Institute of Informatics SAS
Bratislava

Armed Forces Academy
of gen. M.R. Štefánik
Liptovský Mikuláš

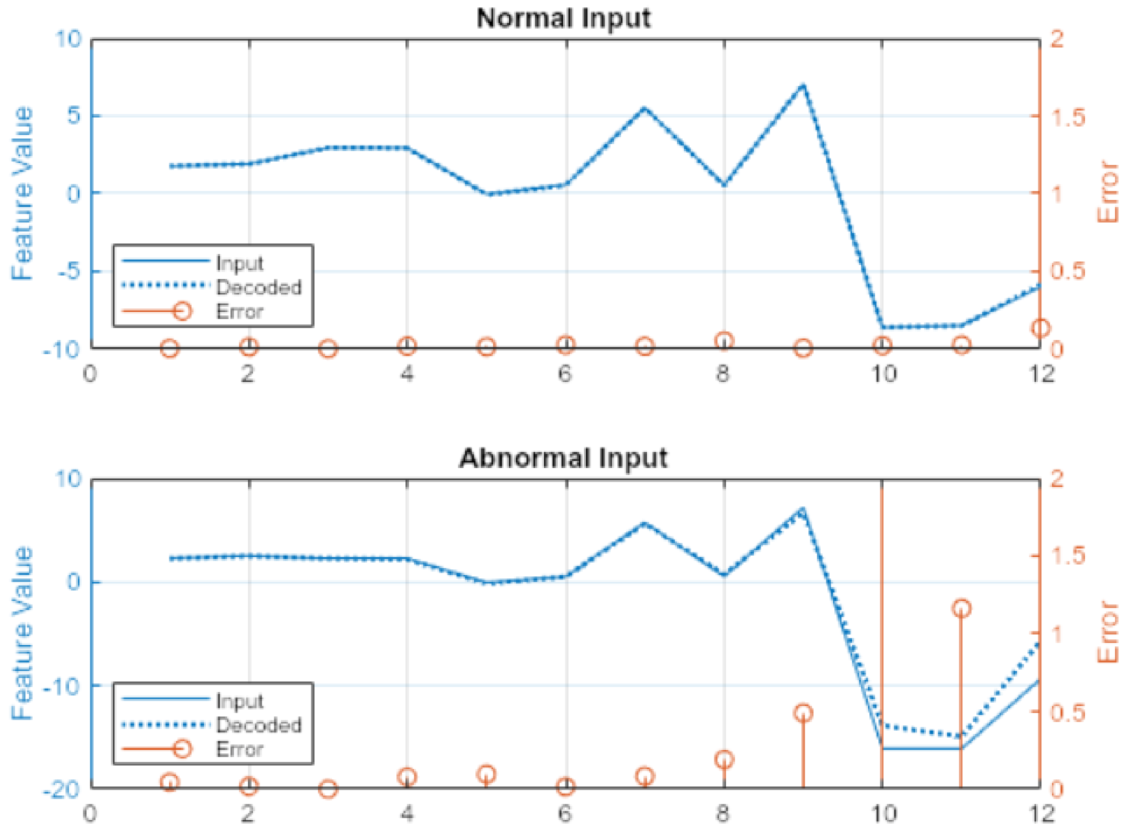
A Contribution to DDoS Attack Detection Based on Deep Neural Networks

Bianca Badidová (AOS), Radoslav Forgáč (ÚI SAV),

Miloš Očkay (ÚI SAV), Martin Javurek (AOS)

Anomaly detection in computer networks

- Process of capturing network characteristics or behaviour that is atypical of the network
- Aims to ensure network security
  - *Network monitoring*
  - *Traffic data analysis*
- Numerous approaches including
  - *Statistical methods,*
  - *streaming algorithms,*
  - *machine and deep learning methods etc.*



Neural Network Models for Effective Anomaly Detection

- One of the most commonly used approaches
- Profiles of normal and abnormal behavior
- Methods:
  - *Rule-based*
  - *Packet-based*
  - *Flow-based*

Classification ? problem

Chosen approach

- Artificial neural networks
  - *Bidirectional Long Short-Term Memory (Bi-LSTM)*
  - *Gated Recurrent Unit (GRU)*
- Dataset
  - *CIC-DDoS2019*
- Evaluation of the reconstruction error
  - *RMSE (Rooted Mean Squared Error)*
- Setting the threshold vaue
  - *Confusion matrix*
  - *Numerous experiments*
- Model results evaluation
  - *Classification metrics – Accuracy, Recall, Precision, AUC*

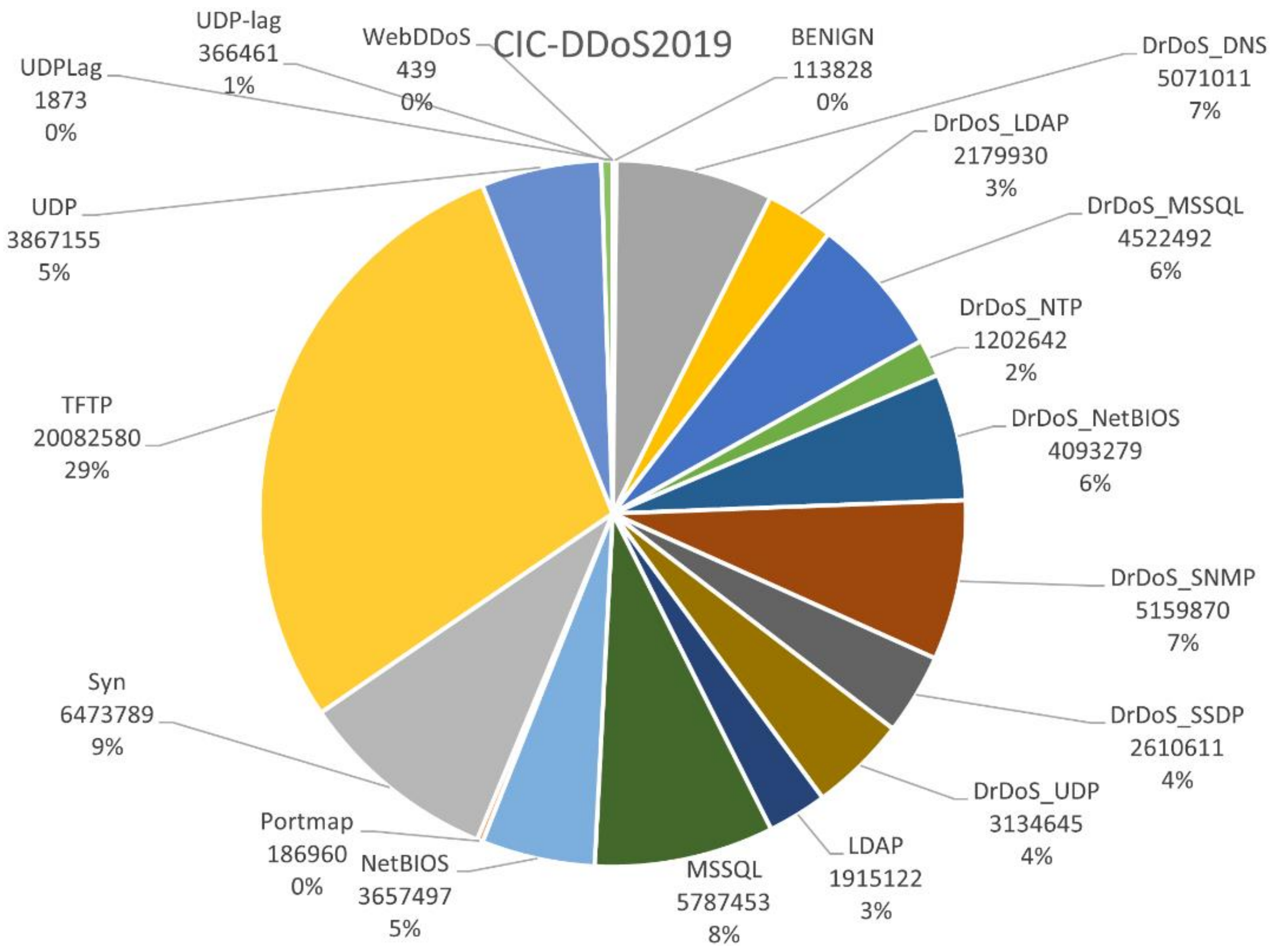
Data

- CIC-DDoS2019

2 days of traffic monitoring

70 427 637 labeled DDoS attack samples

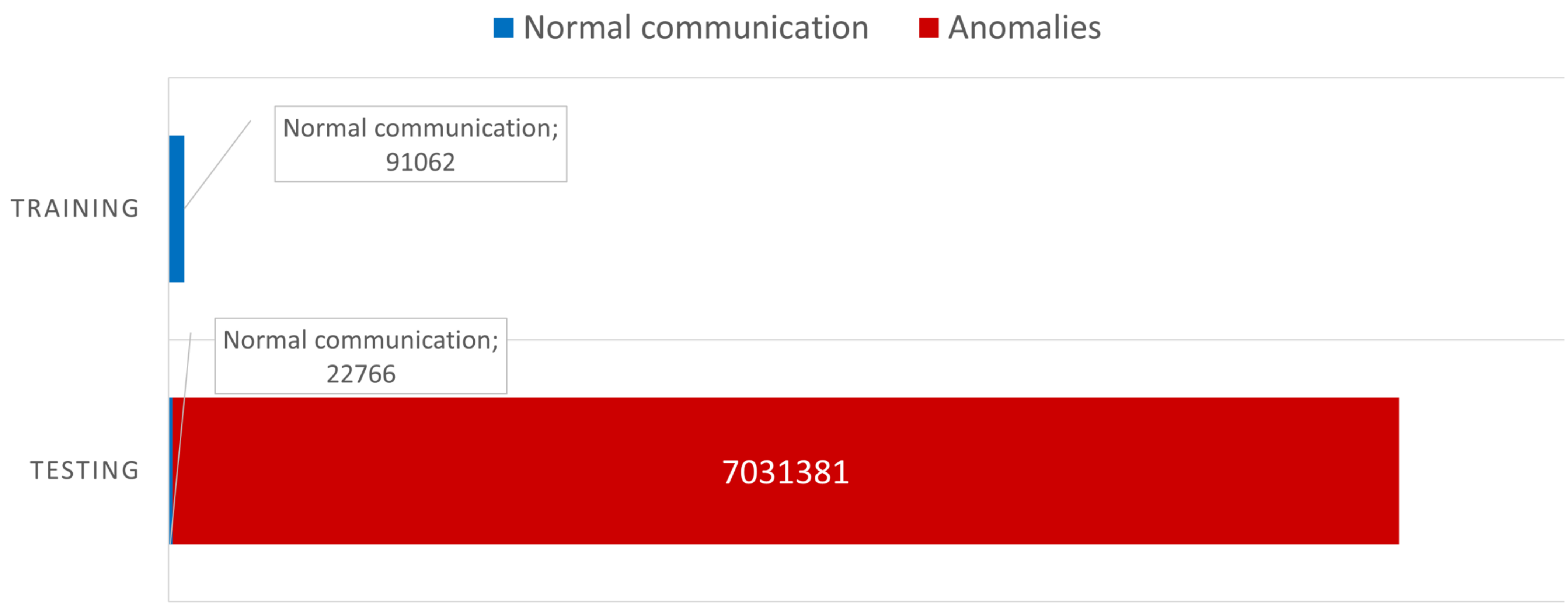
- *19 DDoS attacks*
- *0.16 % benign communication and 99.84 % attacks*


CIC-DDoS2019
BENIGN 113828 0%
DrDoS_DNS 5071011 7%
DrDoS_LDAP 2179930 3%
DrDoS_MSSQL 4522492 6%
DrDoS_NTP 1202642 2%
DrDoS_NetBIOS 4093279 6%
DrDoS_SNMP 5159870 7%
DrDoS_SSDP 2610611 4%
DrDoS_UDP 3134645 4%
LDAP 1915122 3%
MSSQL 5787453 8%
NetBIOS 3657497 5%
Portmap 186960 0%
Syn 6473789 9%
TFTP 20082580 29%
UDP 3867155 5%
UDPLag 1873 0%
UDP-lag 366461 1%
WebDDoS 439 0%

Data preprocessing

1. Reduntant features removal
2. Removal of missing and meaningless values
3. Data normalization

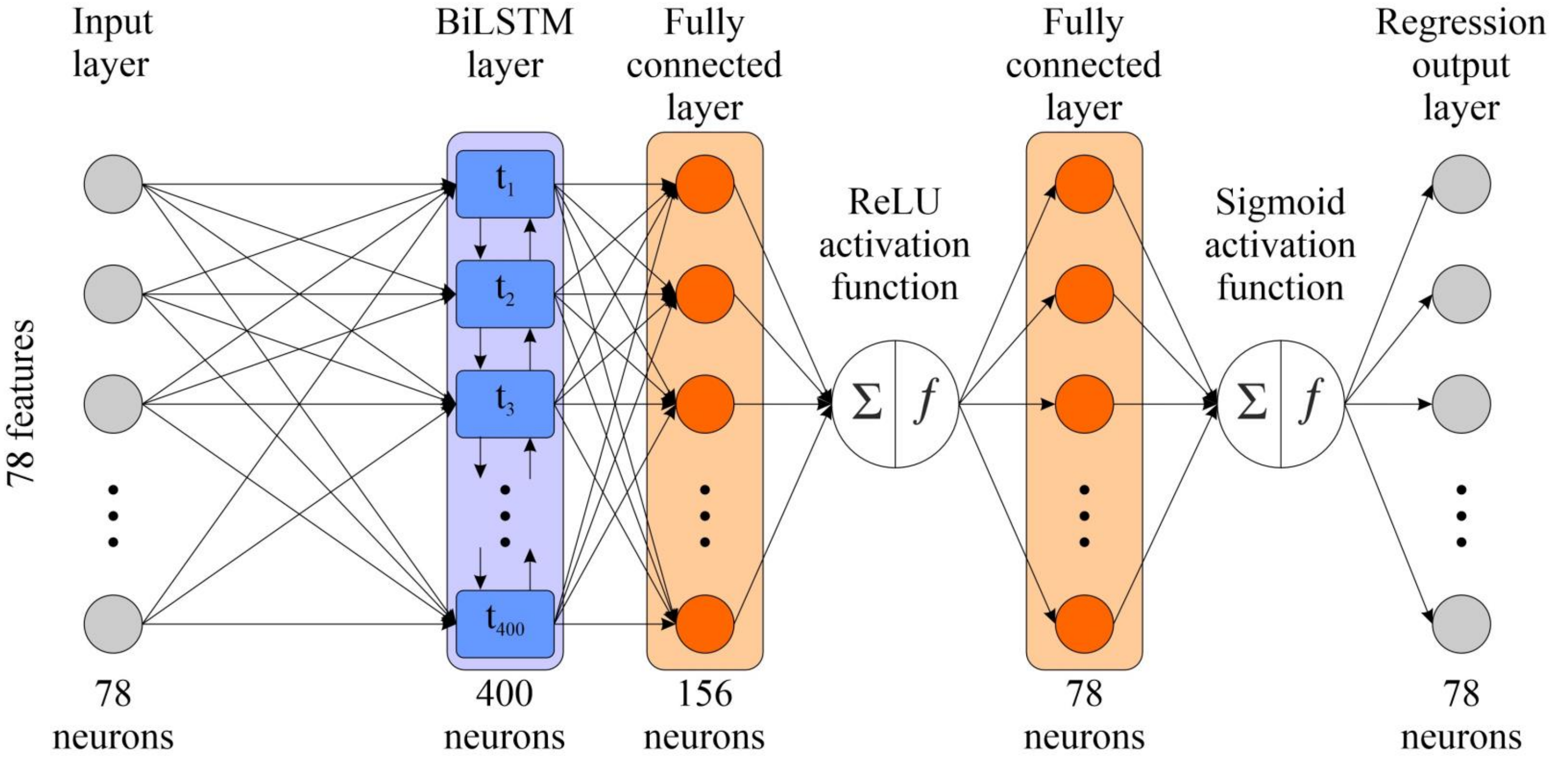
Subsets for training and evaluation



Bi-LSTM

- Deep recurrent neural network
- Input
  - 78 flow features
- Output
  - 78 reconstructed flow features

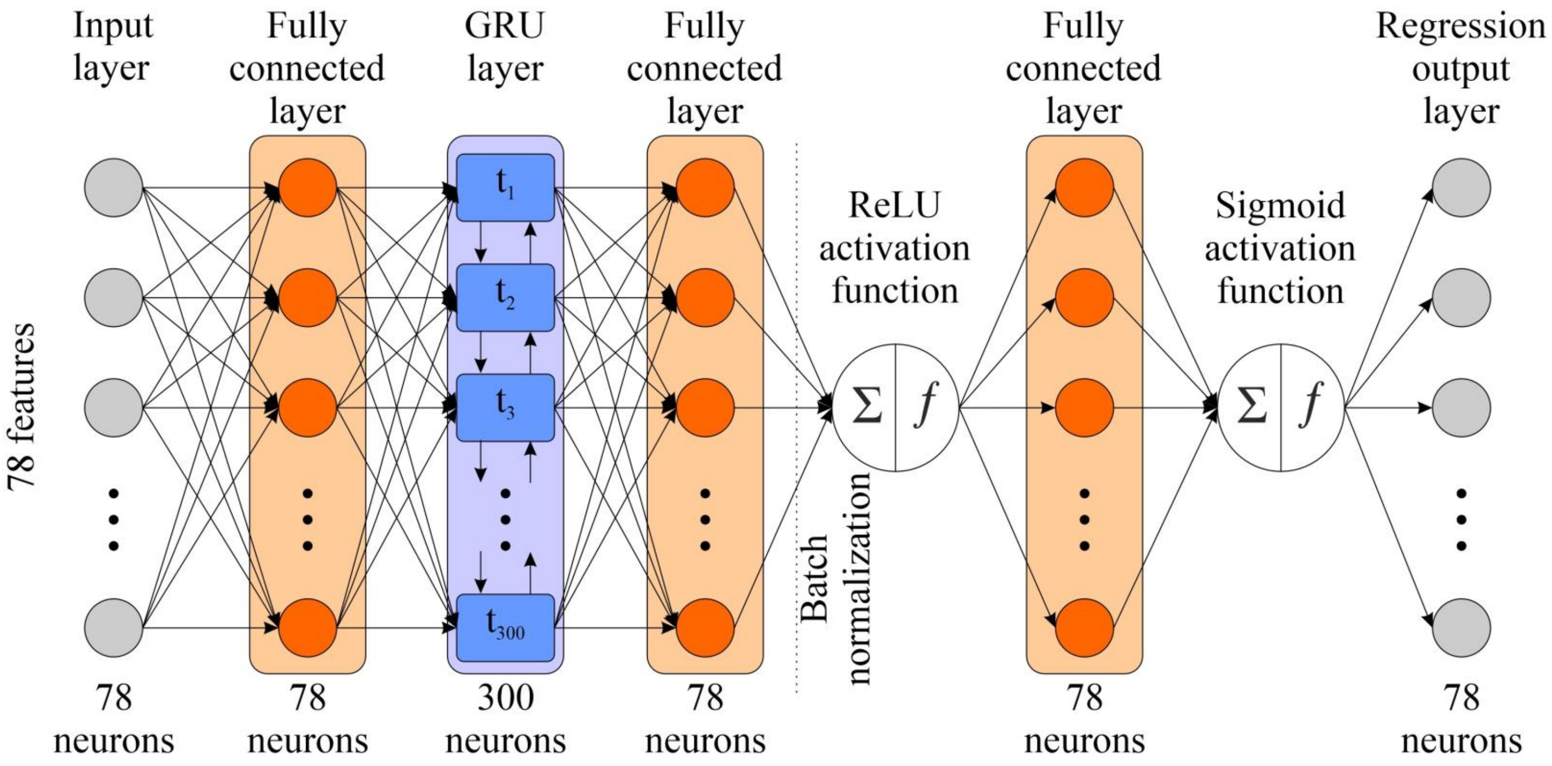
- Hyperparameters
  - Training algorithm – Adaptive moment estimation (ADAM)
  - Mini-batch size – 512
  - Learning rate – 0.001
  - Number of epochs – 10
  - Number of iterations - 1770



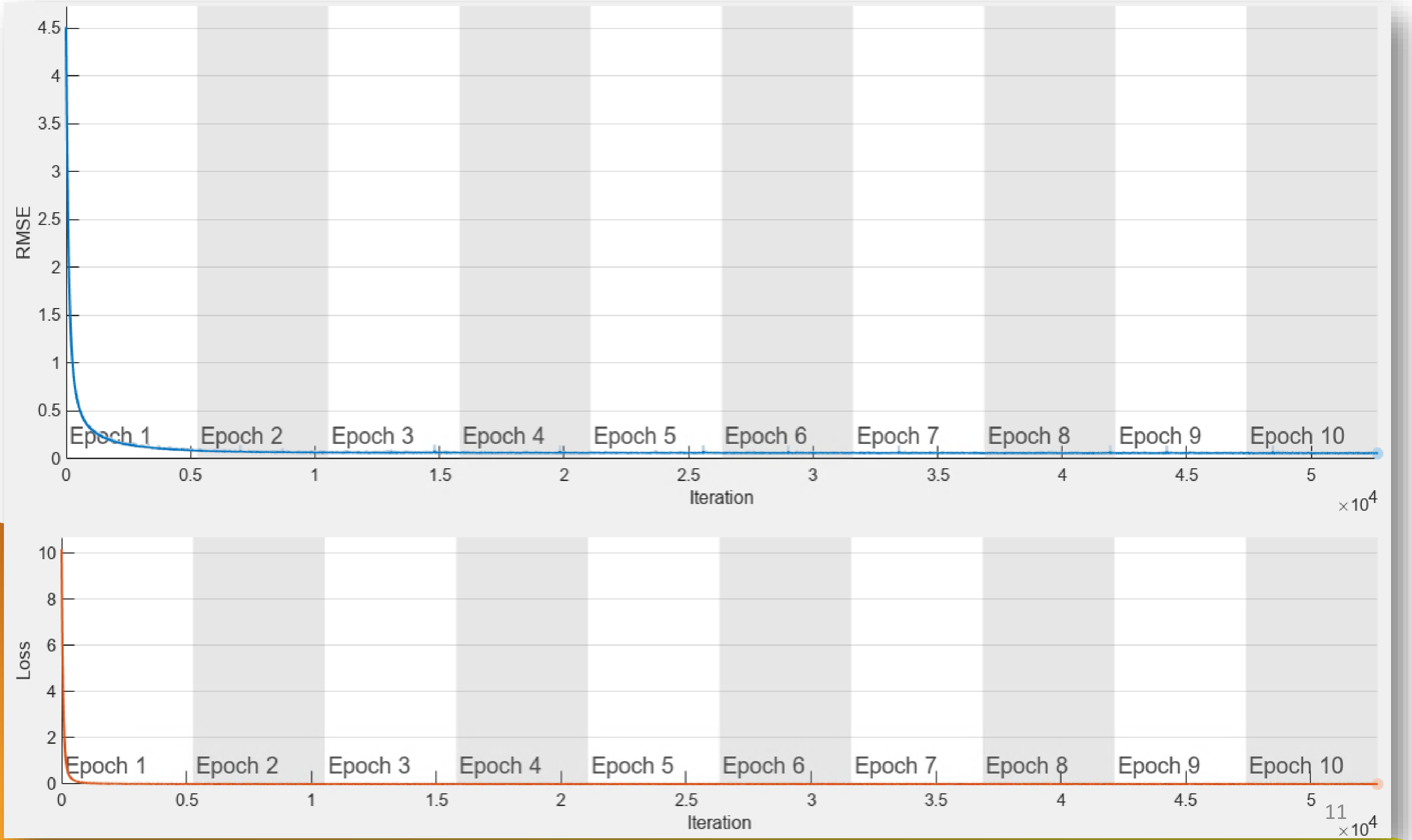
GRU

- Deep recurrent neural network
- Input
  - 78 flow features
- Output
  - 78 reconstructed flow features

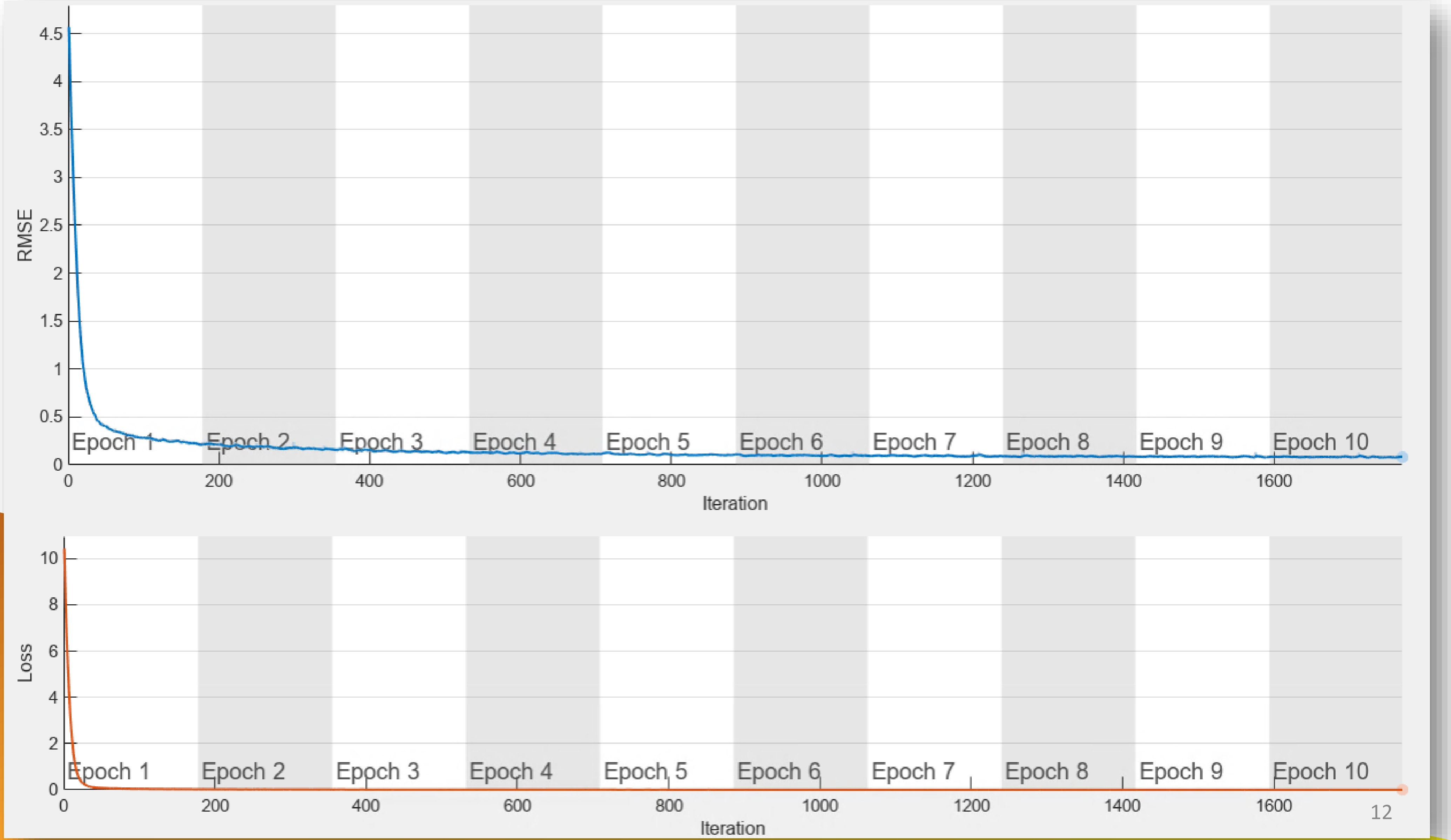
- Hyperparameters
  - Training algorithm – Adaptive moment estimation (ADAM)
  - Mini-batch size – 512
  - Learning rate – 0.001
  - Number of epochs – 10
  - Number of iterations - 1770



Bi-LSTM Training progress



GRU Training progress



Evaluation of the proposed models

TABLE I. BI-LSTM AND GRU EVALUATION

Evaluation Metric	Neural network	
	Bi-LSTM	***GRU***
Accuracy	0.962	0.959
Recall	0.962	0.960
Precision	0.999	0.999
AUC	0.956	0.943
Threshold	0.1	0.1
Training RMSE	0.14	0.008
Training RMSE loss	9.6×10^{-3}	3.4×10^{-3}

Confusion matrices

Predicted Classes

True Classes	Normal Patterns	Anomaly Patterns
Normal Patterns	21 698	1 069
Anomaly Patterns	267 027	6 764 353

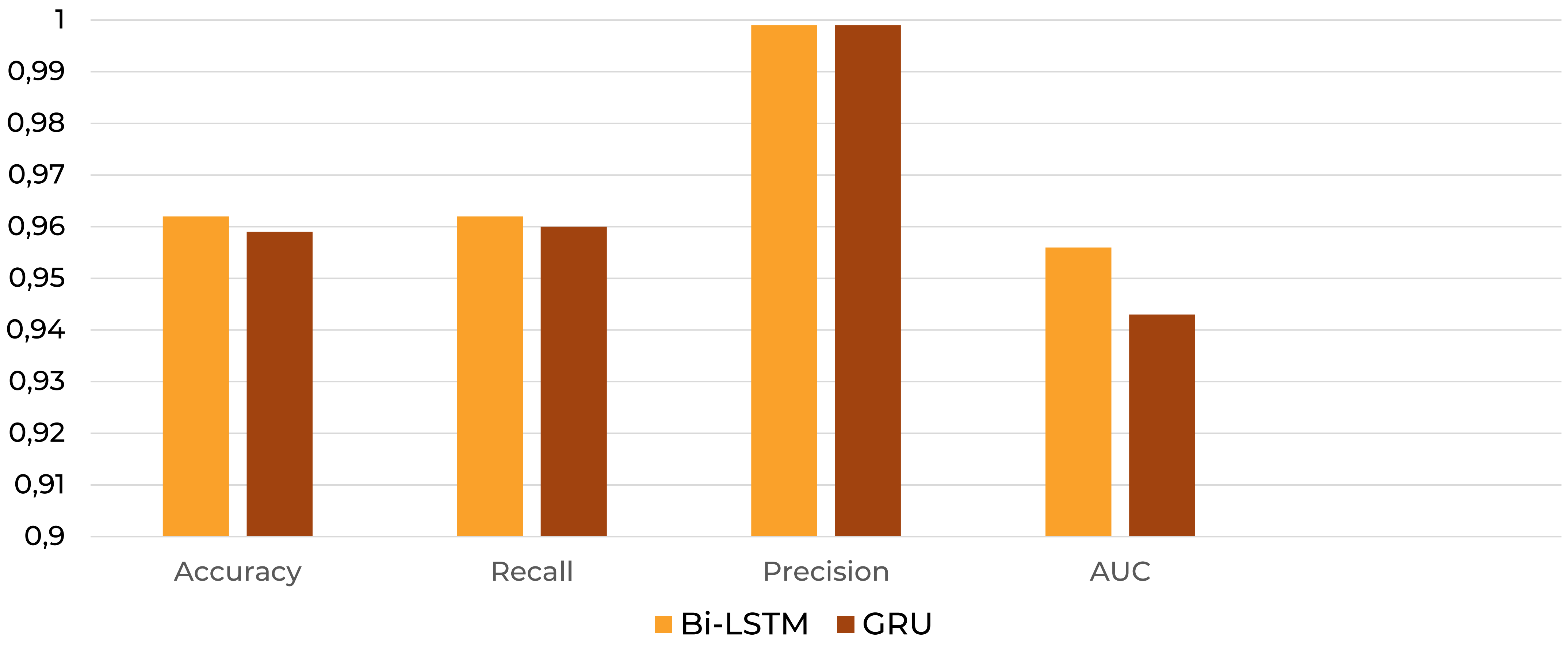
Fig. 5. Bi-LSTM Confusion Matrix

Predicted Classes

True Classes	Normal Patterns	Anomaly Patterns
Normal Patterns	21 073	1 693
Anomaly Patterns	284 729	6 746 652

Fig. 6. GRU Confusion Matrix

Comparison of results



Conclusion

- Importance of understanding the need to choose the right approach, algorithm and model for anomaly detection
  - *Available resources*
  - *Available time*
  - *Available data*
- Data selection and preprocessing
- Successful implementation of artificial intelligence methods to detect anomalies in network flows
  - *2 different topologies of neural networks – Bi-LSTM and GRU on CIC-DDoS2019 dataset*
  - *Same conditions for evaluation*
- Possibility to optimize this solution and implement it into real conditions

Thank you for your attention

Questions?