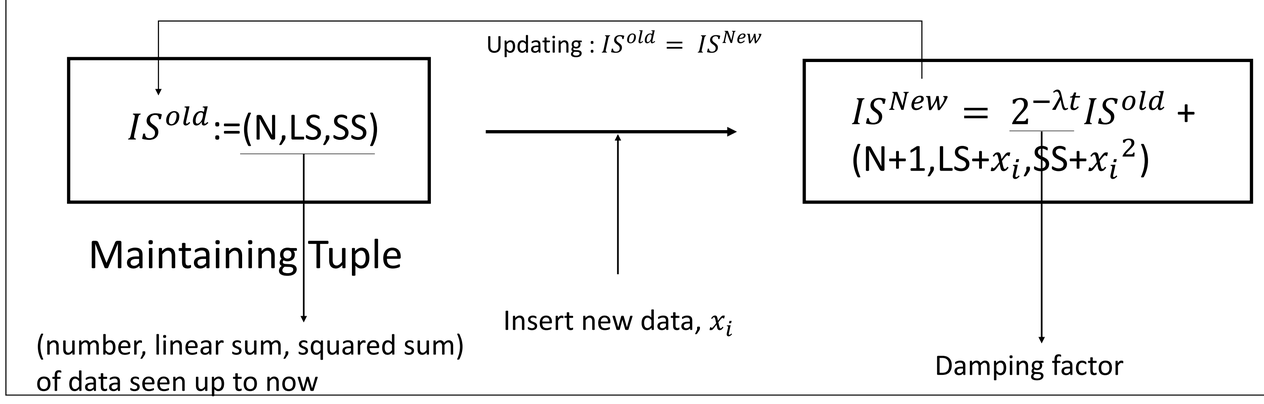
AE-NIDS : Automated Evolving SDN-based Network Intrusion Detection System

Suyeol Lee , Seungwon Shin, Korea Advanced Institute of Science and Technology, KAIST

1. Feature Extractor (From Kitsune, NDSS 2018)

Feature Extractor : extract the current behavior of a data stream

1. Damped Incremental Statistics : O(1) for updating



2. Extracted Features

- Bandwidth of the outbound traffic
- Bandwidth of the outbound and inbound traffic together
- Packet rate of the outbound traffic
- Inter-packet delays of the outbound traffic

2. Challenges and Contributions

Challenges

- Trade off between high accuracy and high recall
- Lack of self-learning
- Inefficient learning algorithm
- No consideration of distributed SDN environment

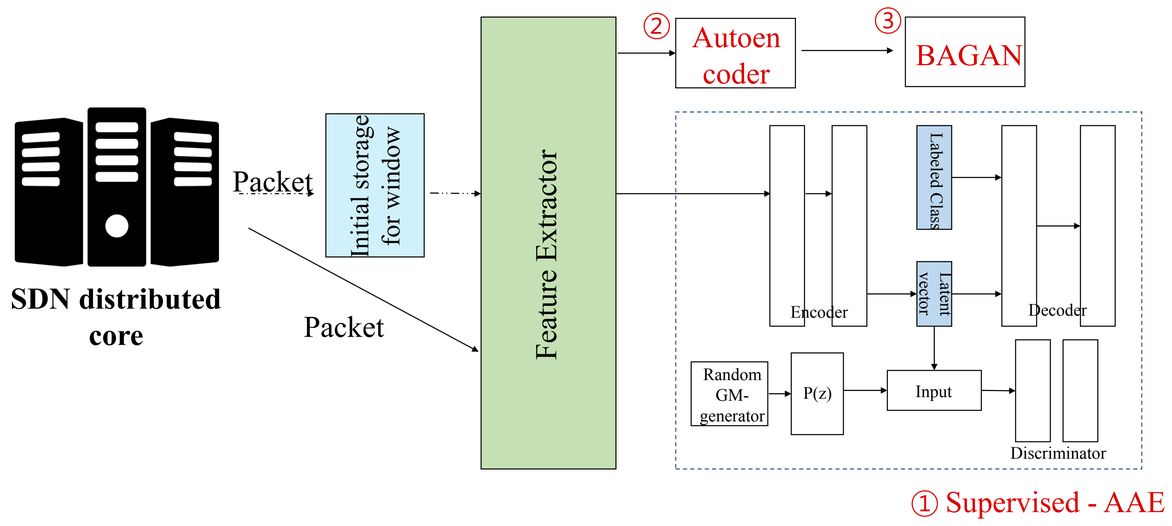
Contributions

- New system with AAE and distance-based automated learning
- Introduce GAN for augmenting imbalanced data and continual learning(EWC)
- Introduce one tool for classification and latent vector learning; AAE
- Federated learning for scalabitiy

2. AE-NIDS design

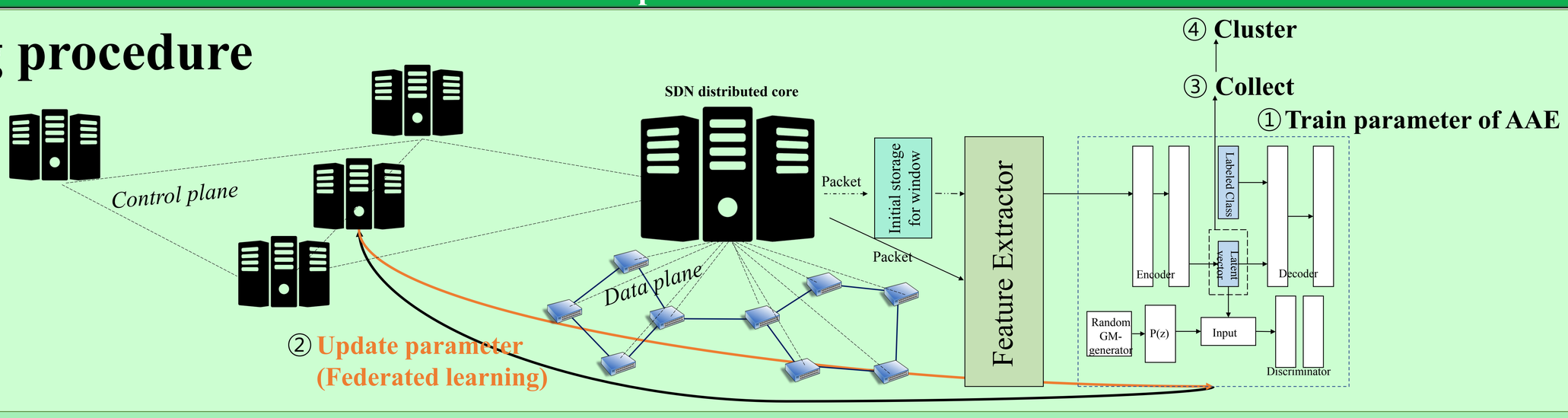
AE-NIDS on each distribued SDN core

= Three deep neural network [1. Supervised – AAE 2. Autoencoder 3.BAGAN] + Feature Extractor

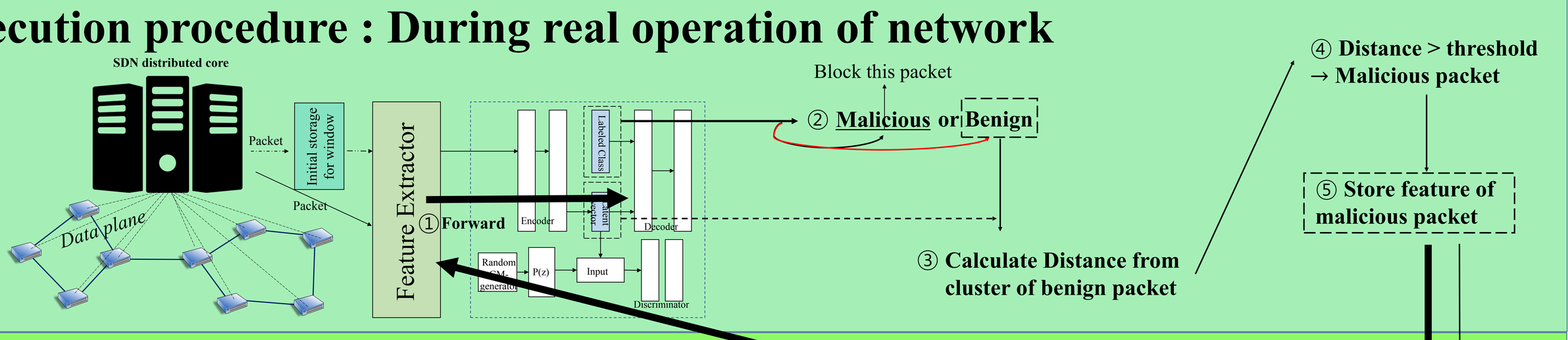


3. AE-NIDS procedures

1. Pre-training procedure



2. Execution procedure : During real operation of network



3. Updating procedure