



ECCO Community Group on Trusted Supply Chains

Knowledge-Sharing Webinar

**Strengthening Trusted Supply Chains: Real-Time Attack
Detection and Critical Dependency Analysis**

November 15th 2024

- Welcome & Introduction by Community Group Chairs (5 min)
- Real-Time Attack Detection and Mitigation: Measurement, Optimization on Real Systems – Prof. Erol Gelenbe (20 min)
- Supply Chain Triage: Identifying Weak Points and Critical Dependencies - Michael Herburger (20 min)
- Q&A (15 min)



ECCO Community Group on Trusted Supply Chains

Introduction

November 15th 2024

- Road-mapping
- Startups/Scaleups - SMEs support
- Human factors
- Skills
- Synergies on cybersecurity for Civilian and Space applications
- **Trusted supply chains**
 - **Chairs: Antonio Skarmeta and José Luis Hernández Ramos**
 - Participants: development of a “proto-community” based on the initial list of experts from ECSO and Pilots, and growing with additional people (44 members so far)
 - Objectives and results
 - Build community of experts on trusted supply chains and Strengthening Trusted and Resilient Supply Chain in Europe
 - Facilitate trusted information sharing about threats (to support prevention and response)
 - Propose a strategy, planning and recommendations to support the NCCs in the implementation of the Strategic Agenda’s Action Plan

Strengthening Trusted Supply Chains: Real-Time Attack Detection and Critical Dependency Analysis

- Webinar today focused on:
 - Strengthening supply chain security through real-time threat detection and mitigation
 - Identifying and addressing weak points and critical dependencies within supply chains
 - Practical strategies to enhance resilience against evolving cyber threats

- This event is part of a webinar series focused on European cybersecurity supply chain.
- List of webinars
 - Organizational and Operation Security in Trusted Supply Chains (March 19th)
 - Certification in the Lifecycle (May 7th)
 - Enhancing Supply Chain Security: Strategies, Case Studies, and Roadmapping (June 14th)
 - Paradigm shift from cybersecurity to cyber resilience (July 22nd)
 - Strengthening Trusted Supply Chains: Real-Time Attack Detection and Critical Dependency Analysis (today)
 - Securing supply chains: an overview on challenges and regulatory initiatives (November 21st)



E. Gelenbe, Y. Yin, Deep Learning with Random Neural Networks, IEEE 2016 International Joint Conference on Neural Networks (IJCNN), pp; 1633-1638, IEEEExplore.

E. Gelenbe, M. Nakip: IoT Network Cybersecurity Assessment With the Associated Random Neural Network. *IEEE Access* 11: 85501-85512 (2023)

E. Gelenbe, M. Nasereddin: Protecting IoT Servers Against Flood Attacks with the Quasi Deterministic Transmission Policy. *IEEE TrustCom 2023*: 379-386 (Best Paper Award)

J. Bergquist, E. Gelenbe, and K. Sigman, "On an Adaptive-Quasi-Deterministic Transmission Policy Queueing Model", 32nd IEEE MASCOTS'24 Conference on Modeling, Analysis and Simulation of Computer and Telecommunication Systems, October 21-23, 2024, Krakow, IEEEExplore, 2024.

E. Gelenbe, M. Nakip, and M. Siavvas, "System-Wide Vulnerability and Trust in Multi-Component Communication System Software", *IEEE Network*, Early Access, 2024.

E. Gelenbe, B. Can Gül, and M. Nakip, "DISFIDA: Distributed Self-Supervised Federated Intrusion Detection Algorithm with Online Learning for Health Internet of Things and Internet of Vehicles," , *Internet of Things*, vol. 28, 12/2024.

E. Gelenbe, M. Nakip, and M. Siavvas, "System-wide vulnerability of multi-component software", *Computers & Industrial Engineering*, 196, 10/2024.

M. Nakip and E. Gelenbe, "Online Self-Supervised Deep Learning for Intrusion Detection Systems", *IEEE Trans. Inf. Forensics and Sec.* , 19, 5668-5683, 05/2024.

IoT Servers/Gateways

Fragile, Vulnerable & Low Power & Low Cost

Low Performance, Easy to Attack & Compromise

May be Compromised by Botnets, DDoS Attacks, Malware

Contain Many Low Cost Devices: Low Computational Power, Factory Initialization

Some Devices May be Battery Operated or Rechargeable/Energy-Renewable

Communications Among the Nodes (e.g. UWB, Ethernet, MAC, ..)

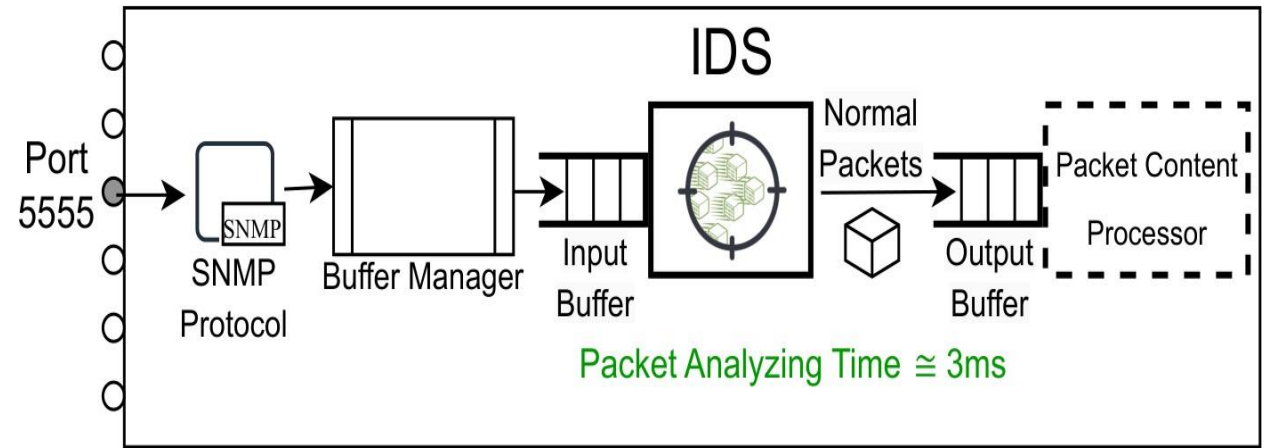
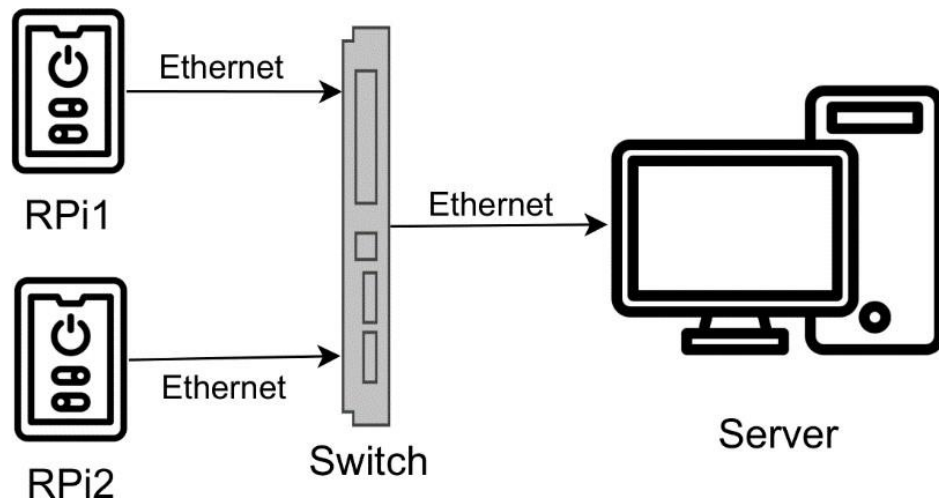
A Combination of IP Nodes, Ethernet, WiFi, UWB

Networks of Devices and Servers that are Difficult to Coordinate and Self-Regulate

Nodes May Transmit Asynchronously, Periodically or Synchronously

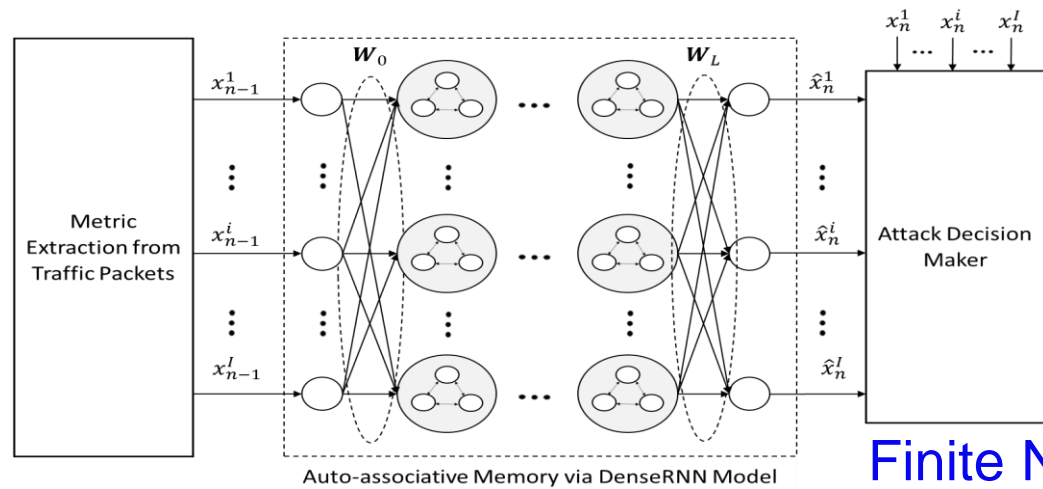
Multi-Core Servers and NUCs Typically used as Gateways & Servers

Measurements at a Server/Gateway Protected by Intrusion Detection System (IDS)



- Normally operating (uncompromised) RPi's periodically send UDP packets containing the measurements of the temperature of the RPi.
- The Server supports the UDP protocol with SNMP for incoming packets, and operates the IDS that uses an accurate AD algorithm reported in [30], and supports the other normal processing needs of incoming UDP packets.

IDS or AD: Dense Random Neural Network based Auto-associative Attack Detection



The Auto-Associative Dense RNN (AADRNN)

A Multi-Layer Feedforward Architecture

Finite Number of Neuronal Clusters Rather than Single Neurons

Each Cell Contains a Recurrent Network with Infinitely Many Neurons

x_n^i Actual value of Metric for the packet .

\hat{x}_n^i Expected value of Metric for the packet via Dense RNN.

Mathematical Tool — The Random Neural Network

Infinite Discrete State Space & Continuous Time Markov chain

Number of Neurons is n — State of the RNN at time t is a Vector of Natural Numbers

$$K(t) = (K_1(t), \dots, K_i(t), \dots, K_j(t), \dots, K_n(t))$$

$K_i(t) \geq 0$ is the Internal State or Potential of Neuron i

If $K_i(t) > 0$, we say that Neuron i is excited and it may fire at t^+ and send an excitatory spike w.p. p^+_{ij} or an inhibitory spike w.p. p^-_{ij} after an exponentially distributed time of rate r_i

If $K_i(t) = 0$, Neuron i is “quiescent” and cannot fire at t^+

If $K_i(t) > 0$, Neuron i fires: It sends a spike to some other Neuron j , w. p. $p_{ij} = p^+_{ij} + p^-_{ij} \geq 0$

Its state changes $K_i(t^+) = K_i(t) - 1$, and for Neuron j we have

$$K_j(t^+) = K_j(t) + 1 \text{ (excitation) or } K_j(t^+) = [K_j(t) - 1]^+ \text{ (inhibition)}$$

Excitatory and Inhibitory Spikes also arrive from Outside the Network to Neurons



Rates and Weights

If $K_i(t) > 0$, then Neuron i fires with probability $r_i \Delta t + o(\Delta t)$ in the interval $[t, t + \Delta t]$ From Neuron i to Neuron j

Excitatory Weight or Firing Rate is $w_{ij+} = r_i p_{ij+}$

Inhibitory Weight or Firing Rate is $w_{im-} = r_i p_{im-}$

Total Firing Rate is $r_i = \sum_{m=1}^n w_{ij+} + w_{ij-}$

To Any Neuron i , from Outside the Network :

External Excitatory Spikes arrive at rate Λ_i

External Inhibitory Spikes arrive at rate λ_i



Chapman-Kolmogorov Equations

$p(k, t) = \Pr[x(t) = k]$ where $\{x(t): t \geq 0\}$ is a discrete state - space Markov process,

and $k_{ij}^{+-} = k + e_i - e_j$, $k_{ij}^{++} = k + e_i + e_j$

$k_i^+ = k + e_i$, $k_i^- = k - e_i$:

The **Chapman - Kolmogorov** Equations

$$\begin{aligned} \frac{d}{dt} p(k, t) = & \sum_{i,j} [p(k_{ij}^{+-}, t) r_i p_{ij}^+ 1[k_j(t) > 0] + p(k_{ij}^{++}, t) r_i p_{ij}^-] + \sum_i [p(k_i^+, t) (\lambda_i + r_i d_i) + \Lambda_i p(k_i^-, t) 1[k_i(t) > 0]] \\ & - p(k, t) \sum_i [(\lambda_i + r_i) 1[k_i(t) > 0] + \Lambda_i] \end{aligned}$$

Let :

$$p(k) = \lim_{t \rightarrow \infty} \Pr[x(t) = k], \quad \text{and} \quad q_i = \lim_{t \rightarrow \infty} \Pr[x_i(t) > 0]$$

Theorem If the C - K equations have a stationary solution,

then it has the "product - form" $p(k) = \prod_{i=1}^n q_i^{k_i} (1 - q_i)$, where



The Random Neural Network (RNN)

Product Form Solution

$$\lim_{t \rightarrow \infty} \text{Prob}[K_1(t)=k_1, \dots, K_i(t)=k_i, \dots, K_n(t)=k_n]$$

$$= \prod_{i=1}^n q_i^{k_i} (1-q_i)$$



$$0 \leq q_i = \frac{\Lambda_i + \sum_j q_j r_j p_{ji}^+}{r_i + \lambda_i + \sum_j q_j r_j p_{ji}^-} < 1$$

External Arrival Rate of Excitatory Spikes ω_{ji}^-
 Probability that Neuron i is excited Λ_i
 Firing Rate of Neuron i r_i
 External Arrival Rate of Inhibitory Spikes ω_{ji}^+



Theorem (Gelenbe 93, Gelenbe - Schassberger 95)

The system of non-linear equations

$$q_i = \frac{\Lambda_i + \sum_j q_j r_j p_{ji}^+}{r_i + \lambda_i + \sum_j q_j r_j p_{ji}^-}, \quad 1 \leq i \leq n$$

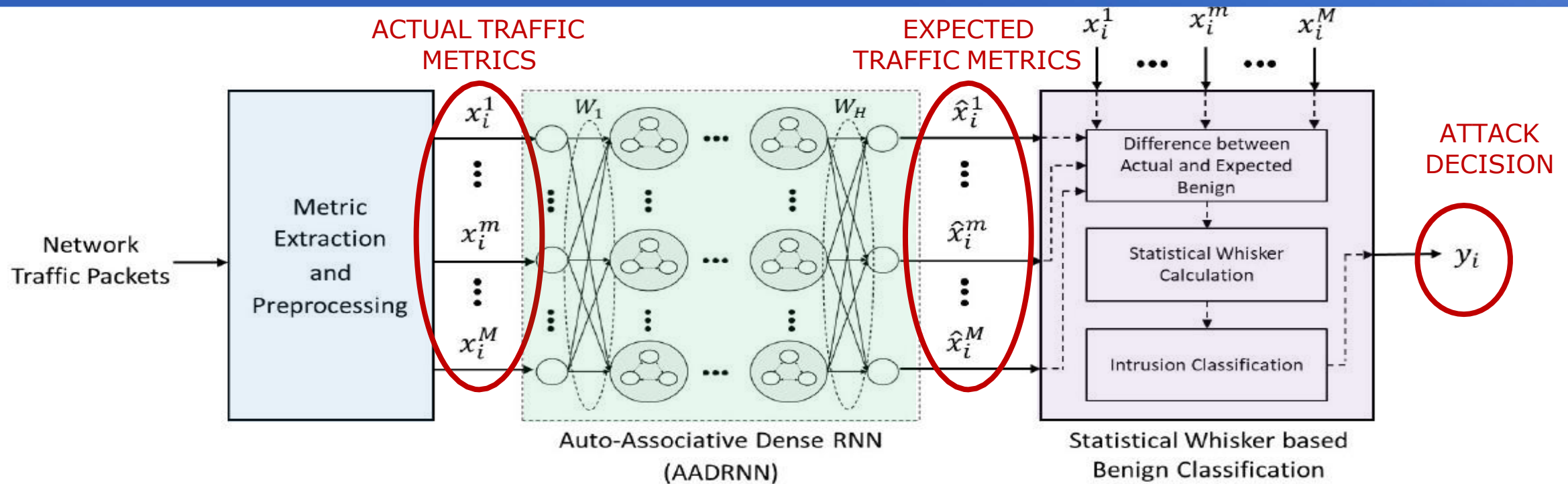
has an unique solution if all the $q_i < 1$.

Theorem (Gelenbe et al. 99) *Let $g : [0,1]^v \rightarrow R$ be continuous and bounded. For any $\varepsilon > 0$, there exists an RNN with two output neurons q_{o+}, q_{o-} s.t.*

$$\sup_{x \in [0,1]^v} |g(x) - y(x)| < \varepsilon \quad \text{for} \quad y(x) = \frac{q_{o+}}{1 - q_{o+}} - \frac{q_{o-}}{1 - q_{o-}}$$



Offline Auto-Associative Learning for Botnet Attack Detection

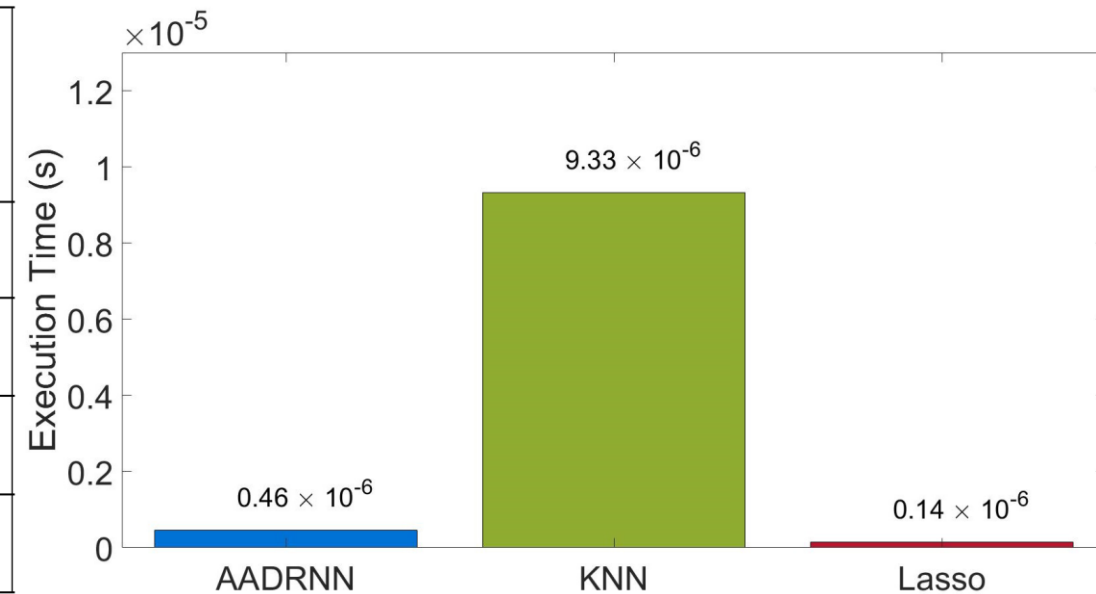


- Traffic metrics are calculated using high-level (anonymous) packet header information, without knowledge of network architecture or devices
- AADRNN learns ONLY from NORMAL traffic. It generalizes information gained to estimate expected metric values.

Offline Learning Botnet Attack Detection

➤ Mirai Botnet attack from Kitsune dataset⁷ | 764,137 packets | 107 distinct IP addresses

Attack Detection Methods	Accuracy	True Positive	False Negative	True Negative	False Positive
AADRNN	99.84	99.82	0.18	99.98	0.02
KNN	99.79	99.79	0.21	99.75	0.25
Lasso	99.78	99.75	0.25	99.95	0.05
Simple Thresholding	93.18	93.09	6.94	93.63	6.37



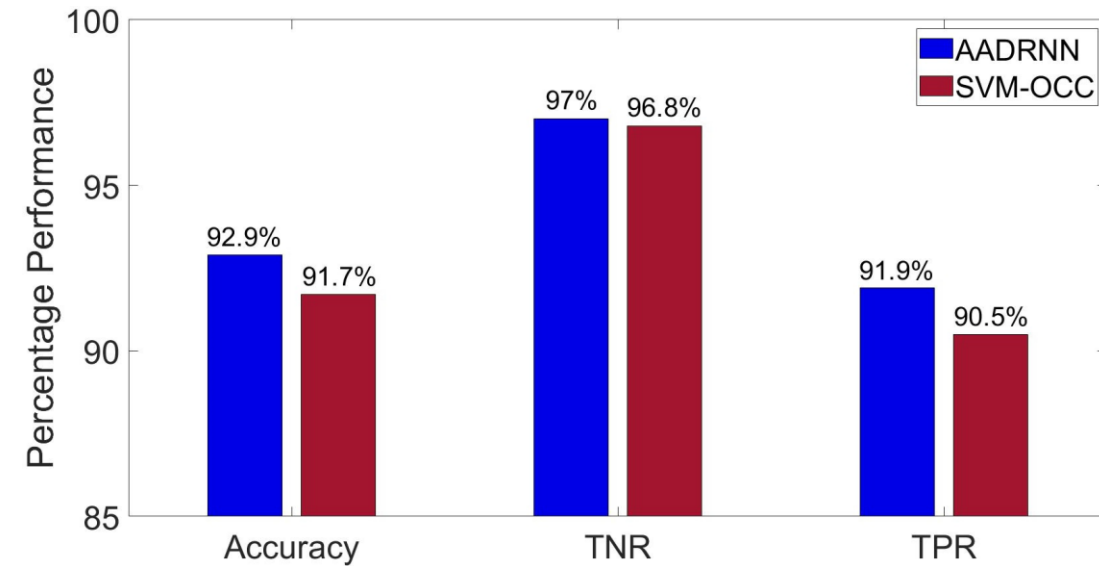
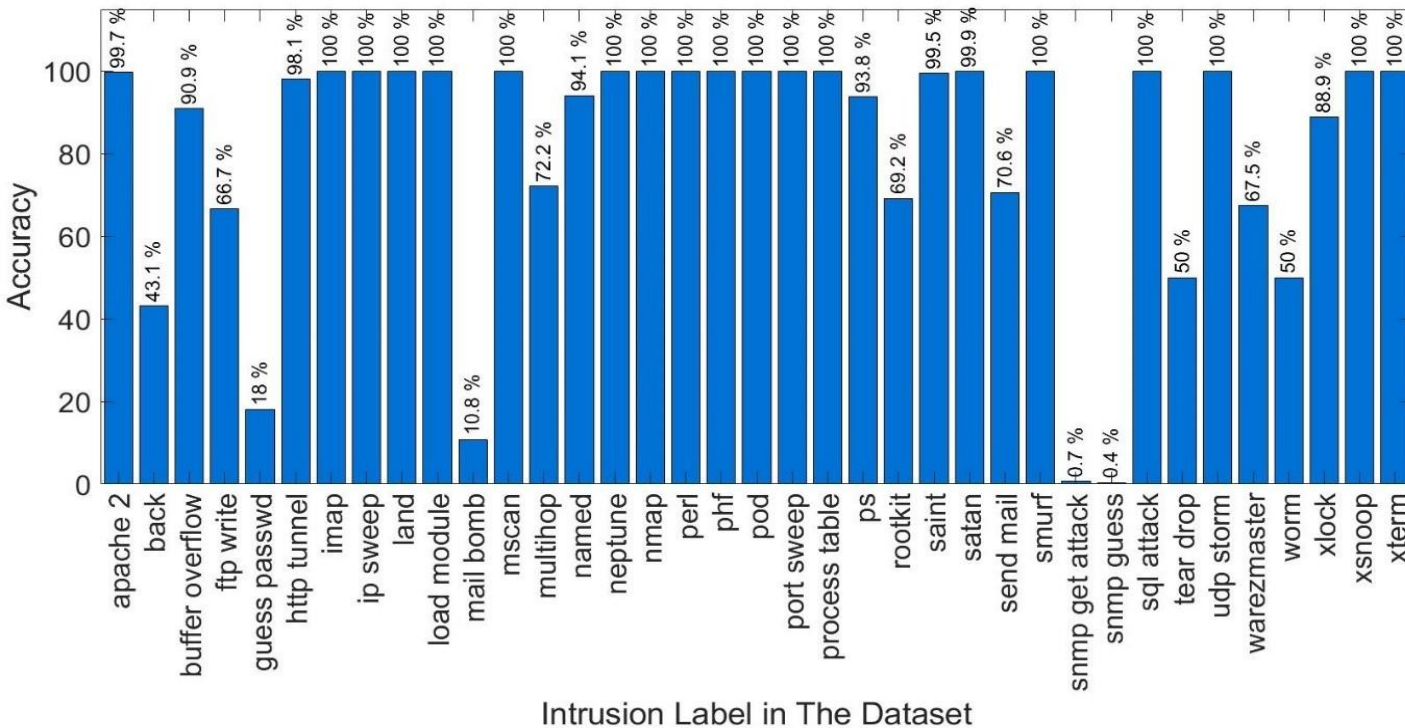
➤ AADRNN has high performance with low execution time and outperforms compared methods.

➤ Can AADRNN detect other types of attacks?

⁷ "Kitsune Network Attack Dataset," August 2020. [Online]. Available: <https://www.kaggle.com/ymirsky/network-attack-dataset-kitsune>

Simultaneous Detection of Various Types of Attacks

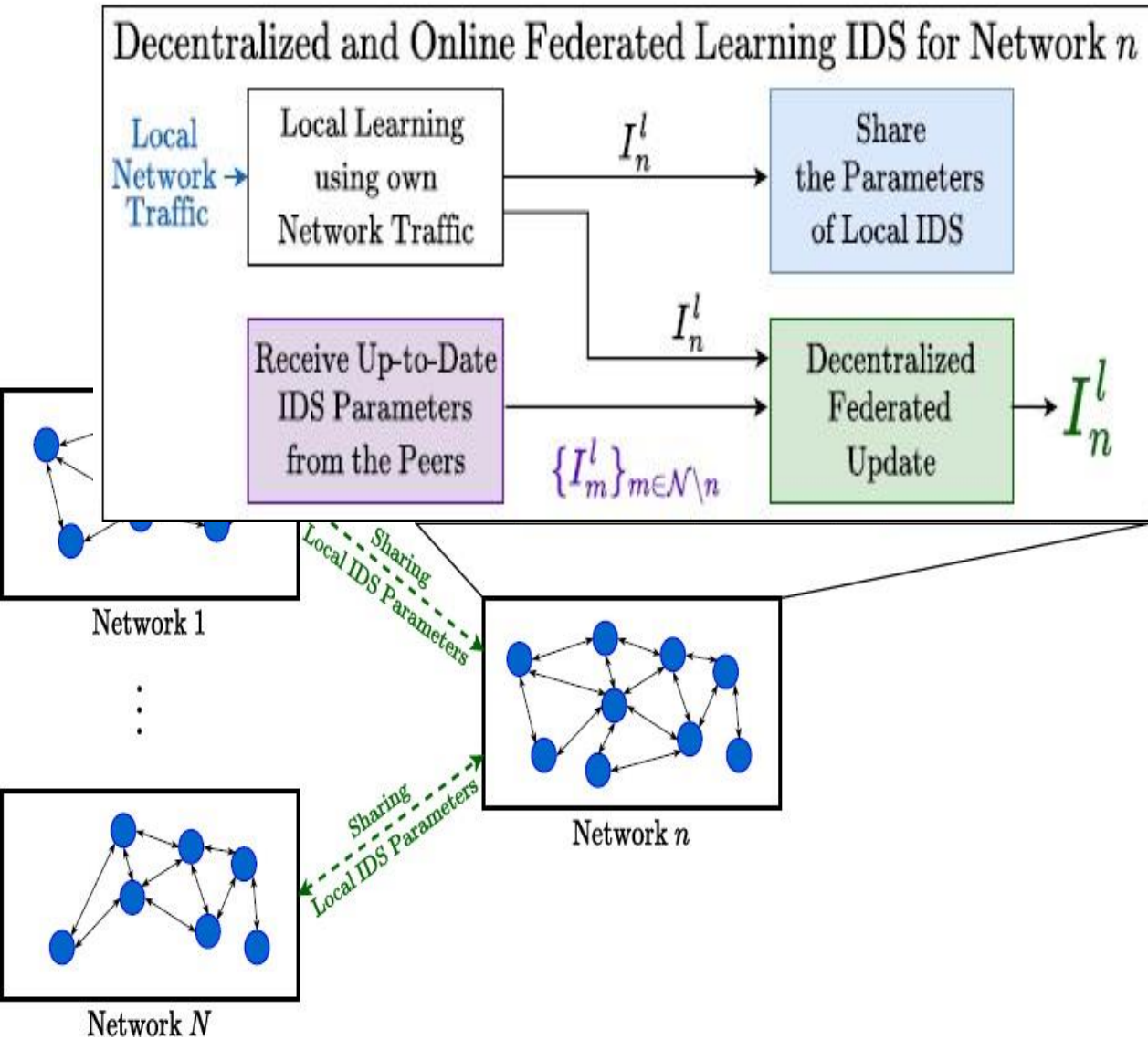
- KDD Cup'99 dataset⁸ | 41 network traffic features | 37 different attack types



- AADRNN achieves accuracy above 98 % for 21 out of 37 attack types.
- It outperforms Support Vector Machine – One Class Classifier (SVM-OCC)
- How will AADRNN react (adapt) if normal network traffic drastically changes?

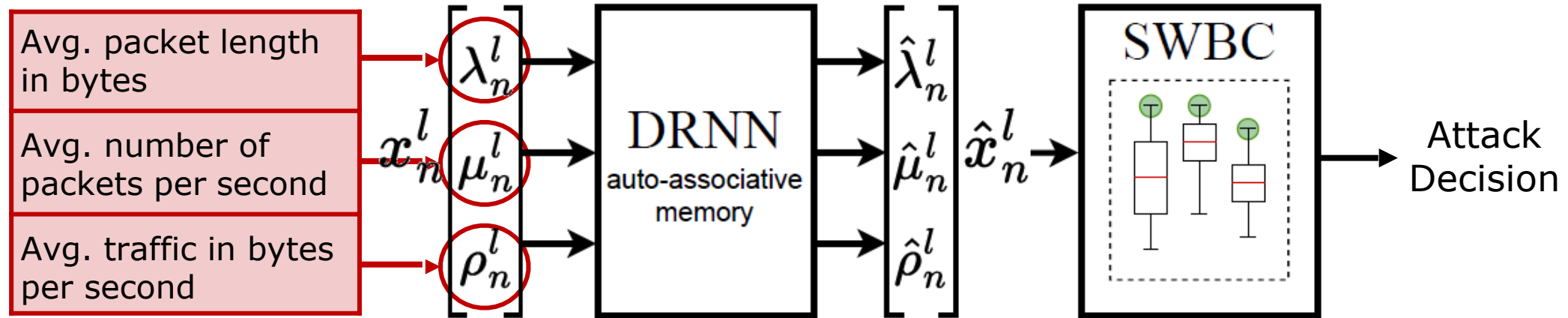
⁸ "KDD Cup 1999 Data." [Online]. Available: <http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html>

Decentralized and Online Federated Learning Intrusion Detection (DOF-ID)



- The DOF-ID architecture hosts many distinct components of a supply chain.
- Each component utilizes an instance of a common IDS and
 1. **Learns directly from its local traffic data,**
 2. **Exchanges parameters with other components,**
 3. **Incorporates other nodes' up-to-date knowledge into its IDS via Decentralized Federated Update.**
- DOF-ID improves the overall security of all collaborating nodes as it
 - **Takes advantage of the experience of each node,**
 - **Preserves the confidentiality of the local data at each of these nodes.**

Attack or Intrusion Detection System



- Deep Random Neural Network (DRNN) is used to create Auto-Associative Memory of "benign" network traffic.
- DRNN always estimates the expected traffic metrics for benign traffic.
- Local Learning algorithm uses learning data contains only normal traffic and
 - Minimizes a reconstruction loss for the learning data
 - Computes decision parameters based on only the normal traffic statistics

DISFIDA: Distributed Asynchronous Federated Learning

Receive up-to-date
IDS parameters
from peers

Select the set of
concurring nodes

Update the
parameters of each
segment of the IDS

Adapt the updated
IDS to local network
traffic

➤ A set of nodes that concur with for most of the decisions of local IDS for the local normal traffic:

$$\mathcal{C}_n^l = \{m : \frac{1}{l} \sum_{k=1}^l \mathbf{1}(I_m^l(x_n^k) = y_n^k) \geq \Theta, \forall m \in \mathcal{N} \setminus n\}$$

➤ The IDS parameters are updated separately for each DRNN layer and decision parameters averaging with the closest concurring node for that parameter:

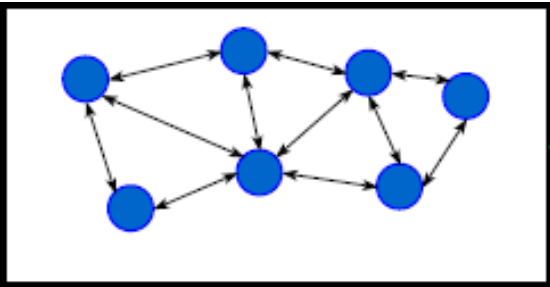
$$\theta_n^l \leftarrow c \theta_n^l + (1 - c) \theta_{m_\theta^*}^l \quad \Bigg| \quad m_\theta^* = \arg \min_{m \in \mathcal{C}_n^l} \left(\left| \theta_n^l - \theta_m^l \right| \right).$$

➤ The output layer weights of DRNN are updated via extreme learning machine to fully adapt to the local benign network traffic:

$$W_{(n,H)}^l = (\hat{X}_{(n,H-1)}^l)^+ X_n^l.$$

Performance Evaluation: Usecase & Datasets

MIRAI

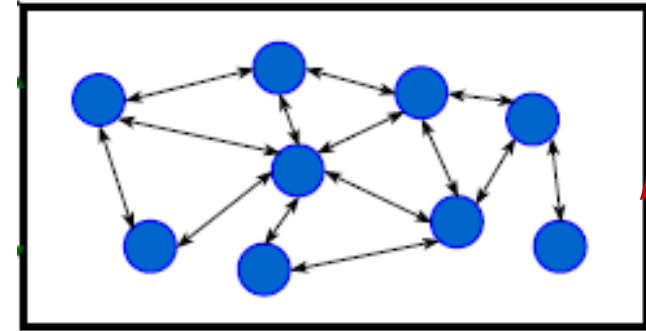


Network 1

➤ "Mirai Botnet" attack data from the **Kitsune dataset**:

- 107 unique IP addresses
- 764,137 packets transmitted
- in approx. 2 hours

DoS
HTTP

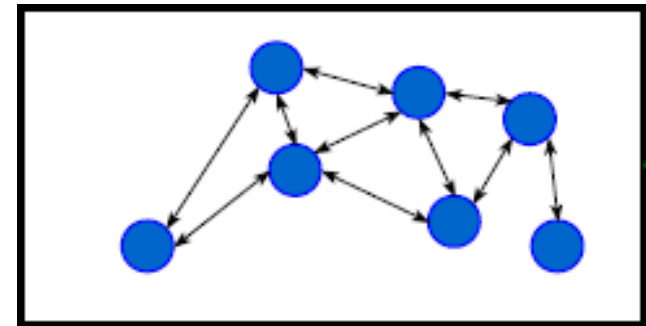


Network n

"DoS HTTP" and "DDoS HTTP" attacks from the **Bot-IoT dataset**:

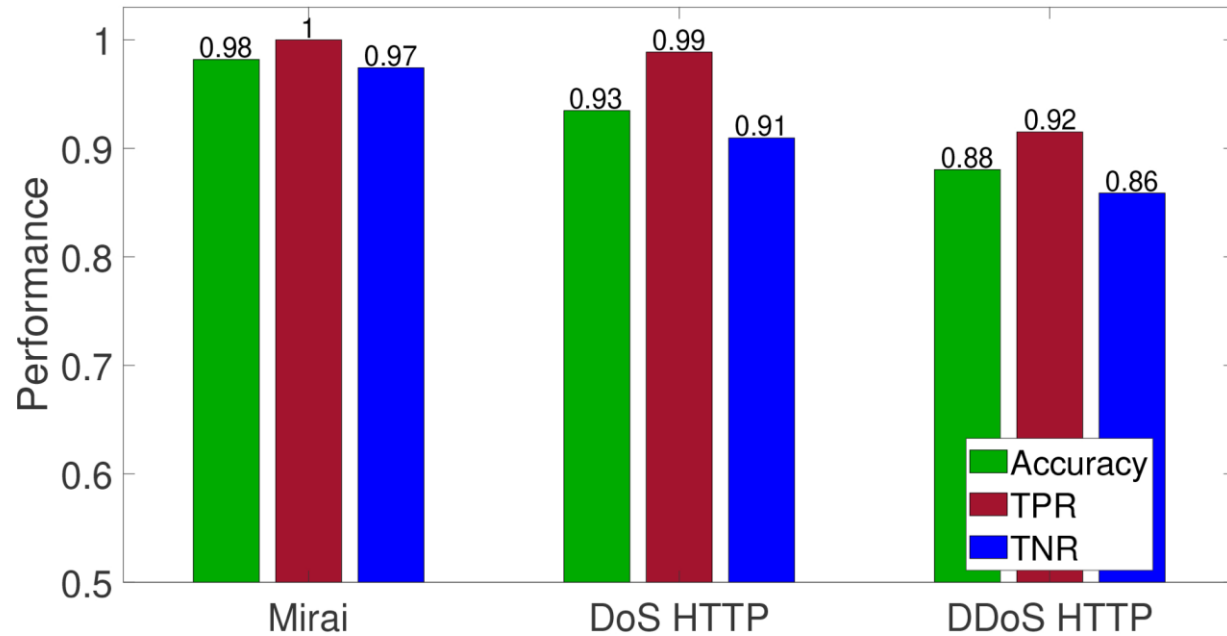
- DoS HTTP attack data:
 - 29,762 packets transmitted
 - in 49 minutes
- DDoS HTTP attack data:
 - 19,826 packets transmitted
 - In 42 minutes

DDoS
HTTP

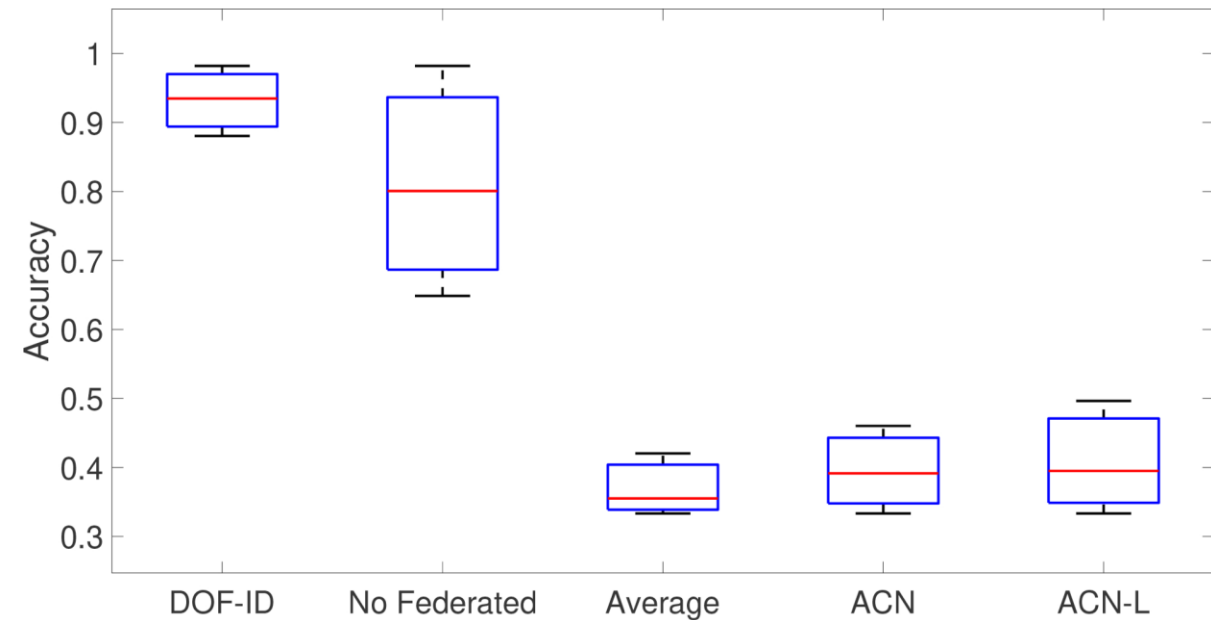


Network N

Performance Evaluation

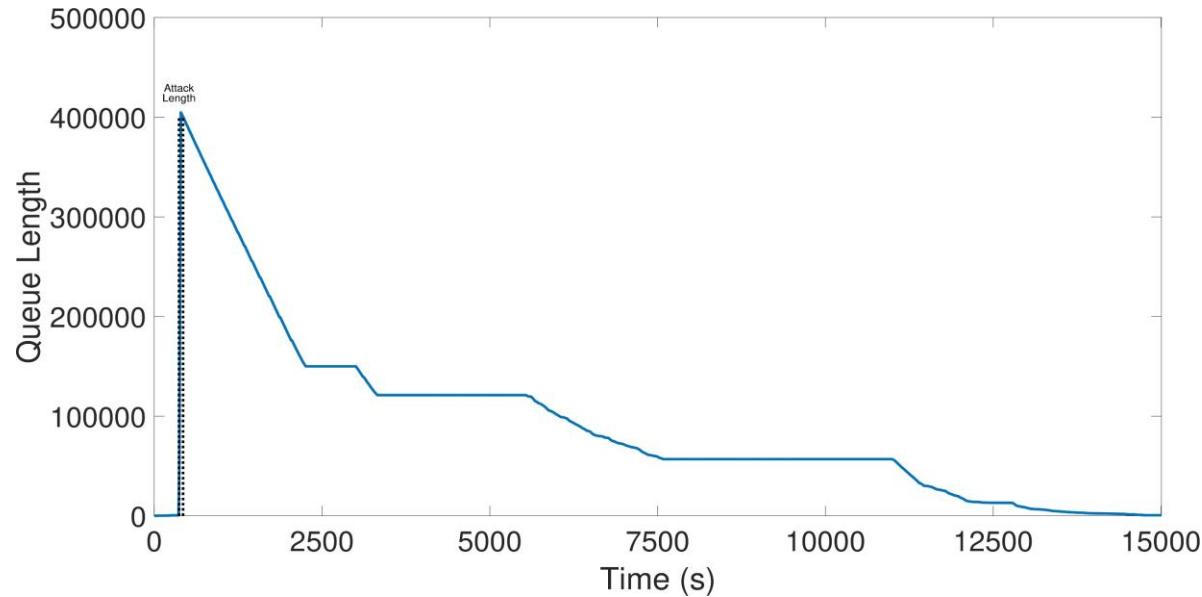


- Nodes achieve above 0.88 accuracy.
- All nodes detect local intrusions with high TPR (above 0.92).
- For any node, the federated update time is about 29.6 ms.
- The nodes suffer from some false alarms.

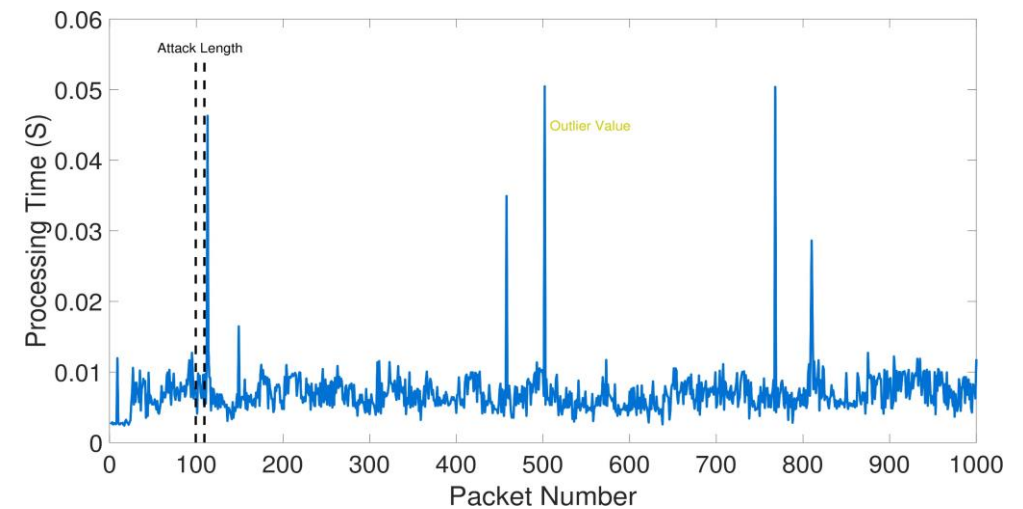
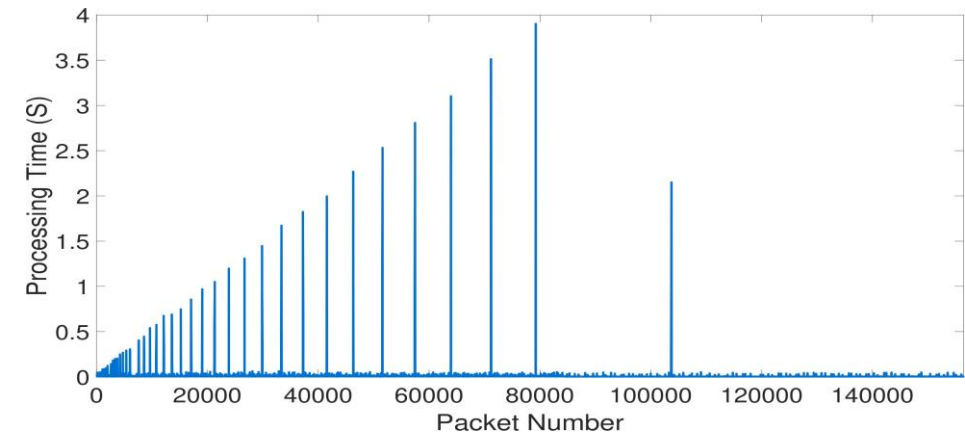


- DOF-ID has the best accuracy among all methods compared.
- “Average”, which is one of the most common federated update methods, performs poorly as network traffic across nodes varies considerably.

Many Attack Types, e.g. Botnets, Create Floods: Effect of a Flood Attack on the Gateway/Server



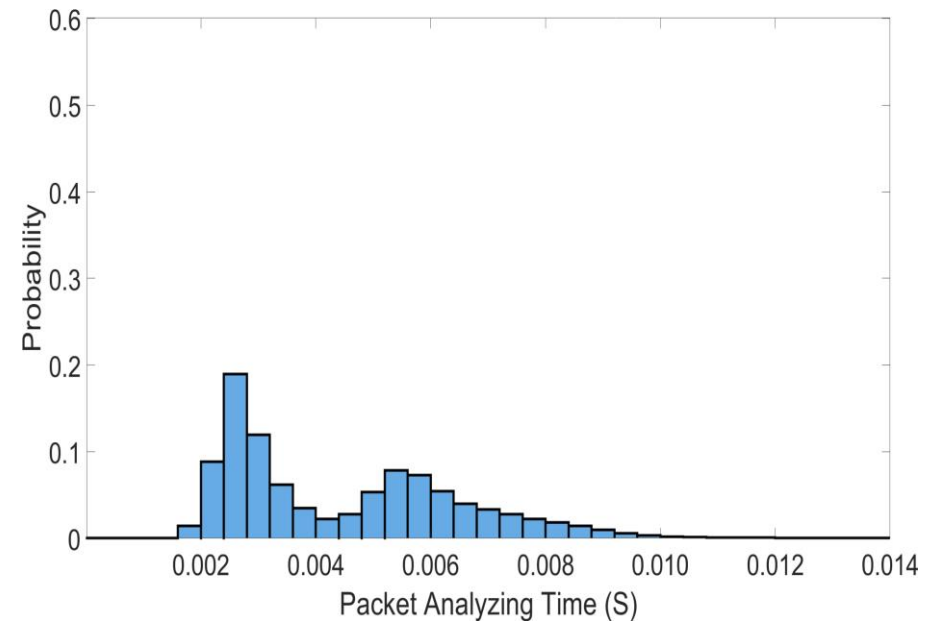
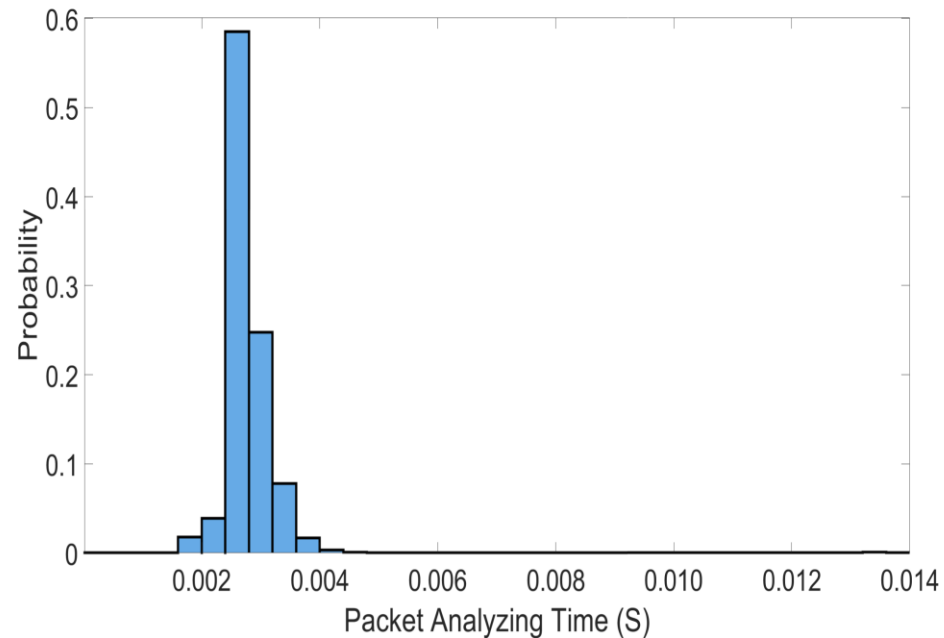
- Huge packet queue forms at the Server input prior to the IDS module during a 60-second UDP Flood Attack launched from one of the Ras-Pis, Resulting in **Large Outliers in IDS Processing Times**
- **Rapid backlog of packets (about 400,000 packets), followed by congestion and processing delays (about 5 hours), due to server paralysis for long time intervals**



Measurements on the Real System :

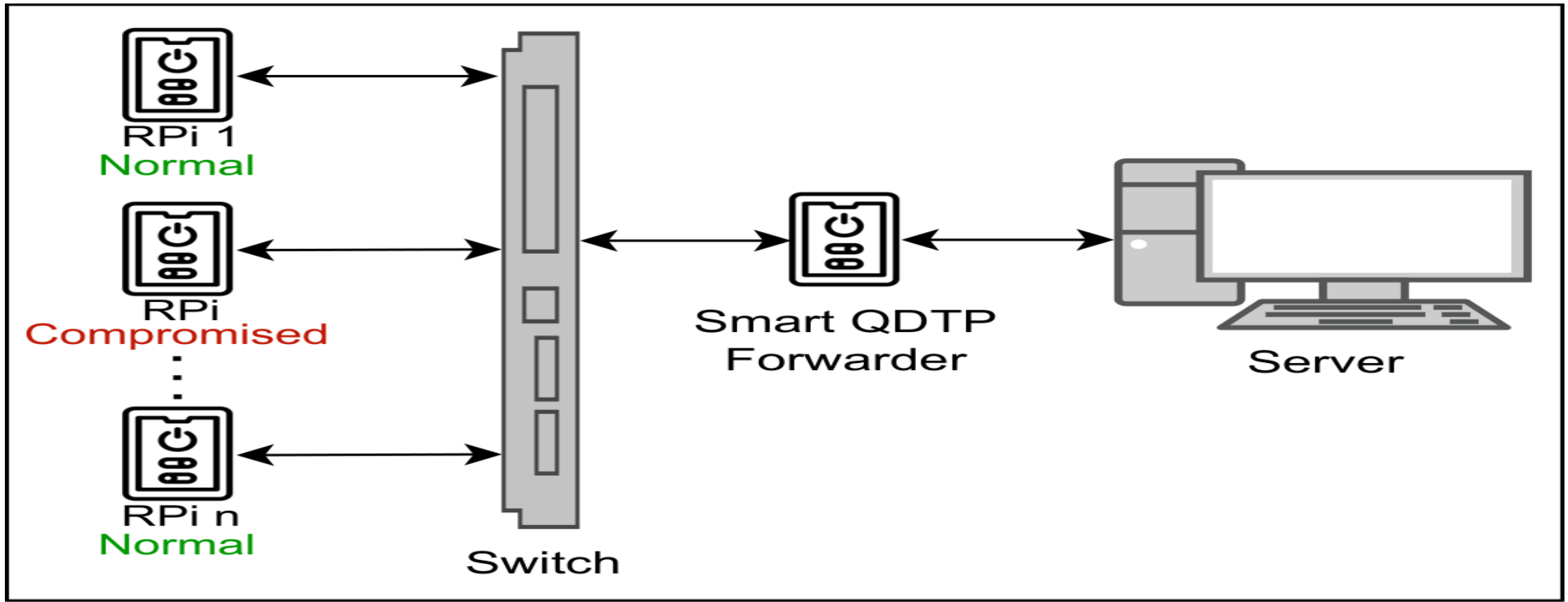
Histogram of the Server's IDS processing time per packet

Without QDTP Traffic Shaping

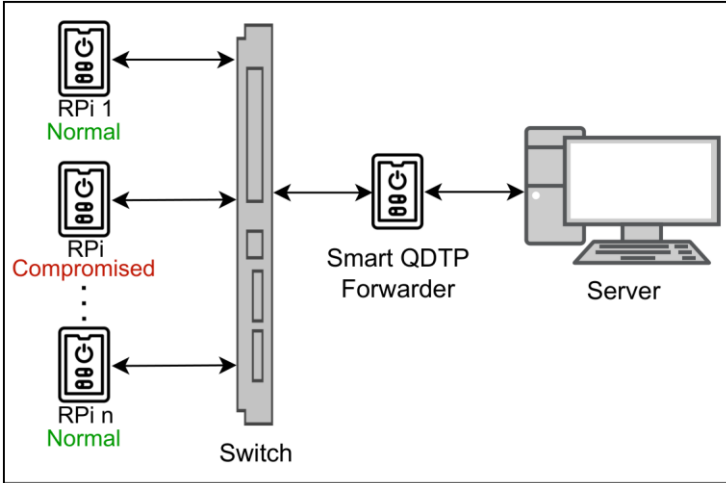


- (Right) - Attack - IDS Average Average Processing Time 65% Higher
- **3ms ==> 4.82 ms**

Smart Quasi-Deterministic Transmission Policy Forwarder (SQF) between the Network Switch and the IoT Server/Gateway



Traffic Shaping with QDTP (Gelenbe-Sigman ICC 2022)



$$t_{n+1} = a_{n+1} \quad \text{if } a_{n+1} > t_n + D,$$

$$= t_n + D, \quad \text{if } a_{n+1} \leq t_n + D$$

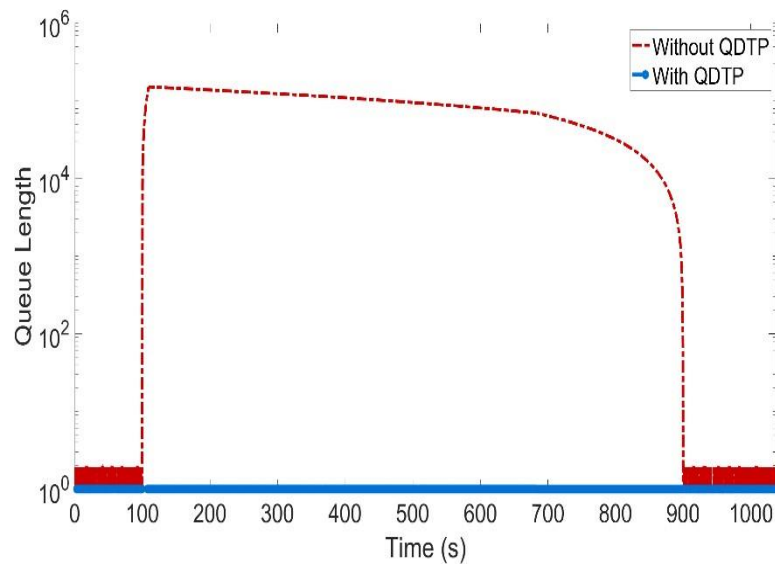
$$W_{n+1}^{\text{QDTP}} \equiv t_{n+1} - a_{n+1} = [W_n^{\text{QDTP}} - (a_{n+1} - a_n) + D]^+$$

$$W_{n+1}^{\text{Server}} = [W_n^{\text{Server}} - (t_{n+1} - t_n) + S_n]^+$$

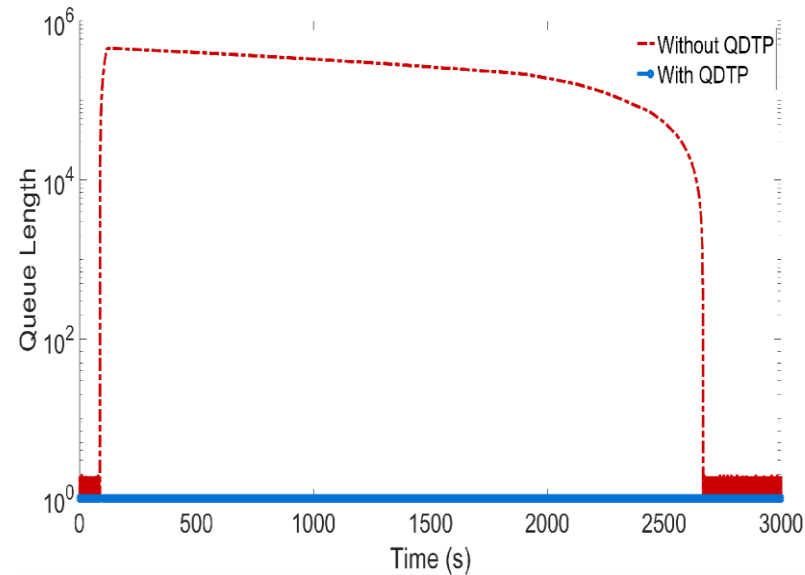
Key Theorem

If $D \leq S_n \rightarrow W_{n+1}^{\text{QDTP}} + W_n^{\text{Server}} \leq W_n^{\text{FIFO}}$

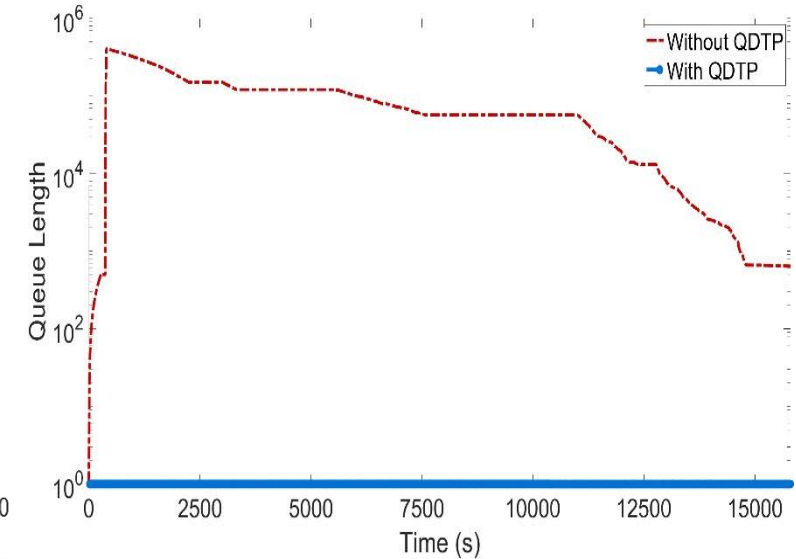
Server Queue Length with Smart QDTP



- Attack Duration = 10 sec
- $D = 3$ ms
- Number of Packets ≈ 153667



- Attack Duration = 30 sec
- $D = 3$ ms
- Number of Packets ≈ 470000

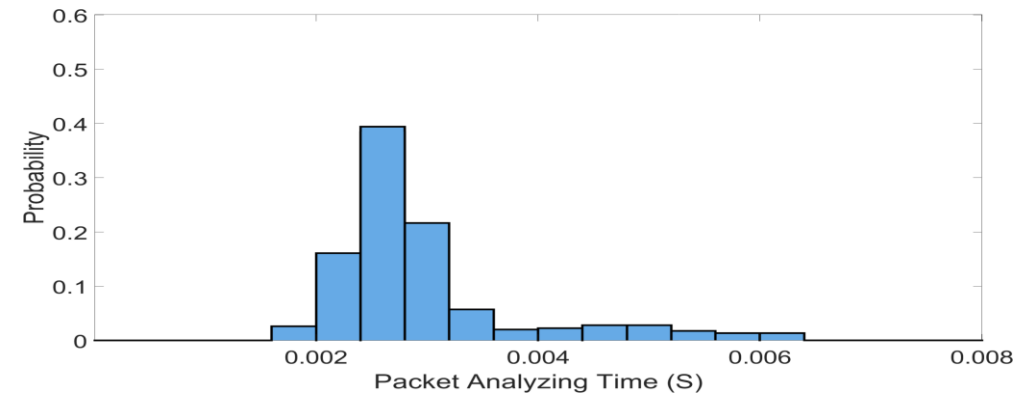
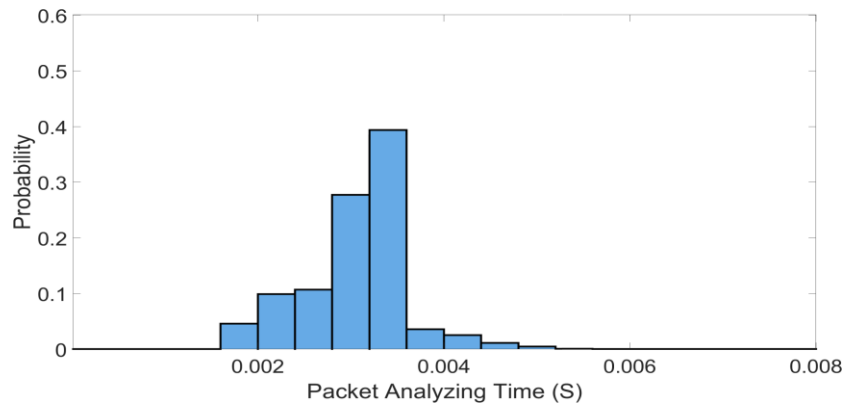
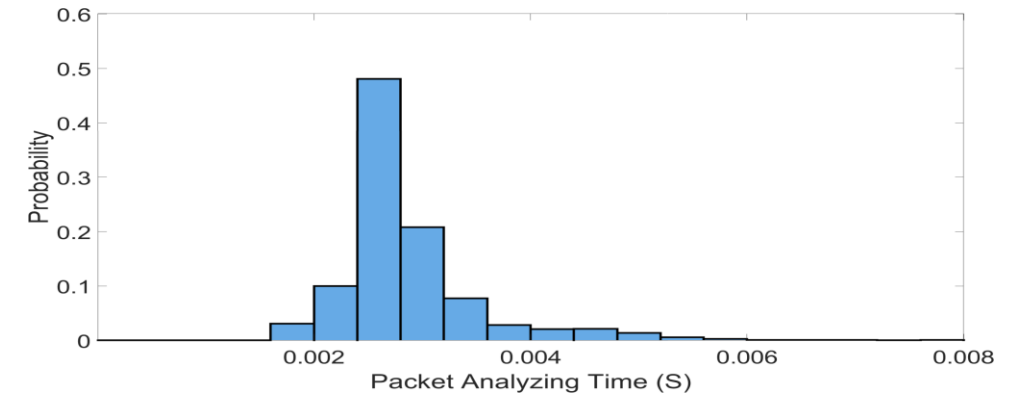
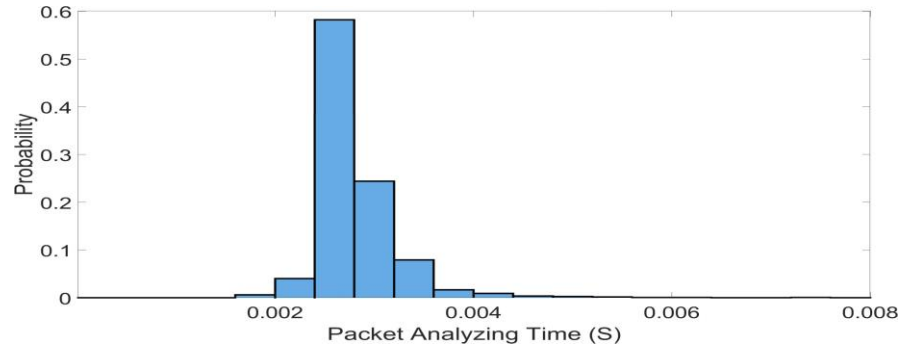


- Attack Duration = 60 sec
- $D = 3$ ms
- Number of Packets ≈ 400000

- The blue curve shows the packet queue length of the server when using SQDTP. Because the value of D we use is very close to the average value of T_n measured to be 2.98 ms, the fluctuations in T_n causes a small packet queue buildup.

Effect of The Smart QDTP Forwarder (SQF)

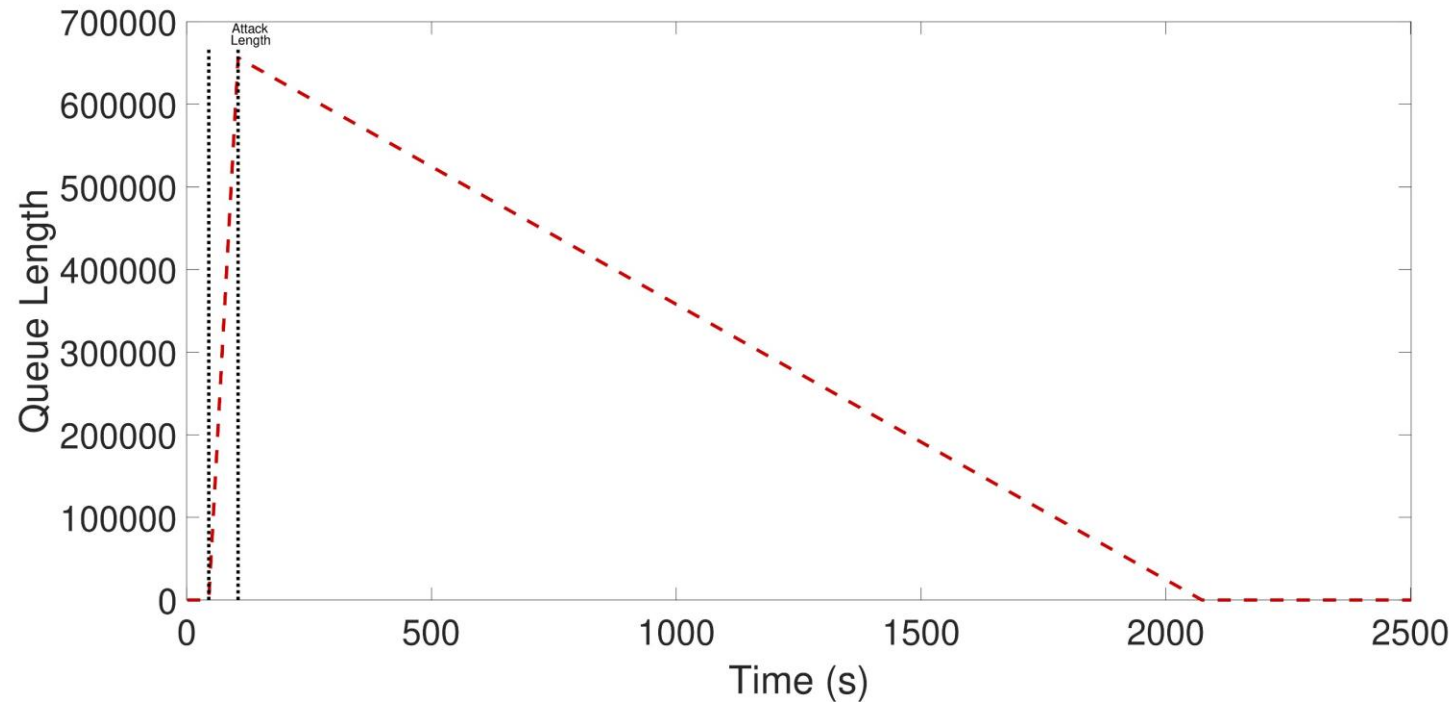
Histogram of measurements: Server's IDS processing time per packet
With SQF



- (Above) - No Attack – D=2.7ms Average Processing Time = 2.97 ms, Variance = 0.0041²
- (Below) - Attack - Average Processing Time = 3.28 ms (Higher by 10% avg.), Variance = 0.0023²

- (Above) - No Attack – D=3.2ms Average Processing Time = 3.00 ms, Var = 0.0036²
- (Below) - Attack - Average Processing Time = 2.99 ms, Var = 0.006²

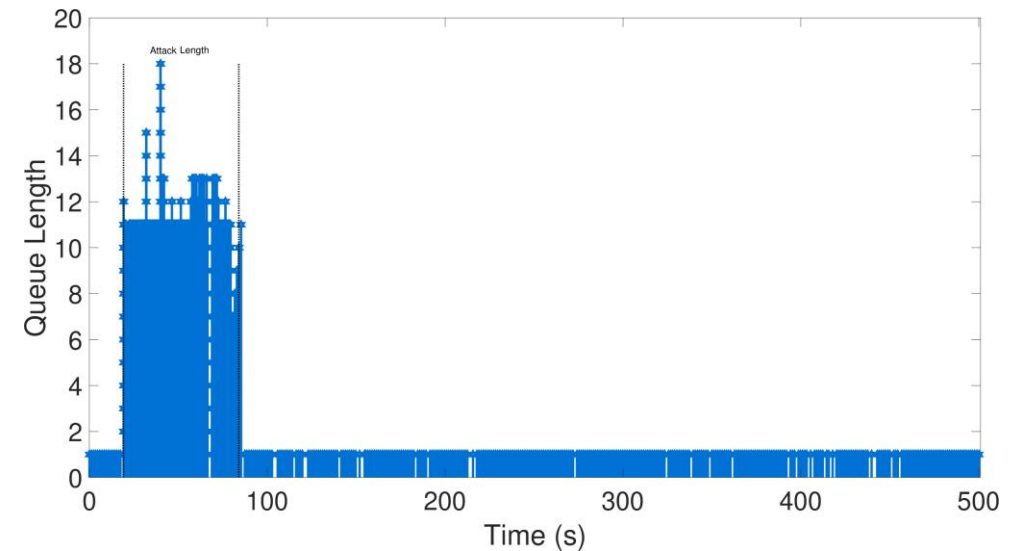
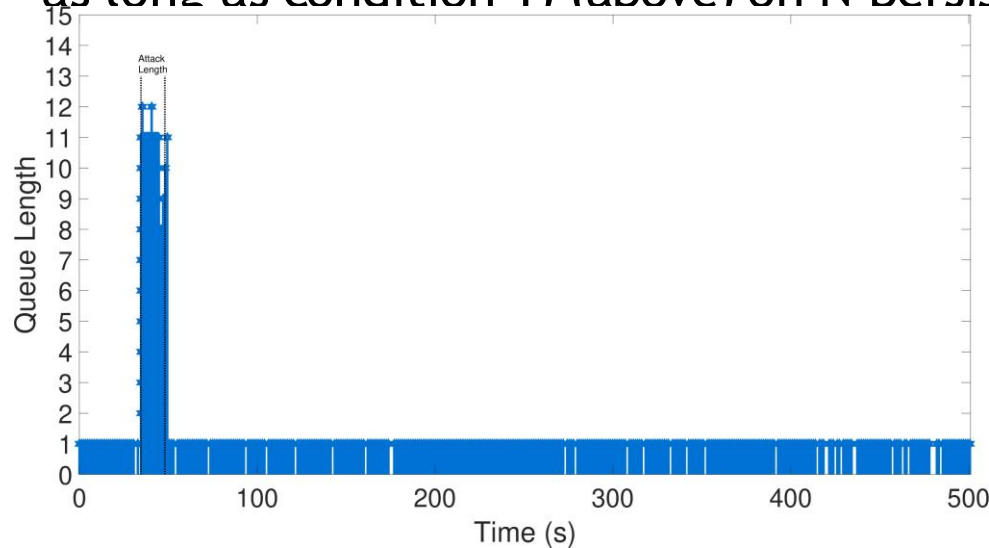
Linear Scale Queue Length with the Smart QDTP Forwarder (SQF)



- We observe that when the attack lasts for 60 seconds, the number of received packets is $\approx 680,000$, and due to the paralysis of the Server in several time intervals, many packets are dropped.

Queue Buildup & Simple Attack Mitigation

- Mitigation with parameters N, K : If the SQF receives more than N packets in a time interval smaller than or equal to D , it drops all incoming packets for the next $K.D$ time units. The action is repeated as long as condition 1) (above) on N persists.



- We chose $N = 10$, $K = 3$, and $D = 3$ ms
- The figures show the packet queue length at the server during the experiment when the attack lasts "10 seconds (left), 60 seconds (Right)" and the mitigation action is applied. The result is a very small accumulation of packets at the server during the attack period, and then after the attack ends the SQF can continue to operate normally.

Adaptive Mitigation

- (N) Normal Operation: the IDS Tests for Successive W-Packet Windows
- (A) If an Attack is Detected by the IDS in the Current W-Packet Window, Drop Packets in the Input Queue, Skip Testing for the next m Packets, and Test Again the next W-packet Window:
 - * If the IDS says « Attack » then Repeat the Process (A),
 - * Else Move Back to Normal Operation (N), i.e. test each Successive W-Packet Window



ADAPTIVE Mitigation to Minimize Average Cost C(AAM)

$$C(AAM) = \alpha E[K] + \beta E[\boxtimes]$$

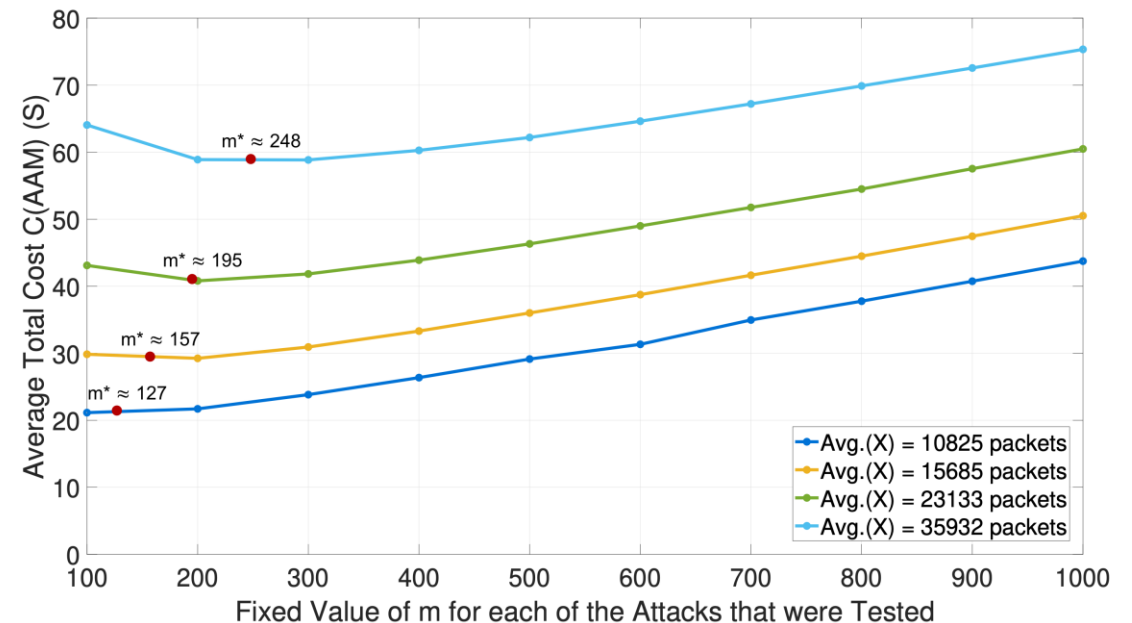
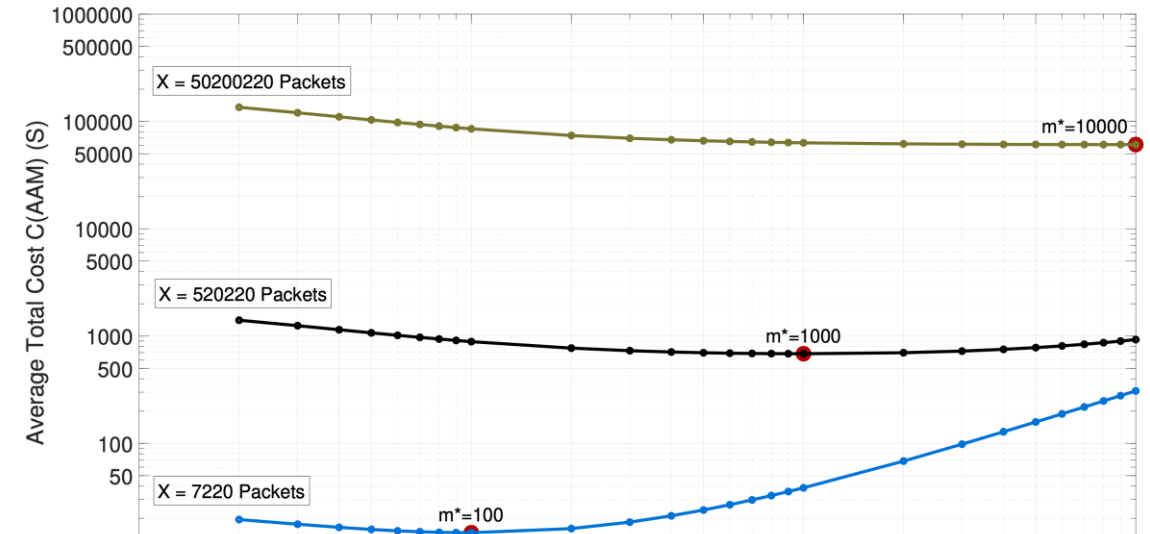
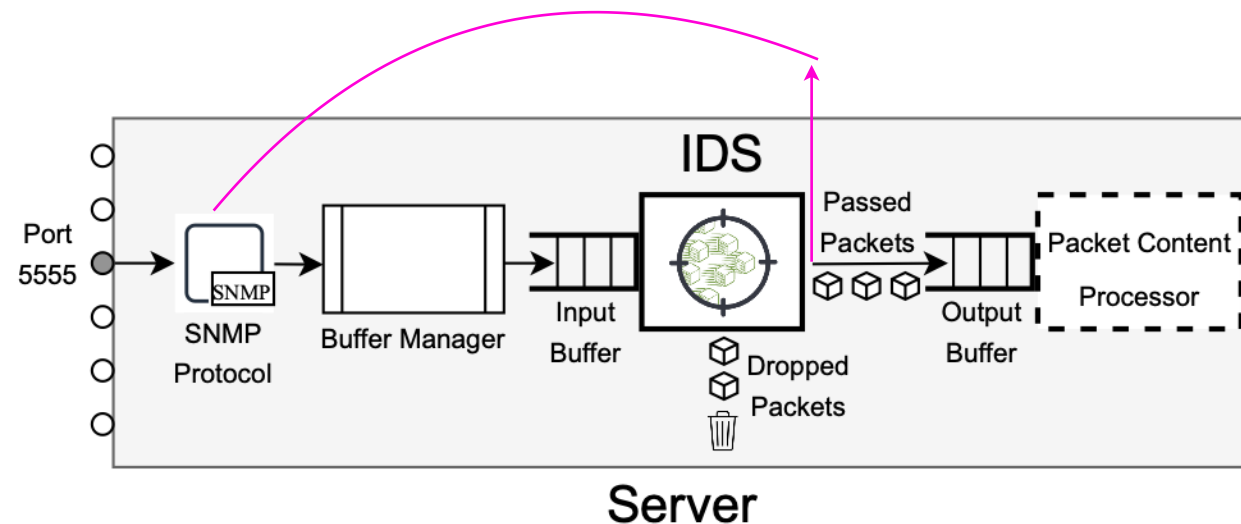
$$\boxtimes = N \boxtimes W, \text{ with } E[\boxtimes] \uparrow \boxtimes W \left[\frac{E[X] - W}{m + W} + \frac{1}{2} \right].$$

$$K = \boxtimes W [(1 - f)X + 6 - X],$$

$$\text{and } E[K] \uparrow \boxtimes W [(1 - f)E[X] - W + \frac{1}{2}(m + W)]$$

$$\uparrow W \boxtimes [(1 - f)E[X] + \frac{1}{2}(m - W)].$$

Sample Each m Packets Examine a window W and Drop



- Incorporate Self-Supervised Learning of local normal traffic into Federated Learning to reduce the number of false alarms,
- Address the overall energy consumption, distributed communication costs, and the possible performance slowdown that may be caused by federated learning,
- Expand the experimental setup for large networked systems such as supply chains, smart grids or large IoT networks, and develop Mitigation Methods for Cyberattacks against Supply Chains
- Investigate the Vulnerabilities that may be introduced to the Learning Process

Thank You for Your Attention
Erol Gelenbe

Can Such Effects be Included in Digital Twins ??

Questions?



Supply Chain Triage

Identifying Weak Points and Critical Dependencies (for NIS-2)

Mag. Michael Herburger, BA MA PhD

FH-Assistant-Professor and Research Project Manager @ University of Applied Sciences Upper Austria, Department „Supply Chain Management“

Senior Manager for Supply Chain Cybersecurity @ PwC Austria, Department „Cybersecurity and Privacy“

in addressing ICT/OT supply chain cybersecurity

- A significant challenge stems from terminology, since various definitions were identified in all the reviewed documents. These refer to supply chain cybersecurity and what it entails, but also to the various entities involved in the supply chain, e.g. managed service provider. This situation creates confusion, especially concerning the **scope** of each different approach. It also makes the comparison of these approaches challenging.
- This confusion around terminology is also reflected in national policy documents and can pose challenges for NIS2 directive's implementation. Therefore, efforts to create **a common understanding** in the scope of ICT/OT supply chain management should be undertaken.

Scope NIS-2

- Direct suppliers
 - But address subcontracting
- IT and OT suppliers
 - Only?
- New and existing suppliers
- ENISA NIS-2 „Implementing Guidance“

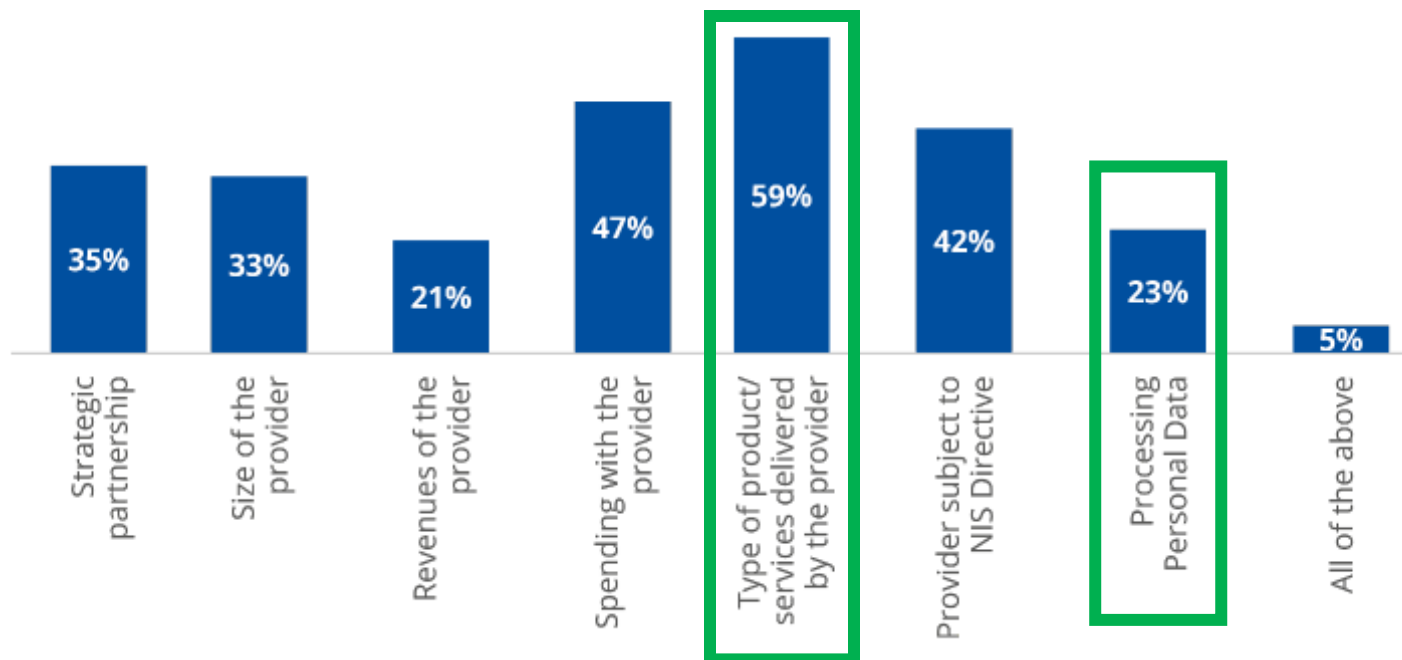
Type of supplier and provider	Function
Manufacturers ¹⁰	<ul style="list-style-type: none">• Design, develop, manufacture, and deliver products and components to their customers.• Source hardware and software components in their supply chain.• Deliver products which can serve multiple purposes; i.e. similar products are sold to different product users with different use scenarios.• Liable for their part of delivery and service provided.
System integrators (service providers for engineering services)	<ul style="list-style-type: none">• Engineer systems that are used in production environments.• Design and deploy systems, such as automation solutions used in industries and critical infrastructure.• Can include civil work such as deployment of network infrastructure or pipelines for example in turnkey solutions.• Play an essential part in cybersecurity design and implementation in (critical) infrastructure.
ICT service management	Managed Service Providers (MSPs) <ul style="list-style-type: none">• Provide services related to the installation, management, operation or maintenance of ICT products, networks, infrastructure, applications or any other network and information systems, via assistance or active administration carried out either on customers' premises or remotely.
	MSSP <ul style="list-style-type: none">• Assists entities in areas such as incident response, penetration testing, security audits and consultancy (NIS2 directive, Article 6(40)).• Offers services, such as:<ul style="list-style-type: none">• assessment – e.g. penetration testing, or conformance to specific security requirements or standards;• implementation – e.g. implementation of security controls such as malware detection in an infrastructure;• management – e.g. security operating centre (SOC) services for incident response.
Providers of digital services ^{11 12}	Cloud computing services, include: <ul style="list-style-type: none">• infrastructure as a service,• platform as a service,• software as a service (SaaS), and• network as a service.

From type of suppliers to a list of relevant suppliers

- List of all suppliers
 - But what does this mean for big groups? → 10-100k suppliers
- Use of „purchasing category/product group“
- Analysis of purchased products
- Data quality?
- Use stakeholders knowledge
 - „internal consumer“ know details about purchased products
- Next step: realise a risk-based approach to identify the criticality of relevant suppliers

From list of relevant suppliers to supplier categorization

Business criteria for ICT/OT supply chain risk analysis*



Are these cybersecurity criteria for evaluating the relationship to the suppliers?

Problem: Cybersecurity criteria are not yet operationalised (not like purchasing volume, on time delivery, product quality)

From list of relevant suppliers to supplier categorization

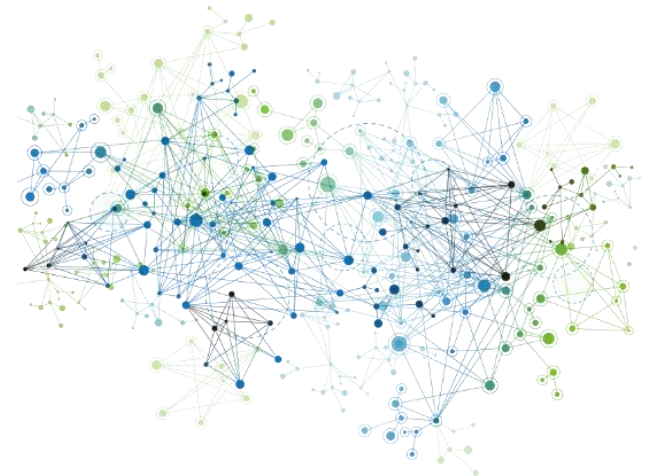
Purchasing criteria OLD

Purchasing volume, quality aspects, on-time delivery, number of complaints

Purchasing criteria NEW - Supply Chain Cybersecurity criteria









Several different/additional criteria must be used to determine the criticality of supply chain partners and components:








- Does the SC partner have access to your company's intellectual property?
- Does the SC partner have access to your company's or customer data?
- Does the SC partner have access to your company's system and network infrastructure?
- Is there an EDI interface (or similar) to the SC partner?
- Is the SC partner a single source?
- Is the SC partner involved in your company's development and/or innovation process?
- Does a failure at the SC partner lead to a production stop or a production restriction?
- Does the SC partner supply a smart product?
- Does the SC partner supply fast-moving items or do you supply the SC partner with fast-moving items?
- Is the SC partner highly integrated into the production process?
- Can the SC partner and its products/services be quickly replaced by alternatives?
- Does the SC partner have remote maintenance access to your systems?
- Does your company purchase software as a service from the SC partner? *



* Source: List of questions (>50), based on NIST, NCSC-Framework, and other related Standards and Guidelines.

Supply Chain Assets to consider

SUPPLIER ASSETS TARGETED BY A SUPPLY CHAIN ATTACK		
	Pre-existing Software	e.g. software used by the supplier, web servers, applications, databases, monitoring systems, cloud applications, firmware. It does not include software libraries.
	Software Libraries	e.g. third party libraries, software packages installed from third parties such as npm, ruby, etc.
	Code	e.g. source code or software produced by the supplier.
	Configurations	e.g. passwords, API keys, firewall rules, URLs.
	Data	e.g. information about the supplier, values from sensors, certificates, personal data of customers or suppliers themselves, personal data.
	Processes	e.g. updates, backups or validation processes, signing certificates processes.
	Hardware	e.g. hardware produced by the supplier, chips, valves, USBs.
	People	e.g. targeted individuals with access to data, infrastructure, or to other people.

CUSTOMER ASSETS TARGETED BY A SUPPLY CHAIN ATTACK		
	Data	e.g. payment data, video feeds, documents, emails, flight plans, sales data and financial data, intellectual property.
	Personal data	e.g. customer data, employee records, credentials.
	Software	e.g. access to the customer product source code, modification of the software of the customer.
	Processes	e.g. documentation of internal processes of operation and configurations, insertion of new malicious processes, documents of schematics.
	Bandwidth	e.g. use the bandwidth for Distributed Denial of Service (DDoS), send SPAM or to infect others on a large scale.
	Financial	e.g. steal cryptocurrency, hijack bank accounts, money transfers.
	People	e.g. individuals targeted due their position or knowledge.

Supplier categories and defined measures

2 potential approaches for deriving measures

- 1) Define measures per question
 - + precise risk-based approach
 - time consuming and complex
- 2) Define measures per supplier category
 - + less complex and less time consuming
 - broader risk-based approach

Use of 4 categories

- low, medium, high, critical

Additionally, think about using different supplier types

Measures	L	M	H	C
Audits				X
Certifications			X	X
Self-Assessments		X	X	X
Automated Evaluations & Ratings		X	X	X
Risk Analysis		X	X	X
Vulnerability Scans	X	X	X	X
Due Diligence Checks	X	X	X	X

Thank you very much!

Contact

michael.herburger@fh-steyr.at

michael.herburger@pwc.com

@LinkedIn