Security
in
Dynamically Changing Systems

Dr. Sevil Şen
ssen@cs.hacettepe.edu.tr

CHIST-ERA Conference, May 2022

My talk today

About our group

Dynamically changing systems

- Ad hoc networks
- IoT

Security issues in dynamic systems

Transfer learning approach for security

- generating suitable intrusion algorithms for new devices
- detecting new types of attacks

wise

Wireless Networks and Intelligent Secure Systems

Cyber Security
Malware analysis
Intrusion detection
Trust management

Intelligent Systems
ML
Evolutionary computation
Applications on security

Wireless Networks/ IoT
Routing
Load balancing
Security

Follow @huWISElab

https://wise.cs.hacettepe.edu.tr/

dynamically changing systems

- Systems that are dynamic by their very nature due to mobility
  - Ad hoc networks
  - Vehicular ad hoc networks (VANETs)
  - Flying ad hoc networks (FANETs)
  - Internet of Things

- Systems evolving every day
  - Emergence of new attacks

- Heterogoneous Systems
  - Nodes with different computation and communication capabilities

security issues in dynamic systems

Mobility

- Hard to differentiate normal behaviour of the system from anomaly/malicious behaviour.
- Cannot rely on physical protection.
- Security architecture might change as well.

Heterogoneity / Resource-Constraints

- A solution developed for a particular type of device might not be suitable for other types of devices.
- Developing a solution for each device is a costly approach.

New types of attacks

- With the increasing popularity of distributed systems, we expect new attacks to emerge.

ml-based solutions

- In order to explore the complex characteristics of systems, machine learning methods, which rely on long training time, are usually proposed in the literature.

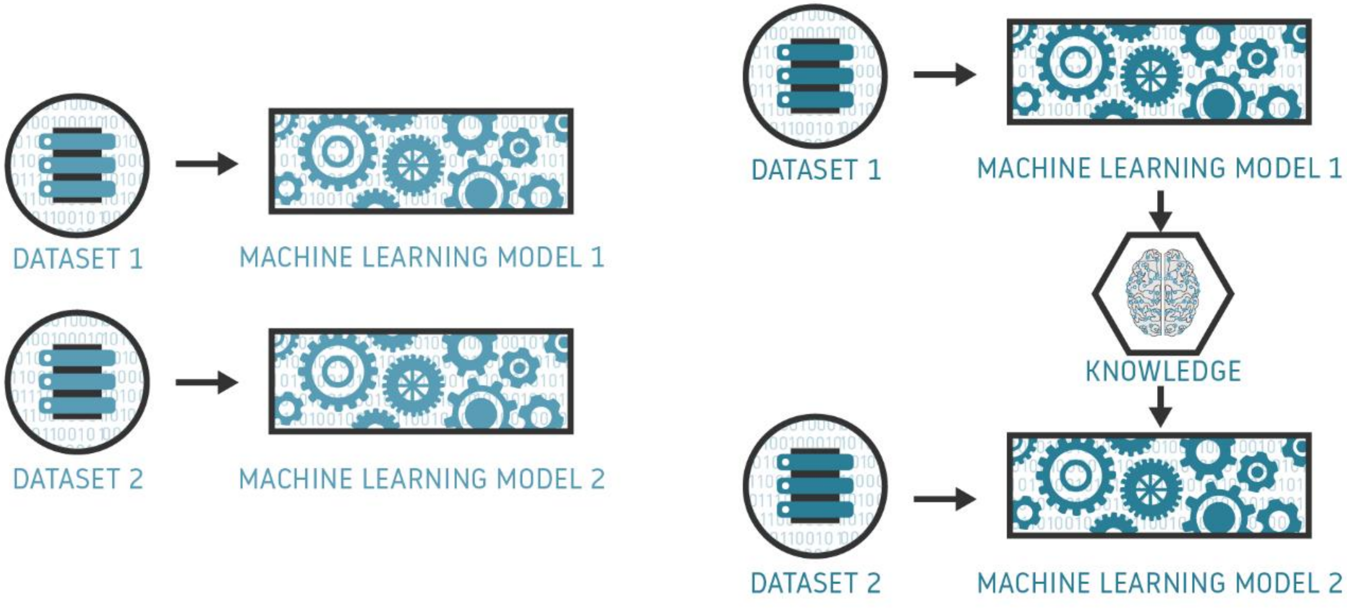
- However these systems need to learn a new model when the environment changes.

- Adapting to changes & developing effective security solutions in a timely-manner is crucial for some systems.

transfer learning in security

Trasfer learning helps move the knowledge learned in a task/domain to a new task/domain.

- reduce the learning time needed in in the new task/domain.
- produce higher initial and final performance for the learned model in the new task/domain compared to learning without transfer.



https://datascience.aero/transfer-learning-aviation/

transfer learning approach for IoT Security

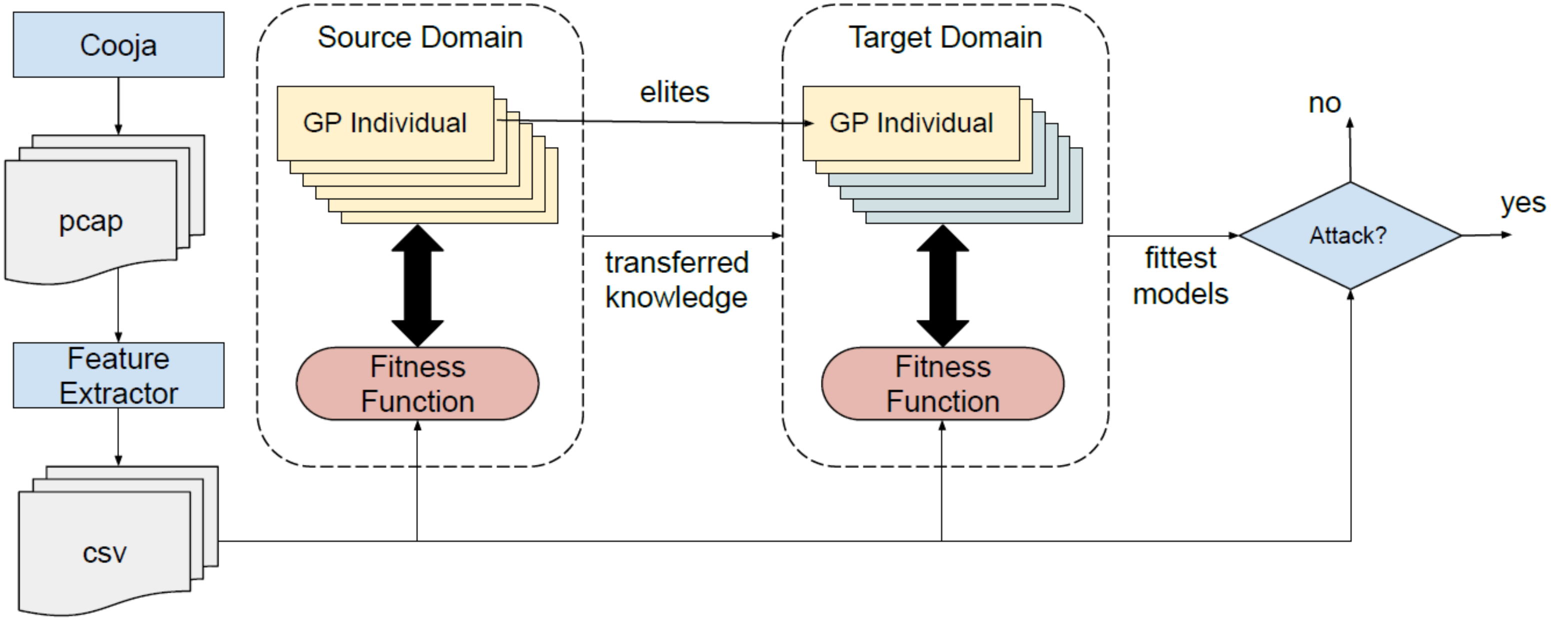
IoT security has attracted significant interest by researchers due to new characteristics:

- heterogeneity of devices
- resource constraints
- new attacks

Transfer learning is employed in the following two settings:

1. Transferring knowledge for generating suitable intrusion algorithms for new devices.
2. Transferring knowledge for detecting new types of attacks.

transfer learning approach for IoT Security



The proposed approach

- Produces more effective solutions than the traditional approach.
- Significantly reduces learning time, which is an important factor for putting devices/networks in operation in a timely manner.

the work I am presenting..

The talk I am giving today appeared at

IEEE Transactions on Information Forensics and Security, 2021.

In case you’d like to read the full paper:

Yılmaz, S., Aydogan, E., & Sen, S. (2021). A Transfer Learning Approach for Securing Resource-Constrained IoT Devices. *IEEE Transactions on Information Forensics and Security*, *16*, 4405-4418.

conclusion

Many systems are dynamically changing in time by their very nature.

Dynamicity introduces complexity to such systems.

Ml-based solutions are promising for discovering such complex properties of systems.

Transfer learning-based solutions could help these systems adapt to changes in a timely manner.