \cdot 2^4$</td>
<td>64</td>
<td>48</td>
<td>96</td>
<td>112</td>
</tr>
<tr>
<td>$w_3 = w_3 \cdot 2^0$</td>
<td>5</td>
<td>2</td>
<td>5</td>
<td>2</td>
</tr>
</tbody>
</table>

**Total Weight** 1605 2098 613 2162

**Binary Conversion**

<p>| | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>$w_1$</td>
<td>11</td>
<td>100</td>
<td>01</td>
<td>100</td>
</tr>
<tr>
<td>$w_2$</td>
<td>100</td>
<td>11</td>
<td>110</td>
<td>111</td>
</tr>
<tr>
<td>$w_3$</td>
<td>101</td>
<td>10</td>
<td>101</td>
<td>10</td>
</tr>
<tr>
<td>$w_1 = w_1 \cdot 2^9$</td>
<td>11000000000</td>
<td>100000000000</td>
<td>10000000000</td>
<td>10000000000</td>
</tr>
<tr>
<td>$w_2 = w_2 \cdot 2^4$</td>
<td>1000000</td>
<td>110000</td>
<td>1100000</td>
<td>1110000</td>
</tr>
<tr>
<td>$w_3 = w_3 \cdot 2^0$</td>
<td>101</td>
<td>10</td>
<td>101</td>
<td>10</td>
</tr>
</tbody>
</table>

**Total Weight** 1100100101 | 100000110010 | 1001100101 | 100001110010

for accumulating the criteria weight along the (shortest) path. We can bound the number of bits needed for accumulating the bound on the shortest path, by summing up all weights of the criteria in hand over all the edges in the graph.

Finding the $k$-shortest paths with the ensemble weights results that these are $k$-shortest paths in the most important criteria, as all other criteria do not compete with the most important part of the weights when computing the shortest path(s). Thus, the second criterion breaks ties among the paths as above with the same value of the first criterion. In particular, if the heaviest shortest path according to the first criterion is $w_1$, the selection from the set of the shortest path with weight $w_1$ will be according to the second prioritized criterion if the set of shortest paths with $w_1$ is chosen according to the second criteria where $w_2$ is the heaviest among them, then from the set of paths with weights $w_1$ and $w_2$ paths with the lightest weight according to the third criterion are chosen, and so on and so forth.

The ensemble of the criteria weight into one weight implies finding monotonic multi-criteria $k$-shortest paths that are not necessarily disjoint (as the $k$-shortest Simple Paths) and also for edge/node disjoint paths, all in polynomial time as long as $k$ is fixed.

Our approach is based on generalized Dijkstra algorithm for the multi-criteria shortest path. Using the Dijkstra algorithm, it is possible to determine the shortest distance (or the least cost/ least delay) between a start node and any other node in a
graph. The idea of the algorithm is to continuously apply original Dijkstra algorithm with the precomputed ensembled weight for each edge and remove the edge which holds more weight than Threshold \((T)\).

For multiple criteria, to avoid the exponential number of paths, we reduce the set of all criteria as a single value for each edge. We reduce the prioritized multi-criteria by a reduction to a single criterion. Let us define the ensembled edge weights as follows.

Let \(W_i = \sum_{e \in E} w_i(e), 1 \leq i \leq q\). Let \(l_i = \lceil \log_2(W_i + 1) \rceil, 1 \leq i \leq q\), and let \(r_q = 0\), \(r_i = \sum_{j=i+1}^q l_i, 0 \leq i \leq q-1\). The ensembled weight of the edge \(e \in E\) is defined to be \(EW(e) = \sum_{j=1}^q (2^j w_i(e))\). As usual we define the ensembled weight of any path \(P\) as \(EW(P) = \sum_{e \in P} EW(e)\).

Our approach consists of the following steps: \(Q\) is the set of nodes for which the shortest path has not been found. Initialize the source node with distance 0 and all nodes with distance “infinite”. At each iteration, the node \(v\) that has the minimum distance (sum of weights \(EW\)) value to the source is added to the \(S\), which provides the shortest path from the source node to the destination node.

For computing the multi-criteria \(k\)-shortest simple paths, we use the Dijkstra algorithm for computing the shortest paths and Yen’s algorithm \([19]\) for computing \(k\)-paths. Consider two lists, first list \(A\) for permanent shortest paths from the source node to destination node in sorted order, and list \(B\) for tentative/candidate shortest paths. Initially, find the first shortest path from the source node to destination node using \(Dijkstra(G, s, t)\) and make a local copy for graph \(G\), which we use in execution after finding one path. The \(k^{th}\) shortest paths may share edges and sub-paths (path from the source node to any intermediary nodes within the path) from \((k - 1)^{th}\) shortest path.

Then take \((k - 1)^{th}\) shortest path and make each node in the path unreachable in turn, i.e. remove a particular edge that goes to the node within the route. Once the node is unreachable, find the shortest path from the preceding node to the destination. Then we have a new path that is created by appending the common sub-path (from the source node to the preceding node of the unreachable node) and adds the new shortest path from the preceding node to the destination node. This path is added to the list \(B\), only when it has not appeared in list \(A\) or list \(B\) before. After repeating this for all nodes in the path, we have to find the shortest path in list \(B\) and move that to list \(A\). We just have to repeat this process for \(K\) times.

### 2.2 Prioritized Multi-Criteria 2-Shortest Node/Edge Disjoint Paths

In this section we present 2-shortest path node/edge independent algorithm, see Eilam-Tzoreff \([39]\) and the references there in, to the case of prioritized criteria from a single source to a single destination. Without loss of generality, we detail the extension for a particular such algorithm, namely, for \([40]\).

For finding 2-shortest disjoint paths, consider the approach when multi-source and multi-destination are given. We make two copies of our source and destination and connect all copies of source and destination to the neighbors of the original source and destination and find the 2-shortest disjoint paths. Akhmedov \([40]\) introduced \((|V|^7)\) time algorithm for computing the 2-Disjoint Shortest Paths. Our approach uses the algorithm of Akhmedov \([40]\).
Our approach consists of the following steps: First, make 2 fixed copies of the given source and destination, and connect those copies to the neighbors of the original source and destination. Reduce the prioritized multi-criteria by a reduction to a single criterion. Choose two-pair of sources and destinations and compute 2-Disjoint Shortest Paths, while computing the path algorithm check the condition of rigidness. The quadruple \((s_1, t_1, s_2, t_2) \in V\) is called rigid iff \(s_1, t_1 \in L(s_2, t_2)\) and \(s_2, t_2 \in L(s_1, t_1)\), where \(L(s_i, t_i)\) represents is a set of all nodes belonging to at least one shortest path between \(s_i\) and \(t_i\).

Our approach explained briefly using an example in Fig. 4 we consider a graph \(G = (V, E)\), locate the source and destination node in the graph \(G\) (Fig. 5). Replace the chosen nodes with 2-copies and connect with the original neighbors (Fig. 6) and then compute the multi-criteria 2-shortest disjoint path.

![Fig. 4. A given graph \(G = (V, E)\)](image)

![Fig. 5. Locate the source (node \(F\)) and destination (node \(B\)) in the given graph \(G\)](image)
Fig. 6. Replace the chosen nodes with 2-copies and connect with the original neighbors.

Acknowledgement

We thank Yefim Dinitz for valuable discussion and helpful comments.

References


Toward Provable One-Way Functions

(Preliminary Short Note, PhD Track)

Hagar Dolev\(^1\) and Shlomi Dolev\(^2\)

\(^1\)School of Computer Science, Hebrew University and Bezalel, Jerusalem, Israel
\(^2\)Dept. of Computer Science, Ben-Gurion University of the Negev, Beer-Sheva, Israel

June 27, 2020

Abstract

The existence of a provable one-way function is a long-standing open problem. This short note presents an example towards the existence a provable one-way function, example in which both directions are polynomial. Namely, we prove that given a sorted array it takes \(\Theta(n)\) operations to randomly permute the array values uniformly over the permutation space, while (comparison based) sorting of the permuted array (of big enough values) requires in the worst case (and in the average case) \(\Theta(n \log n)\) compare operations.

We also present a candidate cryptosystem based on permutations of random polynomial values.

Keywords: One-way functions, Cryptography, Merkle Puzzles

1 Introduction

One Way functions are functions of the shape \(f : x \rightarrow f(x)\) such that they are easy to compute, and they are hard to “decipher”, meaning given a random image of \(f(x)\) it is hard to compute \(x\). Where easy means they have a polynomial time \(p\) Turing Machine that given an input \(x\) computes \(f(x)\) in polynomial time, and hard means that given a random \(f(x)\) we cannot compute \(x\) in the same polynomial time \(p\).

These functions play an important role in modern cryptography. Unfortunately, there is no provable one-way function, and the currently functions that are used in practice as one-way functions are assumed to be one-way functions, rather than proven to be such functions. Sometimes later revealing a weakness e.g., [5].
2 The One Way from Sorted Array to (uniformly) Unsorted and the Way Back

The lower bound on comparison-based sorting is a basic result in computer science. The number of possible permutations of the inputs is \( n! \), thus, the number of decision tree leaves is \( \log n! \) which is bigger than \( \log(n/2)^{n/2} \) which is in turn \( n/2 \log n/2 \), thus, \( \Omega(n \log n) \). Shuffling a sorted array can be performed by randomly and independently choice of a sequence of \( n \) indexes of the array, and swapping the first value of the array with the value appearing first in the indexes sequence, using the resulting array as an input for swapping the second array entry with the value residing in the index that appears second in the indexes sequences, and so on and so forth, yielding \( \Theta(n) \) operations, for producing a shuffled array (that is for symmetric reasons) chosen uniformly over all permutation possibilities.

It is known that the average depth of a leaf in binary tree with \( n! \) leaves is \( \Theta(n \log n) \). Thus, with very high probability sorting a uniformly random chosen instances of shuffled array are as hard as the worst case (the importance of average case hardness as the Shortest Vector Problem over lattices and the permanent are demonstrated when implementing Merkle puzzles schemes e.g., [4, 3]).

There are \( \Theta(n) \) sorts that are not comparison based. These sorts, e.g., counting sort or Radix sort, are based on a limited range of the array values, while we can choose input arrays with values of enough number of bits to imply that Radix sort is less efficient than comparison-based sort.

Others, such as bucket sort, are designed for the average case and are based on distribution of the array elements, while we can choose and produce arrays (sorted arrays to be shuffled) with inconvenient distributions. Thus, enforcing the use of comparison-based sorting\(^1\).

3 Merkle Puzzles Use-case

We demonstrate the usefulness of such one-way function by using Merkle puzzles. Alice may receive or produce \( k \) sorted arrays. To produce a sorted array Alice may repeatedly chose a random value and add the chosen value to the previous element in an array, where the previous element of the first value is set to be zero.

Alice randomly shuffle each of the arrays, recording the permutation of the shuffle investing \( O(kn) \) computation time. The permutation of the shuffle maybe recorded as part of the values, multiplying (possibly by shifting) each element in the array by at least \( n \) and adding the original index prior to shuffling. Then removing the index and dividing/shifting back post shuffling and post recording the permutation.

\(^1\)In particular, one can assume a computing device that (is optimized to) supports comparisons rather than operations needed for non-comparison-based sorts, as in many cases in practice.
Note that the permutation can be regarded as a trapdoor $t$, knowing $t$ implies $\Theta(n)$ operations for “sorting” the shuffled array.

Then Alice sends to Bob the $k$ arrays, Bob randomly selects one, and sorts it in $O(n \log n)$ time, Bob uses the same technique to record the sorting permutation. Now, say, Bob bit-wise xors all the even indices in the sorted array entries and the even indices (padded concatenated to form a sequence that is broken to the length bits of the array entries) of the permutation and send to Alice as a mean to identify his chosen array, without revealing the actual permutation to Eve. Then both use a function (possibly bitwise xor) over the index of the chosen array and the permutation as a shared symmetric key. The symmetric key is secure for a while.

Alice and Bob can repeat the procedure, this time encrypting the arrays with the previous key(s), so that Eve cannot start solving the new set of puzzles prior to revealing the puzzle (array) chosen previously by Bob (See [4, 3]).

We note, that one approach is to explore hard in average instances of complexity class that is provable higher than $P$ and $NP$ as suggested in [2], and randomly use (short) instances as puzzles, however unlike in the case of one-way functions, in such cases Alice invest significant computation power (even more than Eve) prior to sending the puzzles to Bob.

4 More Secret Permutations and Secret Shared Polynomials

The number of possible permutations is exponential in $n$. Choosing an arbitrary random permutation rather than the sorted permutation as the secret may yield a greater gap in the computation of the one way versus the way back direction.

There is a possibility to describe a permutation of $n$ values by a polynomial of degree $n - 1$, where the $x$ of a value in the array is the index in the array, and the $y$ is the actual value. One can randomly choose a polynomial $p$ of degree $n - 1$ over a finite field, and use the free coefficient as done in secret sharing, so $n$ points on the polynomial are needed to reveal the free coefficient. Then calculate the values in the array according the randomly chosen polynomial $p$.

The obtained array can then be randomly permuted. Then, requiring re-ordered to fit a polynomial with the free coefficient as the one of $p$. Furthermore, to enforce considering many (preferably all exponential number of) permutation and avoid information leakage on the free coefficient, two such arrays based on two random polynomials, can be independently constructed. The free coefficients of the two arrays can be bitwise xored (just like one-time pad for each other).

The elements of the two arrays maybe shuffled together to form a permutation of $2n$ elements, or in fact, $n$, if each array consists of $n/2$ elements that are defined by a random polynomial of degree $n/2 - 1$.

Furthermore, one can build a symmetric key cryptosystem, where the random shuffling
permutation is the shared key, and the message is bitwise xored with the two free coefficients. Thus, coping with leakage of a free coefficient in case of known-plaintext attack.

The permutation secret key can be co-ordinately replaced even in every communication, by using the randomness of the polynomials.

5 Conclusions

We believe that the approach in which random function is used for one way, implying the need to cancel the randomization effect is a promising direction for provable one-way function also for higher complexity classes.

Acknowledgments. We thank Moti Yung for correspondence on the subject.

References


Video synthesis of an exemplary patient exercise as part of a physiotherapeutic treatment

Itai Dror, Ofer Hadar
School of Electrical and Computer Engineering
Ben Gurion University of the Negev
Enhancing Robotic Physiotherapeutic Treatments using Machine Learning

- Czech-Israeli Cooperative Scientific Research, 2019–2021
- Czech Technical University in Prague, Ben Gurion University
- Research fields: Machine learning, robotic physiotherapy, remote medicine.
- The presented preliminary video synthesis is one of the tasks of the cooperative scientific research
Normalized drawing of subjects’ vertexes (different colors represent different subjects)
Openpose software finds human joints coordinates

https://github.com/CMU-Perceptual-Computing-Lab/openpose

25 key points coordinates for skeletal modeling
Distribution of angles between joint vertexes throughout the exercise
Goals of the exemplary patient video synthesis research

• Investigates the usefulness of this approach for medical application as part of a physiotherapeutic treatment program.

• Motivate patients to perform better when they see themselves performing their exercise as well as their instructors.

• Consider gradual program, synthesize only a small improvement at a time.
Input/output variables

- **Input 1:** Video or image(s) of a patient exercise performing the physiotherapist exercise but his performances lack the complete movement of one or more of his limbs.

- **Input 2:** Video of a physiotherapy exercise performed correctly by a professional instructor.

- **Output:** A synthesized convincing artificial video animation that shows the patient as he is performing the exercise precisely as his instructor.
The following papers with code may accomplish the video synthesis

<table>
<thead>
<tr>
<th>Code</th>
<th>Github stars</th>
<th>Code by authors</th>
<th>Written in</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="https://github.com/NVIDIA/vid2vid">https://github.com/NVIDIA/vid2vid</a></td>
<td>7400</td>
<td>Yes (Nvidia)</td>
<td>Python, Pytorch</td>
</tr>
<tr>
<td><a href="https://github.com/NVlabs/few-shot-vid2vid">https://github.com/NVlabs/few-shot-vid2vid</a></td>
<td>1300</td>
<td>Yes (Nvidia)</td>
<td>Python, Pytorch</td>
</tr>
<tr>
<td><a href="https://github.com/nyoki-mtl/pytorch-EverybodyDanceNow">https://github.com/nyoki-mtl/pytorch-EverybodyDanceNow</a></td>
<td>820, 371, 315, 164</td>
<td>?</td>
<td></td>
</tr>
<tr>
<td><a href="https://github.com/AliaksandrSiarohin/monkey-net">https://github.com/AliaksandrSiarohin/monkey-net</a></td>
<td>246</td>
<td>Yes</td>
<td>Python, Pytorch</td>
</tr>
<tr>
<td><a href="https://github.com/AliaksandrSiarohin/first-order-model">https://github.com/AliaksandrSiarohin/first-order-model</a></td>
<td>4800</td>
<td>Yes</td>
<td>Python, Pytorch, Jupyter Lab</td>
</tr>
</tbody>
</table>
Why did I started with the “first order model”? 

• Recent
• Github code
• Pretrained models
• Jupyter lab examples
• Very well explained
• One shot learning (Advantage as well as a disadvantage)
Initial results: Source image, driving video (instructor), predicted animation
Common terms and systems’ names

• Face2Face program, 2016, no need for a depth camera
• Video to video synthesis, Nvidia Dec 2018 “Video-to-Video synthesis” paper
• Full body motion transfer
• Image animation from
• “You do what I do” from “Every body dance now” paper
• Deep fake (Deep learning & Fake)
  • Deep fake appeared in Reddit at the end of 2017 approaching 90,000 subscribers and then shut down
• Full body avatar
Opportunities

• Remote medicine applications

• Low cost cinema, artificial characters, automated replacement of stuntmen by actor, advance video editing

• Video compression, high-quality Zoom by sending only facial landmark and real-time reconstruction of the face

• Change appearance, for example, makes less sleepy, filter unwanted actions.

• High quality data augmentation for training deep learning models

• Video games

• Deep fake detection

• Block chains for secured and authenticated video

• Fashion and clothing

• Much more
Negative consequences

- Fake news
- Hoaxes
- Frauds
- Scams
- Identity leakage
- Shaming videos
- Tampering medical images
- Many others
Popular face swap open source software

<table>
<thead>
<tr>
<th>software</th>
<th>Stars</th>
<th>Recent activity</th>
<th>Starting at</th>
<th>Written in</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="https://github.com/deepfakes/faceswap">https://github.com/deepfakes/faceswap</a></td>
<td>31,200</td>
<td>yes</td>
<td>Dec 2017</td>
<td>Python, Tensorflow, Keras</td>
</tr>
<tr>
<td><a href="https://github.com/AliaksandrSiarohin/first-order-model">https://github.com/AliaksandrSiarohin/first-order-model</a></td>
<td>17,000</td>
<td>yes</td>
<td>July 2019</td>
<td>Python, Tensorflow</td>
</tr>
<tr>
<td><a href="https://github.com/shaownlu/faceswap-GAN">https://github.com/shaownlu/faceswap-GAN</a></td>
<td>2800</td>
<td>no</td>
<td>June 2018</td>
<td>Python, Keras, Tensorflow</td>
</tr>
</tbody>
</table>

Face swap detection

<table>
<thead>
<tr>
<th>software</th>
<th>Stars</th>
<th>Recent activity</th>
<th>Starting at</th>
<th>Written in</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="https://github.com/ondyari/FaceForensics">https://github.com/ondyari/FaceForensics</a></td>
<td>1300</td>
<td>no</td>
<td>Sept 2019</td>
<td>Python, Keras, Pytorch</td>
</tr>
<tr>
<td><a href="https://github.com/topics/deepfake-detection">https://github.com/topics/deepfake-detection</a></td>
<td>174, 161, 153, ...</td>
<td>Comment: list of several repositories</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Basic CNN (Convolutional Neural Networks) Autoencoder
Basic deep fake encoder/decoder (simple and powerful programmer’s solution)

GAN (Generative Adversarial Models), Ian Goodfellow, 2014.

https://www.google.com/search?q=generative+adversarial+models&bvm=bv.116750106,d.UMQ&source=lnms&tbm=isch&tm=0&ei=CF7GXXVUGaMx5gYlopY3Cg&sa=X&ved=0ahUKEwig38vXtKrqAhUEtqQKHTLWAGyQ2-cCgQBAw&ved=2ahUKEwig38vXtKrqAhUEtqQKHTLWAGyQ2-cCgQBAw#imgrc=OdLb8ddgNHcANM

CSCML July 2-3, 2020 Ben Gurion University
Conclusions

• Recent human body motion to motion transfer systems can transfer physiotherapy instructor’s movements into patient appearance models.

• Maturity of these models are far from face swap (deep fake) techniques where it’s hard to distinguish between real and fake.

• Need to add hand and face key points to make synthesis more realistic.

• Reconstruction of patient’s appearance based on recent skeletal whole-body human pose estimations including facial and hand joints key points will provide better results.
Thanks!
Entrepreneurship Pitch

Track Chair: Prof. Oded Margalit
Information security practitioners have always had to take a wide-angle view of the world, because there is no aspect of life that is so disconnected from information security that it is immune to problems, or at least the possibility of improvements.

This year’s CSCML Entrepreneurship Pitch Track is a perfect example of this. It is clear that the entrants had a pulse on the current situation in information security, and are gearing up, (in some cases already have did so) to meet the challenge head-on, and in the process – protect all of us.

Entries came from varied areas like cryptoanalysis, IoT, BlockChain, visual analytics, and even the COVID-19 relevant infection prevention. It was heartening, this year as well as in past years, to note that, even in a business focused track, there were entries that could justifiably be considered “for the greater good of the people” – that is, even if they had business motives and priorities, they would still end up benefiting all of us.

These entrepreneurs deserve all the encouragement that we in the community can give them, in whatever form is suitable.

As was the case last years, the Entrepreneurship Pitch Track at CSCML 2020 did an excellent job of fulfilling this objective and consequently was a great success. It received sponsorship from leading VCs (JVP, YL ventures, Pitango, JSCapital, ...) and corporations (Citi, Elron, Mellanox, ...). Seven start-ups pitched in the event, out of which Siraj’s “Leveraging deep learning to automate device connectivity to any platform.” was selected by the Entrepreneurship Pitch Track Committee and the audience as the leading entry and won the $500 prize donated by-Prof. Bezalel Gavish (ATSMA).

FertilEyes: who developed an IoT device and an algorithm to optimize nitrate levels in the soil, received second place, and “Drones’ Cryptanalysis: Detecting Spying Drones” placed third.

Looking forward to an even better CSCML 2021.

Regards,

Prof. Oded Margalit, chair

Entrepreneurship Track
In situ, real-time monitoring of nitrate in soil

Professor Ofer Dahan
Professor Shlomi Arnon
PhD. Student Elad Yeshno
Nitrate water contamination

Graph showing the nitrate concentration in water over the years from 1940 to 2020. The concentration increases from about 20 ppm in 1940 to over 50 ppm in 2020. The diagram illustrates nitrate leaching loss and the water table.
The importance of effective nitrate monitoring in soils:
The economical implications of uncontrolled nitrate application:

GERMANY FACES BILLIONS IN FINES FOR BREAKING EU LAWS ON NITRATE POLLUTION

EMILY MACINTOSH × JUNE 21, 2018

AGRICULTURE  EIR  EUROPE PROTECTS  NATURE  WATER  💘  1  2 MIN READ

The EU’s top court has ruled that Germany is in breach of EU law by not cleaning up its act on water pollution caused by farm fertiliser run-off. The case began in 2016 when the European Commission referred the German government to the EU Court of Justice over non-compliance with the Nitrates Directive – an EU law on water protection that sets limits on excess manure spreading in vulnerable areas.

Source:
German farmers: 'Overregulation is the last thing we need'

Farmers from across Germany have descended on Berlin to take part in a mass protest against the government’s agricultural reform package that foresees a reduction in the use of fertilizers, pesticides and insecticides.

Less fertilizer, less yield

"When we're supposed to reduce the use of fertilizers by 20% as the government wants us to, it means that our plants get 20% less nutrients every year, and that will have a corresponding impact on our yields and our incomes," said the farmer from Bavaria. "I'd love my son to join our business, but if you can't live off it in the future, it doesn't make any sense to keep him interested."
The economical implications of uncontrolled nitrate application:
The importance of effective nitrate monitoring in soils:
The importance of real-time nitrate monitoring in soils

Water resource preservation:
• Excessive use of fertilizers highly contributes to water resources degradation

Smart, efficient agriculture:
• Optimize fertilizers application
• Increase the agricultural yield
The project’s approach
Engineering and practical requirements from nitrate sensor in soils

• Applicability for wide range of nitrate concentration

• Stability at different temperatures, pHs, and immunity for measurement drifts

• Capability for direct and real-time application in soils

• Affordable for commercial use
Nitrate absorbance spectroscopy

- Absorbance wavelength: 235 nm
- Greater absorbance than 300 nm
Nitrate absorbance spectroscopy
Column experiment

Data logger

Sample accumulation chamber

Optical flow cell
Column experiment

- Daily irrigation cycle
- One cycle was altered with nitrate solution
Results - break through curve
Multiple soil types column experiment

- Sandy loam + Compost
- Sandy loam
- Dark clay Soil
Online nitrate monitoring

Figure 11. Nitrate breakthrough curves for (a) sandy loam, (b) sandy loam with 10% compost, and (c) dark clay soil.
Wheat grow column experiment
Wheat grow column experiment

Nitrate (ppm)

Soil Water content(%)
Live nitrate monitoring in Ashalim MOP
Live nitrate monitoring in Ashalim MOP
First generation patents:
Nitrate monitoring system miniaturization

First generation

Second generation

Third generation

IoT Device

TO SCALE
Economic potential for nitrate sensing:
Series of sensors – Big Data
The cannabis market was valued at USD 14.5 billion in 2018, and it is projected to reach 89.1 billion by 2024, with a CAGR of 37% during the forecast period.

“Slumping grain, meat and dairy prices have eroded agriculture incomes, sparking more farmers to adopt so-called precision-agriculture methods to help increase efficiency.

Companies including Deere & Co. are joining the race to create new products for the market that Goldman Sachs Group Inc. estimates could be worth $240 billion by 2050. The U.S. Department of Agriculture said in a report last week that the new technologies are helping to boost profits”
Thank you very much for your attention
The Problem

INFECTIONS - PATIENT’s BIGGEST FEAR *

- Not accountable
- Not monitored
- Not educated
- Not independent

20%-70% Preventable **

70K Deaths

650K infections

~ $17M Loses Annually Per Hospital ***

* BBS-NEWS
** CDC
*** Hospital-Acquired Infections by the Numbers
The Solution

AI Monitoring  Dr Hygiene App

Reduces Fear  Makes Money  Improves Outcomes  Saves Money

Educate  Interact  Disinfect  Monitor

AntisepTech - Company Proprietary & Confidential
Analytics - App

Pilot at the Davidoff Cancer Center, Rabin Medical Center
In collaboration with Dr. Bina Rubinovitch & Dr. Boaz Tadmor

---

**Distribution of interest and knowledge in the various fields**

- % correct answers (trivia) & % interest (FAQ)
- Station a+b

**Usage Distribution of the different interaction's types**

- % engagement FAQ & trivia & SRL
- Station b

**Users Experience Reports**

- Clarity
- Contribution to knowledge
- Easy to use

---

AntisepTech - Company Proprietary & Confidential
#1st Place – National Competition
Empowering the People

Centers for Disease Control and Prevention

“We would like to invite you to continue in the collaboration if you are interested. This would include participating in teleconferences discussing progress, barriers, problem solving etc. We hope you might be interested in continuing the collaboration in this way—we think it might be mutually beneficial.”

Prof. John Jernigan
Deputy director
Division of Healthcare Quality Promotion
CDC’s National Center for Infectious Disease

Columbia University

“Your system is innovative and unique and if the beta testing is promising, it may be very welcome and useful in a variety of healthcare settings. You might also consider alternative health care sites such as nursing homes, ambulatory care clinics, dialysis units, cardiac catheterization units, surgical suites, etc. Please accept my best wishes as you embark on this important venture.”

Prof. Elaine Larson
Associate Dean for Nursing Research
School of Nursing, Columbia University
Leader in the field of Hand Hygiene
B2B Model

- Dr Hygiene - SaaS
- AI Monitoring - On Premise

Annual Licensing + Premium Services

Annual Revenue / US Hospital Bed

$1,250

Potential Customers/Partners

- NIH
- Premier Health
- Nursing Homes
- Addiction Rehab Center
- HealthNet Homecare
- Blue Cross Blue Shield
- STANLEY Healthcare
- Gojo
- Cirrus MD
- Haven
## Significant Milestones

### R&D
- **Educational App**
  - Increasing team size
  - Development
- **Surface Hygiene**
  - Increasing team size
  - Development
  - Pilot – 1st cycle (5th Month, 2 weeks)
  - Initial feedbacks
- **Hand Hygiene**
  - Develop – Best practice

### M&S G&A
- Swiss/Israel program
- Israel Innovation Authority (IIA) submission (+~$200K)
- Design partner: Medical Center (US)
- IIA approval (???)
- Horizon2020 submission (€2M grant and/or up to €12M blended grant/equity)
- Design partner: Nursing Home (US)
- IIA submission (+~$500K)
- Horizon2020 approval (???)
- Distribution agreement
- Funding - next round

### Budget
- **6 Months**
  - Educational App: $430K
  - Surface Hygiene: $670K
  - Hand Hygiene: $700K

- **12 Months**
  - Educational App: $500K
  - Surface Hygiene: $700K
  - Hand Hygiene: $800K

- **18 Months**
  - Educational App: $540K
  - Surface Hygiene: $770K
  - Hand Hygiene: $850K

- **24 Months**
  - Educational App: $600K
  - Surface Hygiene: $800K
  - Hand Hygiene: $900K

### Note
- Horizon2020 approval may require additional matching funding.

---

AntisepTech - Company Proprietary & Confidential
Unique approach
Joins patient and family as an integral part of the health organization infection prevention efforts

Hospital incentives
Improves outcome, saves money, makes money and share accountability with patients

Unmatched visual experience
Awesome interactive visual information alongside educational gamification elements

US patent
Freedom to operate for a few of the most important aspects of infection prevention

Best Hygiene Practices
Seal-of-Approval in the eyes of providers, payers and patients

Design and Brand
Memorial names to gain share of mind
AntisepTech's INFECTION MONITOR

AntisepTech - Company Proprietary & Confidential
Barak Katz (PhD)
CEO

- Responsible for AntisepTech technology, healthcare as well as business aspects jointly with Marty Larson
- Past six years has explored and highly involved in the infection prevention digital health field
- PhD in the field of 3D imaging and incoherent holography

Marty Larson
US Penetration

- Responsible for US market penetration as well as business aspects jointly with Barak Katz
- President of ASCEND and vice president at Greater Dayton Area Hospital Association - GDAHA
AntisepTech
Empowering The People - Preventing Infections
Stream of Distributed Secrets for Quantum-safe Blockchain

Shlomi Dolev, Ziyu Wang
Motivation
Market interests

- Worldwide finance companies and organizations pay a lot of attention on Blockchain.

  ✓ ALFA (Russia)
  ✓ Yes Bank (India)
  ✓ United Overseas Bank (Singapore)
  ✓ Common Wealth Bank (Australia)
  ✓ LatiPay (New Zealand)

J.P. Morgan

- Twelve Chinese banks have already adopted blockchain technology for various cases

Deloitte
A lot of countries have recognized Bitcoin and related cryptocurrency instruments as legal payment methods.

- Permissive (legal to use bitcoin)
- Contentious (some legal restrictions on usage of bitcoin)
- Contentious (interpretation of old laws, but bitcoin is not prohibited directly)
- Hostile (full or partial prohibition)
President Xi leads the Central Committee of the CPC to learn Blockchain and publicly asserts the necessity to develop blockchain related technologies on Oct. 29th, 2019.

=> As the largest emerging market, China is looking forward to every non-cryptocurrency blockchain technology.

BRICS five nations plan to create a blockchain technology for payment settlements to replace SWIFT. (Nov. 15th, 2019).
China and the USA have a trade war.


The 7th round of negotiations of the China-Israel Free Trade Agreement has been successful in 2019.

Cross border trading is still popular even in the post-corona time. Globalization won’t stop, and blockchain is a good tool in this area.
The global blockchain market expected to grow from USD 15 billion in 2020 to USD 60 billion by 2024.

Source: IBM WinterGreen Research, Inc.
Various Application

- A global decentralized payment system instead of traditional and centralized ways like Visa, MasterCard, PayPal, SWIFT, Western Union, and Alipay.
  - Without being controlled by one authority
  - Help undeveloped countries build finance systems

- A decentralized trust infrastructure for global companies and organization, i.e., consortium blockchain which is used by IBM, VMware and Alibaba.

(As far as I know, AntFin sells a blockchain solution, BaaS, having four cloud nodes at the price of million shekels.)

- As know as Internet 3.0 to collect Internet remained values which is valued by a lot of media and entertainment companies including SM Entertainment (Korea) and DMM (Japan)
As known as Internet 3.0 to **collect Internet remained values** which is valued by a lot of media and entertainment companies including SM Entertainment (Korea) and DMM (Japan).

Fans can earn some tokens => which can exchange the movie ticket or other related products.
Blockchain is a technology to solve Decentralized Trust issues

But can current blockchain systems support the demand?
**Current Blockchain** cannot support market visions

- **Bitcoin** users need wait at least **one hour** resulting in an inefficient processing speed, seven transactions per second (TPS), far away from a global payment system like Visa (65,000+ TPS at the peak); It also consumes too much electricity power.

- Bitcoin blockchain (also other partial synchronous blockchain like Libra) relies on a **strong synchronous** network which may not fit the world wide Internet.

- Blockchain (and its based cryptography tools) should have survived the upcoming **quantum** computing era.
A permissioned blockchain:

- **High performance**: can support 175,000 TPS worldwide transactions.
- An **asynchronous** protocol without any timing assumption like the expansive time-out
- Deploying signature-free Byzantine agreement and broadcast tools to achieve **quantum-safety** and high efficiency simultaneously.
Why a permissioned blockchain

- Centralized payment (may suffer “one point” failure)
- Imagining Nokia...

A permissioned blockchain (around 30~100 nodes from large banks and institutes)

- A normal step and seize the chance...
- SodsBC

- A permissionless blockchain (around 10000 nodes)

- Too pioneered and also maybe dead...
- bitcoin

Permissioned blockchain will be more successful and gain more business interests in the industry compared with permissionless blockchain.
Traditional leader-based blockchain:
An expensive time-out, much longer than regular operations

Use a long time-out to identify a malicious leader: Several seconds or even several minutes => if some node is malicious, the protocol is slow down

- Facebook Libra will **suffer** this problem, and **SodsBC** can **overcome** it to make the protocol very fast => Byzantine wait-free
Asynchronous blockchain:
- Every participant proposes a block part.
- All participants agree on the consistent **union** of block parts.
Asynchronous blockchain:
- Every participant proposes a block part.
- All participants agree on the consistent union of block parts.
- If a block part is inconsistent, then excluding this block part.
SodsBC

Asynchrony

- Deciding each block part
- Utilizing a common coin stream

101010101010101010101010101010101010101010111010101010001010111010100101010101011

All participants Vote 1/0 for a block part for finished/unfinished
Repeating voting until the majority vote value equals a common random coin
- Producing coins
  Utilizing a secret sharing scheme

- Deciding each block part
  Utilizing a common coin stream

All participants Vote 1/0 for a block part for finished/unfinished
Repeating voting until the majority vote value equals a common random coin
When we offer the blockchain service, we also generate continuous fresh coins utilizing the blockchain service simultaneously.
Refusing quantum-sensitive cryptograph tools like RSA or ECDSA.

Deploying some symmetric scheme like AES encryption and SHA hash function. Making the security parameter satisfy (believed) quantum-safety.

Deploying perfectly information-theoretical secure secret sharing scheme, which is proved quantum-safety.

A one-degree polynomial (a line): 2 points can interpolate the polynomial/the line; but only 1 point has no information about the secret.
Our prototype LAN Performance:
- LAN: in the same region, Switzerland, Europe.
- Node: 4 Google Cloud standard VM instances, 2 CPUs, 8GB memory
- Performance: around 175,000 TPS, around 2.5x faster than the peak Visa (65,000 TPS)
Our prototype **WAN** Performance:

- **WAN**: 4 VM instances are arranged in four continents: Japan, Australia, the USA and the UK.
- **Node**: 4 Google Cloud **standard** VM instances, 2 CPUs, 8GB memory
- **Performance**: around **21,000 TPS**, faster than all current asynchronous blockchains.
- **Could be faster** like the LAN setting in better bandwidth.
What we can do more by SodsBC

SodsBC has good throughput => we support massive data, not only transactions...

Massive data can also be ordered/agreed in the blockchain
The on-chain data: not just transaction
Opportunities
These value opportunities are reflected in the fact that approximately **90 percent** of major Australian, European, and North American banks are already experimenting or investing in blockchain.
Supporting more vertical applications

- Food-related agriculture and retail.

- Health care insurance and other useful blockchain tool to trace patients in the corona era.

(Recent the second wave of corona in Beijing, scientists find virus from the mouth of the imported frozen salmon...)

Mckinsey

=> How to protect privacy?
The large need for blockchain vertical applications

Even if we have SodsBC as an efficient blockchain consensus engine, the current blockchain automation is not good enough to support these functionalities.

i.e., we want more functional smart contracts (fewer bugs) and protect more privacy.
FSM based Anonymous and Private Quantum-safe Smart Contracts

Shlomi Dolev
Ziyu Wang
Motivation

Automotive transaction system

- Lots of deployed contracts have **bugs** since the programmer does not pay attention to the logic, especially the state transition.
- We want to achieve **the full privacy protection** for contracts, including the user **anonymity**, the **data** privacy and the **business logic** privacy.
Public Ethereum contracts

Contract detail

**Business logic:**
Alice, Bob and Carol want to do a blind/sealed auction

**Input bids:**
Alice $60
Bob $40
Carol $50

The contract details are public to all blockchain observers
SodsMPC contracts

**Contract detail**

**Business logic:**
Alice, Bob and Carol want to do a blind/sealed auction

**Input bids:**
- Alice $60
- Bob $40
- Carol $50

We can do:
- Except themselves, no one knows Alice, Bob and Carol are doing what **business logic**.
- Except themselves, no one knows Alice, Bob and Carol join an auction (user **anonymity**)
- Except him/herself, no one knows the bid values of Alice, Bob and Carol (**data privacy**)

We protect the business logic and data privacy and anonymity simultaneously.
SodsMPC contracts

We do:

✓ MPC for mixing, to break the linkage of inputs/outputs for user anonymity

✓ Blind polynomial based MPC to achieve the business logic and data privacy at the same time.

Alice $100 → $100
Bob  $100 → $100
Carol $100 → $100
SodsMPC contracts

✓ We only expose two transactions in the blockchain.
✓ The only known fact is that a $60 payment from an unknown payer has been paid to the seller
Summary: Sods Blockchain family/suite

- **SodsBC**: the **high performance consensus** engine
  - The algorithm has passed the peer review.
  - The prototype has been tested in different cloud virtual machines all over the world, which shows competitive performance.

- **SodsMPC**: the **full privacy-protection contract** system
  - The paper is reviewing by peers.
  - The MPC mixing prototype has been tested, and we are developing more contract functionalities.

- **SodsZKP**: to be continue ...

  Everything is quantum-safe!
Thank you

Contact Info

Shlomi Dolev
dolev@cs.bgu.ac.il
nhsa@post.bgu.ac.il

Ziyu Wang
ziyu@post.bgu.ac.il
Drones’ Cryptanalysis

Ben Nassi ¹
Prof. Adi Shamir ²

Raz Ben-Netanel ¹
Prof. Yuval Elovici ¹

¹ Ben-Gurion University of the Negev
² Weizmann Institute of Science
About the Research

1) This research was selected by Globes as the biggest discovery made by Israeli university in Israel at September 2018.

2) The research was presented on 41th IEEE Symposium on Security and Privacy and RSA Conference APJ 2019.

3) The research was ranked in the third place at a contest made by IBM of applied security research.

4) Two patents were submitted by BGN on this research.
Agenda

1) Motivation
GOOD NEWS EVERYONE

YOU ARE ABOUT TO GET YOUR PIZZA DELIVERY MUCH MORE FASTER
Drones Adoptions Rates Increase Around the World

• **Drones Adoption**
  Business around the world started to adopt drones for various purposes (e.g., deliveries).

• **“Open Skies” Policy**
  Regulations are being changed for allowing drones to fly in populated areas (adopting an “Open Skies” Policy in cities).
Drones Created a New Threat to Privacy

Not in my backyard! Woman throws stones before using a GUN to get rid of nosy neighbour's drone

Spouses are using DRONES to catch their cheating partners

Kentucky Man Arrested After Shooting Down Neighbor’s Drone

Eyes In The Sky: The Public Has Privacy Concerns About Drones

Are Drones Spying on Miley Cyrus and Selena Gomez?

The drones among us: Reports of drone-related incidents are going up and up and up

Drone complaints soar as concerns grow over snooping
Research Question

In an "Open Skies" era in which drones can fly between us, a new challenge arises: how can we determine whether a drone that is passing near a house is being used by its operator for a legitimate purpose (e.g., delivering pizza) or an illegitimate purpose (e.g., spying on an organization)?
Geofencing Methods for Drone Detection

These methods are able to detect the presence of nearby drones.
Geofencing Methods for Drone Detection

Methods for Detecting the presence of a drone in an “Open Skies” era are irrelevant because:

1. The presence of drones is no longer restricted in populated areas.
2. The difference between legitimate use of a drone and illegitimate use depends on the drone’s camera orientation rather than on the drone’s location.

Conclusion: Geofencing methods are irrelevant for detecting a privacy invasion attack in an “Open Skies” era.
Objective

Main Objective: Detecting a privacy invasion attack.

- Classifying a suspicious radio transmission as an FPV channel.
- Detecting an FPV channel’s quality (FPS and resolution).
- Detecting whether the FPV channel is being used to spy after a victim (even if the victim is not static).
- Locating the spying drone in space.
- Detecting a privacy invasion attack without revealing it to the drones operator.
Agenda

1) Motivation
2) Detection Scheme
Assumptions:
1) The attacker is using Wi-Fi FPV drone (located in a range of up to 5 KM from the victim)
2) The Spying Detection Mechanism connected to an RF scanner with a proper antenna for intercepting suspicious radio transmissions.
Agenda

1) Motivation
2) Detection Scheme
3) Wi-Fi FPV
**First Person View Channel**

**First Person View (FPV) Channel** - a communication channel designed to:

1. Stream the video captured by the drone’s video camera to the operator’s controller.
2. Maneuver the drone.
Wi-Fi FPV Channel

1. Distance up to 5 KM (FCC compliance)
2. Most commonly-used type of FPV, because it eliminates the need to develop a dedicated controller (any devices with a Wi-Fi NIC can be used as controller)
3. Examples for Wi-Fi FPV drones:

   DJI – Mavic Air
   DJI Spark
   DJI Mavic Pro
   Parrot – Bebop 2
   GoPro – Karma

OSI Model - DJI Spark

<table>
<thead>
<tr>
<th>Layer 1 - Physical</th>
<th>IEEE 802.11</th>
</tr>
</thead>
<tbody>
<tr>
<td>Layer 2 - Data Link</td>
<td>IPv4</td>
</tr>
<tr>
<td>Layer 3 - IP</td>
<td>RTP</td>
</tr>
<tr>
<td>Layer 4 - Transport</td>
<td>UDP</td>
</tr>
<tr>
<td>Layer 5 - Session</td>
<td></td>
</tr>
<tr>
<td>Layer 6 - Presentation</td>
<td>Linux</td>
</tr>
<tr>
<td>Layer 7 - Application</td>
<td></td>
</tr>
</tbody>
</table>
Downlink - Video Streaming Channel

Video stream is encrypted.
Does it really make the FPV channel confidential?
Interception of FPV Stream

Given a suspicious Wi-Fi transmission we create an \textit{intercepted bitrate signal}:

1) Sniffing Wi-Fi Packets
   - Enabling NIC’s monitoring mode (attack mode)
   - Sniffing a network using \texttt{Airmon}

2) Extracting a time series signal from unencrypted metadata (2\textsuperscript{nd} layer)
   - Packet length (\texttt{frame.len})
   - Packet arrival time (\texttt{frame.number})

3) Equalizing the amount of samples in every second (by aggregating samples in a fixed window)
Agenda

1) Motivation
2) Detection Scheme
3) Wi-Fi FPV
4) **FPV Channel Classification**
Classifying Suspicious Transmission as FPV Channel

Key Observation: Drone is a flying camera.

Moving Device Detection

Camera Detection
Classifying Suspicious Transmission as FPV Channel

Camera Detection

1) Analyzing the intercepted bitrate signal in the frequency domain.
2) Finding the frequency with the maximum magnitude.
3) Compare the frequency with the maximum magnitude to known FPS of drones {24,25,30,60,96,120}. 
Classifying Suspicious Transmission as FPV Channel

Moving Object Detection

1) Analyzing received signal strength indication measurements for a given device (MAC) over time.
2) Determining that a device is on the move according to measurements change.
Classifying Suspicious Transmission as FPV Channel

We can determine whether a suspicious radio transmission is an FPV channel within 4 seconds with accuracy of 99.9%.

Algorithm 2 Classification of an FPV Channel

1: procedure isFPVChannel?(network, time)
2:     frequency = 70
3:     for (macAddress : network) do
4:         // Detecting Moving Objects
5:         if (isMovingObject(macAddress)) then
6:             bitrate[] = extractBitRateSignal(macAddress)
7:             fft [] = FFT(bitrateArray, frequency)
8:             index = frequencyWithStrongestMagnitude(fft)
9:             // Detecting video channel
10:            if (index == 24 || index == 25 || index == 30) then
11:                return true
12:     return false

We can determine whether a suspicious radio transmission is an FPV channel within 4 seconds with accuracy of 99.9%.
Detecting FPS and Resolution

FPV channel (bits per second) =
Drone to controller traffic (BPS) + Controller to drone traffic (BPS) =

Video stream + Metadata about the transmission + Maneuvering commands + Transmission’s metadata =

Video stream + O(c) =
FPS x Resolution (Delta resolution) + O(c).

Resolution = \frac{FPV \ Channel \ (\text{Bits Per Second})}{FPS}

By applying FFT to intercepted bitrate signal of FPV channel we can detect FPS and use it to calculate the Resolution by analyzing the bitrate per second.
Agenda

1) Motivation
2) Detection Scheme
3) Wi-Fi FPV and Video Compression
4) FPV Channel Classification
5) Detecting whether an FPV channel is being used to spy after a victim
Video Compression Stage

- Optical Sensor Capturing
- Binary Representation
- Video Encoder
- Encryption
- Modulation

Downlink - Video Streaming

H.264 Standards
H.264 Compression Standards

Motion compensation algorithm

Instead of sending an entire frame, a frame is described as delta (changes) from another frame and this information is sent.

- Self Contained Frames (I-Frames)
- Delta Frames (B-Frames and P-Frames)
- Data is sent in a group of picture structure

The result: If there are a lot of changes between two consecutive frames, a lot of data needs to be encoded so the delta frames are much bigger comparing delta frames of two similar consecutive frames.
Influence of Periodic Physical Stimulus on the Frequency Domain

Key Observation: a 3 Hz flickering LED created 6 bursts in the intercepted bitrate signal.
Watermarking a Target Frequency

1. Detecting whether a specific POI is being streamed from FPV channel by:
   - Launching a flicker with a frequency $f$.
   - Testing the change of magnitude of frequency $2f$ of the intercepted bitrate signal in the frequency domain.

2. Frequency of maximum physical stimulus is limited to 12 Hz (because minimal FPS rate of commercial drone is 24 Hz)

We can watermark each and every frequency of the intercepted bitrate signal using a flickering LED.
Evaluation

Video – Detecting a drone that is spying after a person while driving in his car

Video – Detecting a drone that is spying after a person in a house
Results

siren turned on

Smart film flickers

Smart film flickers
Agenda

1) Motivation
2) Detection Scheme
3) Wi-Fi FPV and Video Compression
4) FPV Channel Classification
5) Detecting whether an FPV channel is being used to spy after a victim
6) **Locating a spying drone in space**
Detect the angle between the Drone and the Target
Detect the angle between the Drone and the Target

\[ \text{Angle}(SNR1, SNR2) = 192.72 \times e^{-0.71 \times \frac{SNR2}{SNR1}} \] (8)
Detect the distance between the Drone and the Target

\[ \% \text{ Changing Pixels (SNR}=s) = 1.12 - 3.14 \times 10^{-7} s^4 + 6.96 \times 10^{-5} s^3 - 5.12 \times 10^{-3} s^2 + 1.87 \times 10^{-1} s \]
Detect the distance between the Drone and the Target

1) Determining the FPV resolution of the FPV channel and finding the image’s height.
2) Triggering a physical stimulus using a square flickering (size of at height x height) a specific frequency (e.g., 3 Hz).
3) Calculating the percentage of changing pixels from the intercepted bitrate signal using the formula.
4) Inferring the amount of changing pixels from the FPV resolution.
5) Inferring object’s height and width (in terms of pixels) of the flickering object in a frame.
6) Calculating the distance between the drone to the object using dedicated calculators that takes as input:
   - Real Object Height (LED Board)
   - Image Height
   - Object’s Height in pixels (calculated from the formula)
Locating drones in space

1. Calculating Spherical coordinates \((\theta, \varphi, r)\):
   • \(\theta\) and \(\varphi\) - using the formula to detect angle.
   • \(r\) - using the formula to detect distance.

2. Calculating spying drone’s location (longitude, latitude, altitude) from the spherical coordinates \((\theta, \varphi, r)\):
   \[
   x = r \sin(\theta) \cos(\varphi) \\
   y = r \sin(\theta) \sin(\varphi) \\
   z = r \cos(\theta)
   \]
Locating drones in space
Results
Agenda

1) Motivation
2) Detection Scheme
3) Wi-Fi FPV and Video Compression
4) FPV Channel Classification
5) Detecting whether an FPV channel is being used to spy after a victim
6) Locating a spying drone in space
7) Hiding the flicker from the drone operator
Hiding the Physical Stimulus

Objective – Applying the physical stimulus invisibly.

Requirements:
1. Undetectable by direct observation by the drone’s operator
2. Undetectable by indirect observation by via the drone’s controller
3. Watermark the FPV channel
Optional Methods For Hiding the Physical Stimulus

1. Using an infrared projector
   a) Undetectable by direct observation ✓
   b) Undetectable via the controller ✗
   c) Watermark ✓

2. Applying the physical stimulus to a period of time that is below the eye’s perception (e.g., 10 milliseconds)
   a) Undetectable by direct observation ✓
   b) Undetectable via the controller ✗
   c) Watermark ✓
Hiding the Physical Stimulus

3. Flickering between two similar hues
   a) Undetectable by direct observation ✓
   b) Undetectable by indirect observation ✓
   c) Watermark ✓
Analysis of influence of ambient factors

1. It is better to watermark the frequencies in the range of 6-12 Hz since the frequencies between 1-6 Hz are more noisier.
2. A combination of LED strip and a smart film can provide a solution for detecting a drone during an entire day.
Agenda

1) Motivation
2) Detection Scheme
3) Wi-Fi FPV and Video Compression
4) FPV Channel Classification
5) Detecting whether an FPV channel is being used to spy after a victim
6) Locating a spying drone in space
7) Hiding the flicker from the drone operator
My Twitter: @ben_nassi
My Website: https://www.nassiben.com/
Cyber@BGU - https://cyber.bgu.ac.il/

Questions?
LEVERAGING DEEP LEARNING TO AUTOMATE DEVICES CONNECTIVITY TO ANY PLATFORM

Removing the pain of connecting IIoT devices
MARKET AND OPPORTUNITY

Worldwide installed base of IoT endpoints will grow from nearly 15 billion in 2016 to more than 34 billion by 2025.

The software services market for connecting industrial end-users to the cloud is estimated at $55 billion a year.

Despite the forward momentum, 60% of IoT initiatives stall at the proof of concept stages.

The challenges:
- Lack of standardization
- Huge variety of communication protocols and data formats
- Limited internal expertise
- Range from time to completion

$55 billion

60%
The Challenge

- Lack of standardization
- Huge variety of communication protocols and data formats
  - 50+ Communication protocols
  - Infinite Data formats
- Limited internal expertise
  - Objrct Oriented Programming
  - IoT and Cloud
  - Web Development
  - Network & Communication
  - Security
- Range from time to completion
  - Average Time: 6 months
CURRENT SOLUTIONS

Physical IoT gateways
- Requires the installation of a costly hardware component
- Device specific adaptors
- Manually written Repository of adaptors

Device specific adaptors
- Manually written repository of adaptors

SUPPORT LIMITED PRE DEFINED SET OF DEVICES
Different Stream of Data

Siraj Generic Gateway that Supports Previously Un-observed Devices

Data Consumer / Cloud Platforms

Unified Format
ADVANTAGES

- Quickly and easily adds new data point
- Reduce cost of implementation
- Dramatically reduces implementation time for IoT solutions
- Simplify and speed scalability

Get the freedom to easily connect any device to any platform and expand IoT solution capabilities
THE TEAM

MANAGEMENT TEAM

Othman Alshekh, Co-CEO
Accountant and lawyer. He worked as Senior advisor on KPMG’s Deal advisory and Management consulting team. He completed his internship in Goldfarb Zeligman’s Capital Markets Department. Further, Mr. Alshekh worked on Procter & Gamble’s finance team.

Yussif Alsanha, Co-CEO
Over ten years’ experience in software development and leadership in hi-tech companies. Prior to joining Siraj, Mr. Alsanah served as Director of Software at Allied Telesis Wireless, where he led three software development teams.

MEMBERS OF THE BOARD

Dr. Giora Yaron, Board Chairman
Ph.D. in Applied Physics, High tech entrepreneur.

Prof Jihad El-Sana, Board Member
Ph.D. in Computer Science from Stony Brook University. Head of the Computer Science Department at Ben Gurion University.

Dr. Sara Abu Kaf, Board Member
Doctor of Psychology at Ben Gurion University. Post Doc, Harvard University.

Mr. Hadar Alshekh, Board Member
Businessman and leading business entrepreneur in the Bedouin society.

Mrs. Smadar Nehab, Board Member
Ms. Nehab is an experienced hi-tech executive and entrepreneur.

Othman Alshekh, Co-CEO

Siraj Technologies Ltd. Proprietary
MILESTONES

- Completed POC
- Tested it at Alpha customer
- Working on reach GA
- Awarded a R&D investment from Israeli Innovation Authority for the second year
- Extensive experience in the field of IIoT

AMONG OUR CUSTOMERS AND PARTNERS

- GE Digital
- RAD
- HAM-LET
- Netafim
- mPrest
- e.on
- Israel Innovation Authority
- AICL
- P&G
THANK YOU
FOUNDERS

Prof. Offer Hadar

Yoram Segal

Raz Birman
THE NEED

- Our lives evolve around body movements and facial expressions, engaging with healthy sports to improve quality of life, physiotherapeutic healing, sign language communication, lip reading, and body language are just a few examples.
- Body motion tagging from video, which is captured with a simple home setup, requiring a single smartphone camera, holds a large promise for a wide variety of applications in the fields of remote physiotherapy, professional sports, accessibility for the people with disabilities (deaf and/or mute), video compression, etc.
- Being able to display avatars that mimic the exact same movement of a human model can be designed to perform different tasks within the potential target applications spectrum.
Physiotherapists can find it beneficial to train a robot and/or an avatar, which will provide direct guidance to patients about the quality, quantity, frequency and duration of exercises. The same apparatus can also provide immediate feedback and significantly
SPORT

- Sports trainers will be able to analyse the exact accurate movements of professional athletes in different fields such as Gymnastics, Tennis, Swimming, etc. Evaluating training quality will improve training efficiency of professionals.
SMART HOME GESTURES

- Adaptive environment that changes according to body movements. May be used to trigger notifications on person falling or on detecting violence. May also be used to adjust room lighting and multi-media settings when homeowner falls asleep.
AUTONOMOUS CAR GESTURES

- Autonomous car may be able to detect people waiting in stations and make stopping decisions accordingly.
Autonomous car may be able to detect people waiting in stations and make stopping decisions accordingly.
HUMAN POSE ESTIMATION

1. Right_Shoulder
2. Right_Elbow
3. Right_Wrist
4. Left_Shoulder
5. Left_Elbow
6. Left_Wrist
7. Right_Hip
8. Right_Knee
9. Right_Ankle
10. Left_Hip
11. Left_Knee
12. Left_Ankle
13. Head
14. Neck
15. Spine
16. Pelvis
## Training Datasets

<table>
<thead>
<tr>
<th>Dataset</th>
<th>Single person</th>
<th>Multi-person</th>
<th>Num of Kpts</th>
<th>Num of Person</th>
</tr>
</thead>
<tbody>
<tr>
<td>LSP</td>
<td>Y</td>
<td>N</td>
<td>14</td>
<td>~2K</td>
</tr>
<tr>
<td>FLIC</td>
<td>Y</td>
<td>N</td>
<td>9</td>
<td>~20K</td>
</tr>
<tr>
<td>MPII</td>
<td>Y</td>
<td>Y</td>
<td>16</td>
<td>~25K</td>
</tr>
<tr>
<td><strong>COCO</strong></td>
<td>N</td>
<td>Y</td>
<td>17</td>
<td>~100K</td>
</tr>
<tr>
<td>AI Challenger</td>
<td>N</td>
<td>Y</td>
<td>14</td>
<td>~700K</td>
</tr>
<tr>
<td>PoseTrack</td>
<td>N</td>
<td>Y</td>
<td>15</td>
<td>~160K</td>
</tr>
</tbody>
</table>
The system calculates 17 joint angles per frame from the estimated skeleton information. The joint angles are decomposed into two dimensions of $\theta_x$ and $\theta_y$. 
The system calculates a difference $v\Delta \theta$ from $v\theta$ of one frame before and calculates a difference $v\Delta \Delta \theta$ from the previous $v\Delta \theta$. Then, the system concatenates them and make it 102-dimensional feature vector $v_\alpha$. 
The system calculates the Euclidean distance between all frames of the input video and all frames of all video in the database and divides it by the total number of combinations. That value is defined as $R_\alpha$. 
THE SOLUTION

- Rdaka fundamental Intellectual Property will be a pose dictionary engine that translates movement into labels such as Plier & Relever in ballet, Dunk Shot in basketball, Abduction Exercises for Strength Training, Volley in Soccer and others.

We plan to design and build an algorithmic engine that will detect, classify and tag human body poses, Facial expressions and Lip movements by analysing human joints movements extracted from videos captured with a regular smartphone in non-controlled environments.

| Convert body movement, lips and expressions to text and vice versa | Proper body movement training | Visual remote Microphone | Real-Time implementation | Remote sensing without physical contact |
THANKS
SocPro
Social Protector for Online Social Networks

Nadav Voloch, Ehud Gudes, Danny Hendler

Collaborators:
Omer Sella, Sagiv Mapgavker, Alexander Chinyan, Hagai Ortner, Nurit Gal-Oz
Intro- Social Network data privacy

• During the last years social network privacy issues has been a major concern for users and organizations.

• Cambridge Analytica scandal: data harvesting, personal data trading for political purposes and election interference.
Goal – personal data privacy with free secure connections

- We wish to maintain our personal freedom in the network.
- But we also wish our data will remain secure and will not get to unwanted entities.
- This can be done by a third party software app that identifies potential network hazards, in a user-adapted context.
Current status in Social networks

• Social networks today (Facebook, Twitter, Instagram, etc.) use widely common security preferences.

• The privacy settings are either:
  1. Administrator settings based on reports and other methods.
  2. Dependent on user preferences – need user action.
Most of the users are unaware of their privacy settings.
THE SOCIAL PROBLEM - MOTIVATION

• Information is posted and shared by individuals and organizations in social networks in huge quantities.

• Part of this information is very sensitive and access to it should be better controlled.

• Most users are not aware of their privacy settings, which usually remains in its default state.
We use efficient graph algorithms for that purpose.

SocPro – personal adaptive solution

- Mapping the user’s personal network and giving Trust scores to his friends and their friends (networks).

- We use efficient graph algorithms for that purpose.
Applicative method – identifying weak links

• Identifying problematic users and connections by their attributes
• Today: based on reports, image and text analysis
• Our method: using deeper analysis of the network
Our model – Trust Criteria

• Trust is computed for the user which tries to get access
• The two main criteria for determining the level of trust are:
  • **Connection strength** \((c)\): the connection strength of users is determined by characteristics that indicate their level of closeness such as Friendship Duration (FD), Mutual Friends (MF), etc.
  • **User credibility** \((u)\): the user credibly criterion assesses the user attributes that convey his OSN reputation and trustworthiness, such as Total number of Friends (TF) and Age of User Account (AUA), calculated from the time the user joined the OSN, etc.
Third party Social Network applications exist today but mostly for marketing and traffic boosters. No apps for personal user benefits and privacy.
Third party Social Network application- abilities

• The actual manifestation of the model is done by enforcing the Access Control and Flow control aspects of it on the user’s network.

• This is done according to the social network policies and ethics and by the user’s consent.

• Filtering and Targeting options in social media exists today partially and for different purposes.
Business model

• Today users do not benefit from the third-party use of their personal data.

• The users can buy the app to have a real friend network in which all data is safe.

• The users can decide giving their social data to marketing companies or other interested sides for payment.

• From this exchange the app gets a commission by percentage.
• An important use case for the product is the identification of Fake News.

• The future development of the product can categorize data, and by Trust estimation can prevent harmful and wrong data from spreading.

• This is a very important feature for commercial companies, politicians (in sponsored advertisement via social media), etc.
The basic comprehensive trust model that involves Access and Flow control.

Experimental result that verify the model’s viability.

Theoretical aspects of the research published in a couple of papers (in the next slide).
Our published papers on the model


Current status – Implementation

• Working prototype that can be used on personal networks for Twitter and Facebook.

• The prototype uses a very soft crawler that adheres with the OSN policies and does not violate any ethical or legal aspects.

• Video – next slide.
Prototype simulation video
Development – First year

1. Context identification by Natural Language Processing (NLP) – with Python libraries of GoogleTranslate and VaderSentiment – **Prototype for this part exists- we will now see the demo.**

2. Machine learning for user’s behavior analysis – with Python libraries such as NumPy and PyTorch.

3. Full adaptive intertwined add-on.
Development – Second year

4. Modular software for all platforms (Social Networks).

5. Public exposure and Web platform for wide range use (alpha version release).

6. Adapting the software for Mobile.
Thank you for listening.

Questions?