Attacking and Defending DNP3 ICS/SCADA Systems

Vasiliki Kelli, Panagiotis Radoglou-Grammatikis, Achilleas Sesis, Thomas Lagkas, Eleftherios Fountoukidis, Emmanouil Kafetzakis, Ioannis Giannoulakis, and Panagiotis Sarigiannidis

The research leading to these results has received funding
from the European Union's Horizon 2020 research and innovation program under grant agreement No 833955

Outline

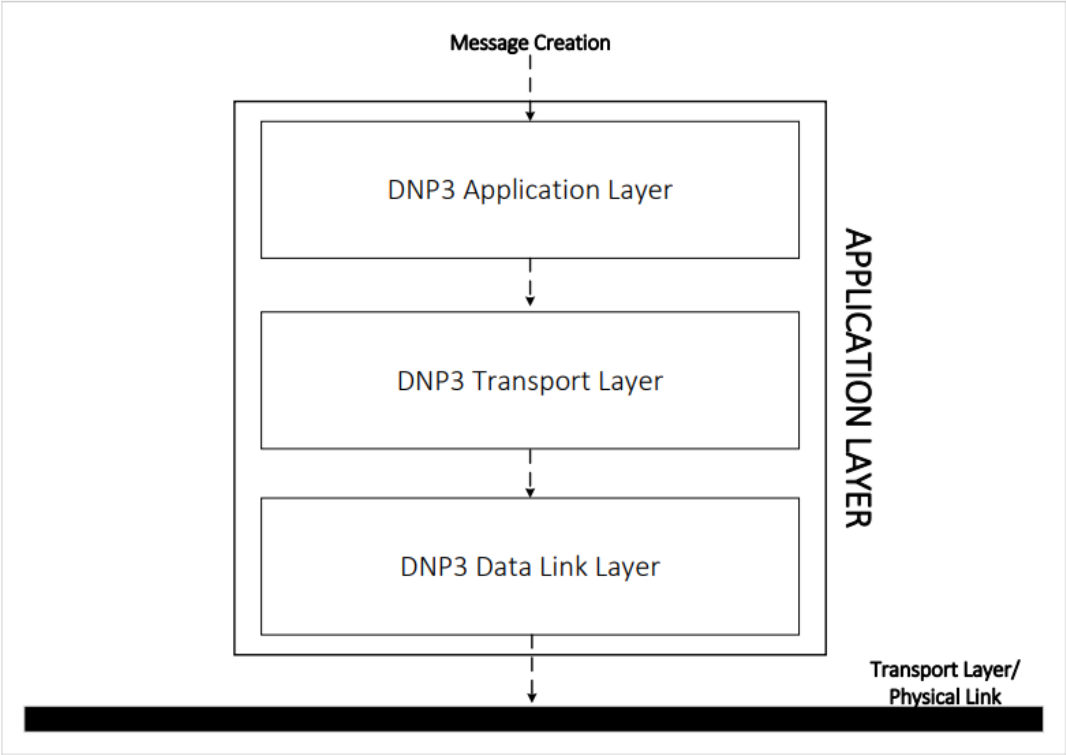
- The DNP3 Protocol
- DNP3-centered Cyberattacks
- DNP3 Attack Detection & Mitigation System
- Evaluation Results
- Concluding Remarks

The Distributed Network Protocol 3 (DNP3) Protocol

- DNP3 is highly utilized in SCADA/ICS
  - Industrial Sector, Smart Grids
- Multi-tier application layer protocol
- Able to run on top of TCP
- Client-Server model
  - Master: Client functions
  - Slave/Outstation: Server functions

The Distributed Network Protocol 3 (DNP3) Protocol: Layers

- Data Link Layer
  - Sends & Retrieves frames
  - Header information (DNP3 source & destination address)
  - Error calculation with Cyclic Redundancy Check (CRC)
- Transport Layer
  - Fragmentation of large packets received by the Application Layer
  - Contains information for fragment reassembly
- Application Layer
  - Creation of the message to be communicated
  - The Application Layer's header differs based on the source of the message



DNP3 Cyberattacks

01

Disable Unsolicited Messages

- Unsolicited messages are sent by the slaves to notify the master of irregularities
- Malicious master instructs the slave to stop sending unsolicited messages

02

Cold Restart

- Malicious master orders the slave to perform a full restart
- DoS is achieved as the slave remains offline during the restart

03

Warm Restart

- Malicious master orders the slave to restart DNP3 applications
- DoS is achieved while the slave remains unresponsive

04

Slave Discovery

- 2 nmap DNP3 reconnaissance scripts
- Identifies if a given IP address belongs to a DNP3 slave

05

Initialize Data

- Command the slave to initialize its data to the default values through packet crafting & MiTM attacks
- Updates from the slave will not reflect the system's actual status

06

Stop Application

- Order the slave to cease all DNP3 functions through packet crafting & MiTM attacks
- DoS is caused as the slave remains offline

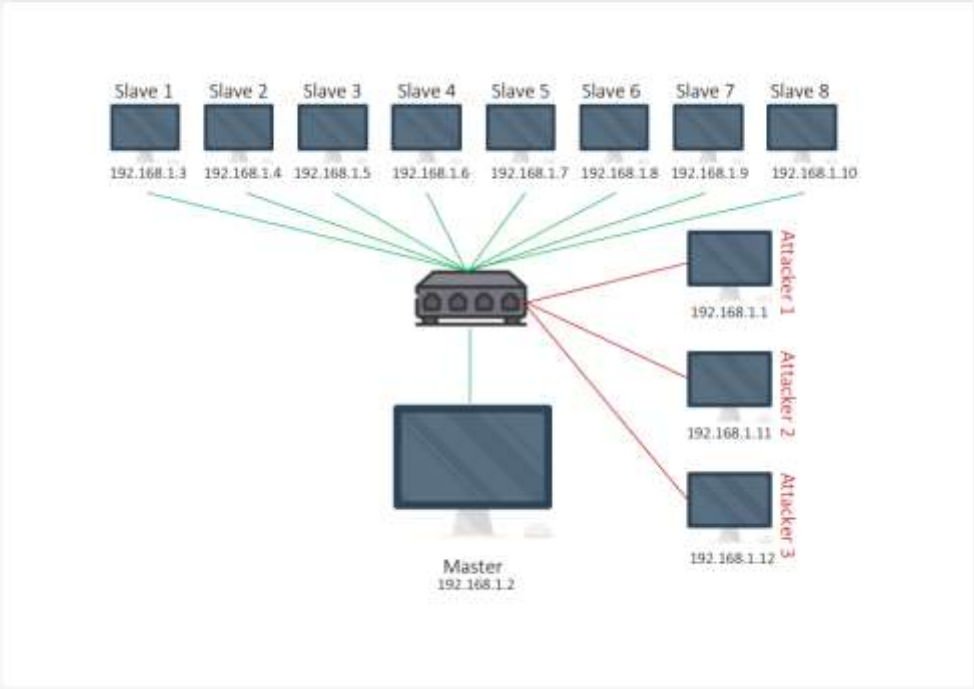
07

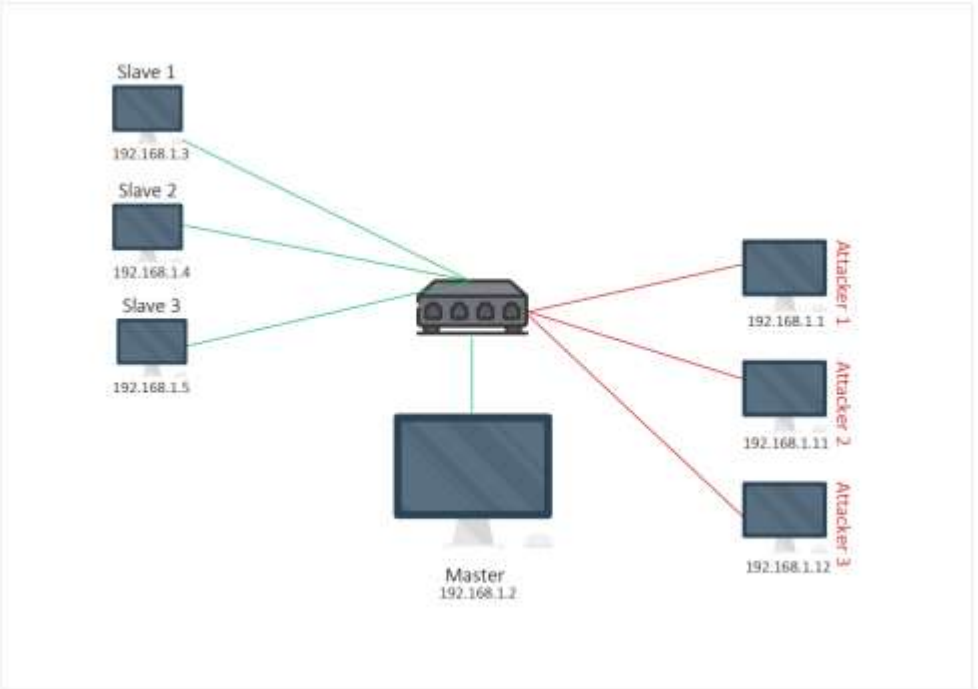
Replay

- Delay the transmission of a legitimate DNP3 packet with MiTM attacks

DNP3 Cyberattacks

DNP3 Cyberattacks





The cyberattacks were run against the two above topologies every [20,30] seconds

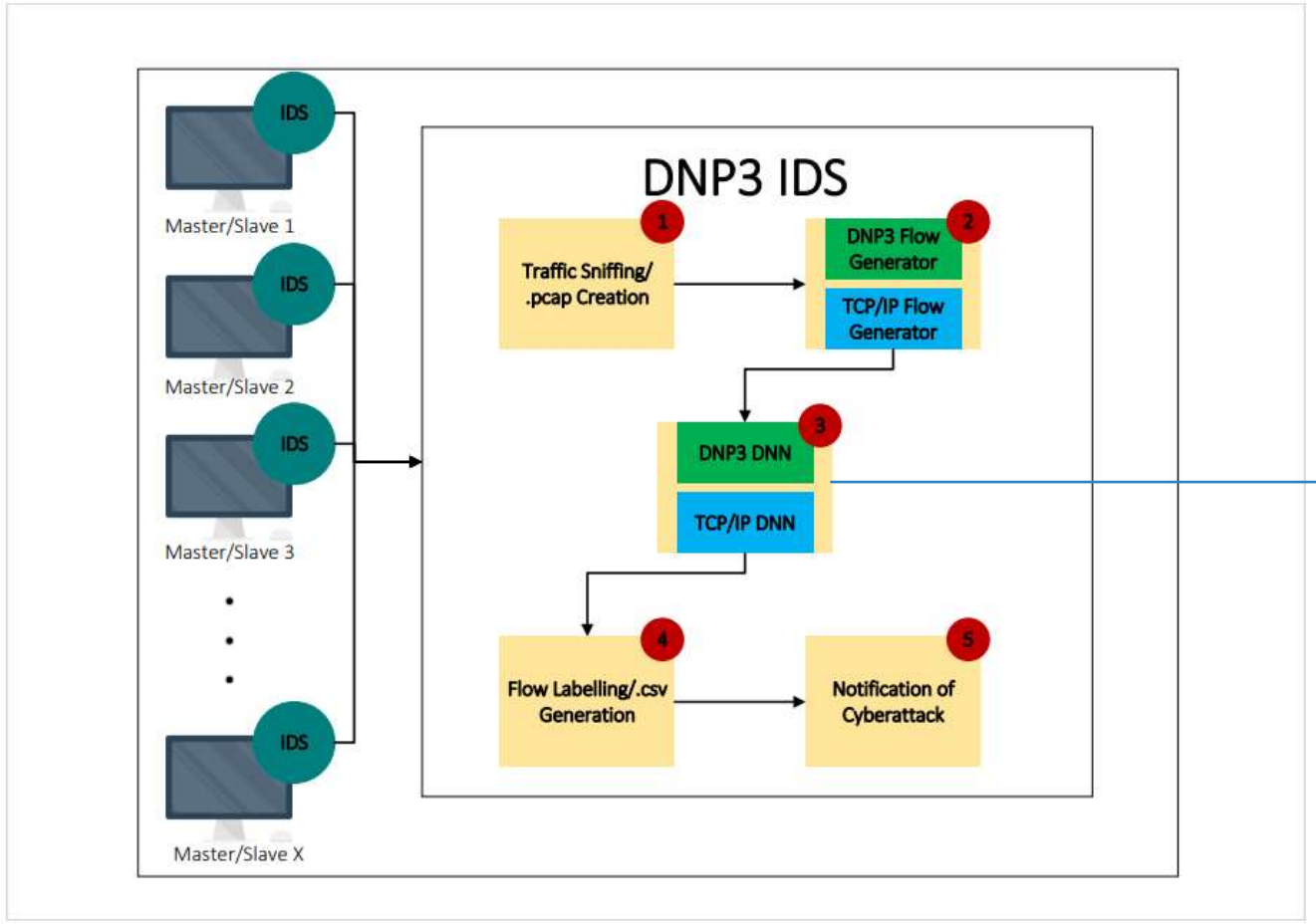
DNP3 Cyberattack Detection & Mitigation

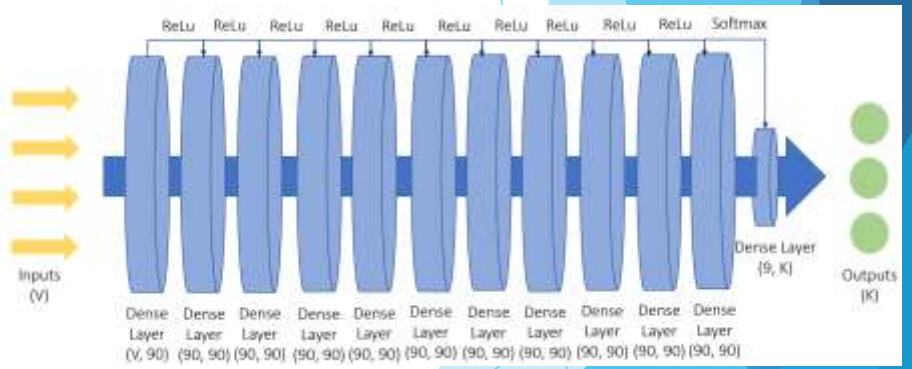
- Network flow-based IDS
- 2 DNP3 cyberattack classification DNNs
- Recognition of 8 DNP3-centered cyberattacks
- Accuracy of 99%
- Comprised by 4 components

DNP3 Cyberattack Detection & Mitigation: Components

1. Traffic Sniffing
   - Traffic generated through the communication of SCADA/ICS is captured
2. Categorization of packets in network flows
   - Utilization of 2 tools
   - Custom DNP3 flow generator
   - TCP/IP flow generator CICFlowMeter
3. A set of DNNs
   - DNN trained with DNP3 flows
   - DNN trained with TCP/IP flows from CICFlowMeter
   - Similar DNN architecture in both cases
4. Alert generation
   - In case of attack detection, an alert gets generated

DNP3 Cyberattack Detection & Mitigation





Classifier Detection Evaluation

DNP3 FLOW-BASED CLASSIFIER EVALUATION

	Decision Tree	DNN	K-NN	Naive Bayes	Random Forest
Accuracy	0.9305	0.9900	0.9494	0.6827	0.905
Precision	0.9306	0.9580	0.9497	0.7222	0.9053
F1	0.9305	0.9565	0.9494	0.6490	0.9049
Recall	0.9305	0.9549	0.9494	0.6827	0.9049

DNNs show higher metrics than any other machine learning classifier

Detection of cyberattacks is more accurate with DNNs

CICFLOWMETER-BASED CLASSIFIER EVALUATION

	Decision Tree	DNN	K-NN	Naive Bayes	Random Forest
Accuracy	0.8818	0.9763	0.8794	0.6377	0.8690
Precision	0.8818	0.8845	0.8797	0.6746	0.8694
F1	0.8818	0.8832	0.8794	0.6022	0.8690
Recall	0.8818	0.8819	0.8794	0.6377	0.8690

DNN Comparative Evaluation

- The DNN trained on DNP3 flows demonstrates higher evaluation metrics
- The DNP3 flow-based DNN recognizes more accurately the majority of DNP3 cyberattacks
- The CICFlowMeter-based DNN classifies correctly all ARP Poisoning data samples
- The two DNNs complement each other

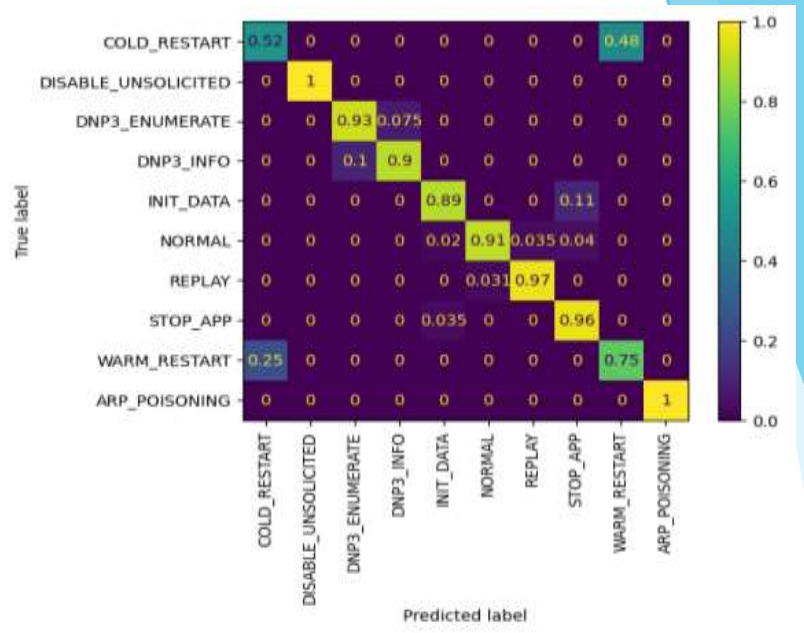


Fig. 7. Confusion Matrix of DNN trained with TCP/IP flows

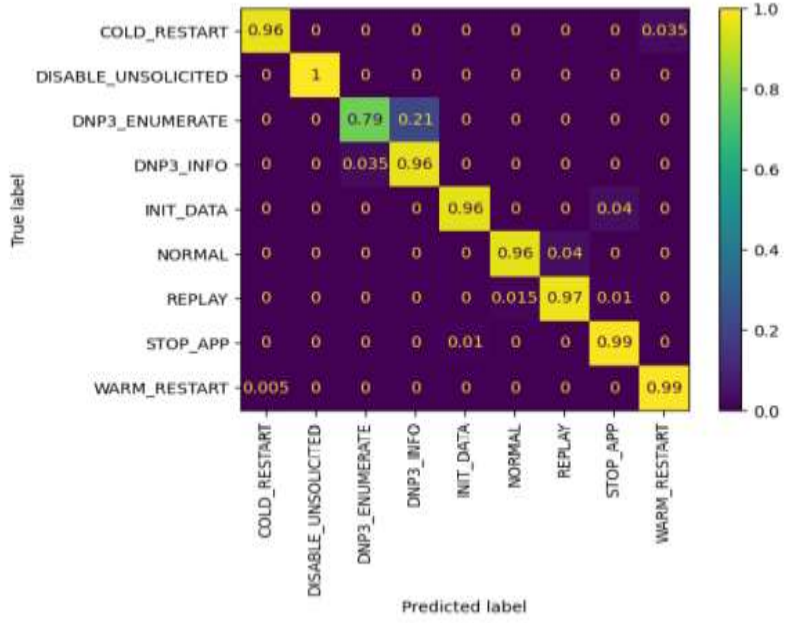


Fig. 6. Confusion Matrix of DNN trained with DNP3 flows

Concluding Remarks

Attacking

Attacking DNP3

- 8 DNP3-centered cyberattacks were implemented
- The vast majority takes advantage of DNP3 vulnerabilities-by-design

Defending

Defending DNP3

- A flow-based, multi-tier IDS featuring DNNs was implemented
- Two flow generating software were utilized
- Two DNNs capable of detecting cyberattacks against DNP3 with accuracy as high as 99% were used

THE END

Questions?