1. Damped Incremental Statistics: \( IS_{old} = (N, IS, SS) \)

Maintaining Tuple

Input: 
- New data, \( x_i \)

Output: 
- Updated IS

\[ IS_{new} = 2^{-\lambda} IS_{old} + (N + 1, IS + x_i, SS + x_i^2) \]

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 scalability

3. AE-NIDS procedures

1. Pre-training procedure

2. Execution procedure: During real operation of network

3. Updating procedure

---

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

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

**Feature Extractor**

- extract the current behavior of a data stream

**1. Pre-training procedure**

**2. Execution procedure**

- 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

**3. Updating procedure**

---

**AE-NIDS on each distributed SDN core**

- Three deep neural network

---

**AE-NIDS design**

- SDN distributed core
- Feature Extractor
- Collect
- Train parameter of AAE
- Cluster
- Autoencoder
- BAGAN
- Distance > threshold
- Malicious packet
- Store feature of malicious packet
- Return to Execution procedure
- Update parameter of AAE with continual learning (EWC)
- If total number of stored packet data is enough

---

**AE-NIDS procedures**

- Feature Extractor (From Kitsune, NDSS 2018)