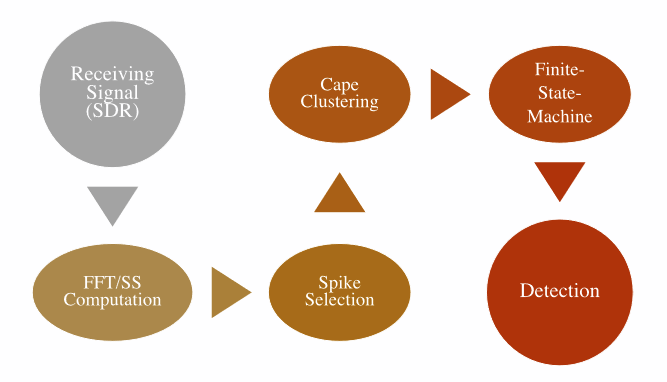
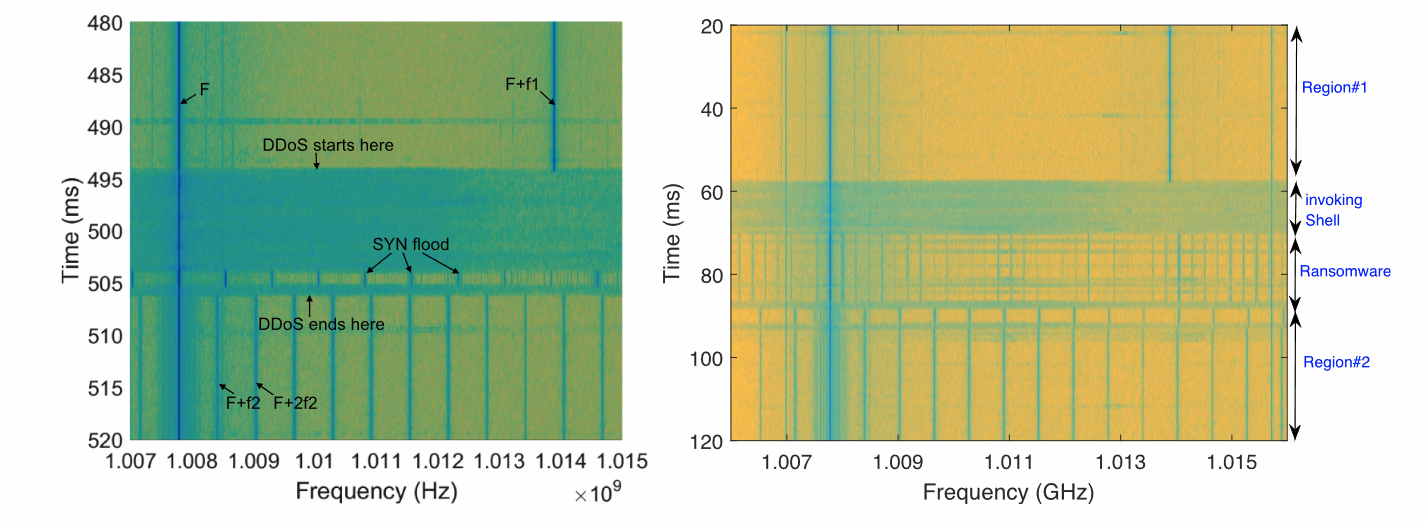
# 10 REMOTE: Robust External Malware Detection Framework by Using Electromagnetic Signals

Nader Sehatbakhsh , Alireza Nazari , Monjur Alam, Frank Werner, Yuanda Zhu, Student Member, IEEE, Alenka Zajic , Senior Member, IEEE, and Milos Prvulovic , Senior Member, IEEE

* Main Idea: The use of radio and other EM sensors to detect aberrant behavior in IoT devices -- detections made by Clustering/Finite state machine model
* Details
  + EM sensors detecting IoT device emissions
    - Small electromagnet probe at 5cm from IoT device
    - Horn radio antenna at 1m from IoT device
  + Arduino/Syringe setup used as proxy for any potential remote device
    - Somewhat resembles the concept of a garage door opener but with a syringe
  + CAPE distance metric clustering
  + Finite-State-Machine as detector
* Challenges/problems and limitations
  + EM interference
  + Overhead and upkeep costs of deploying sensor hardware in IoT
* Evaluation methods and results
  + Penetration testing; Acc.: ~99.9%
* Source:
  + Code: N/A // Some pseudocode in paper
  + Data: Self-Generated
* Screenshots:

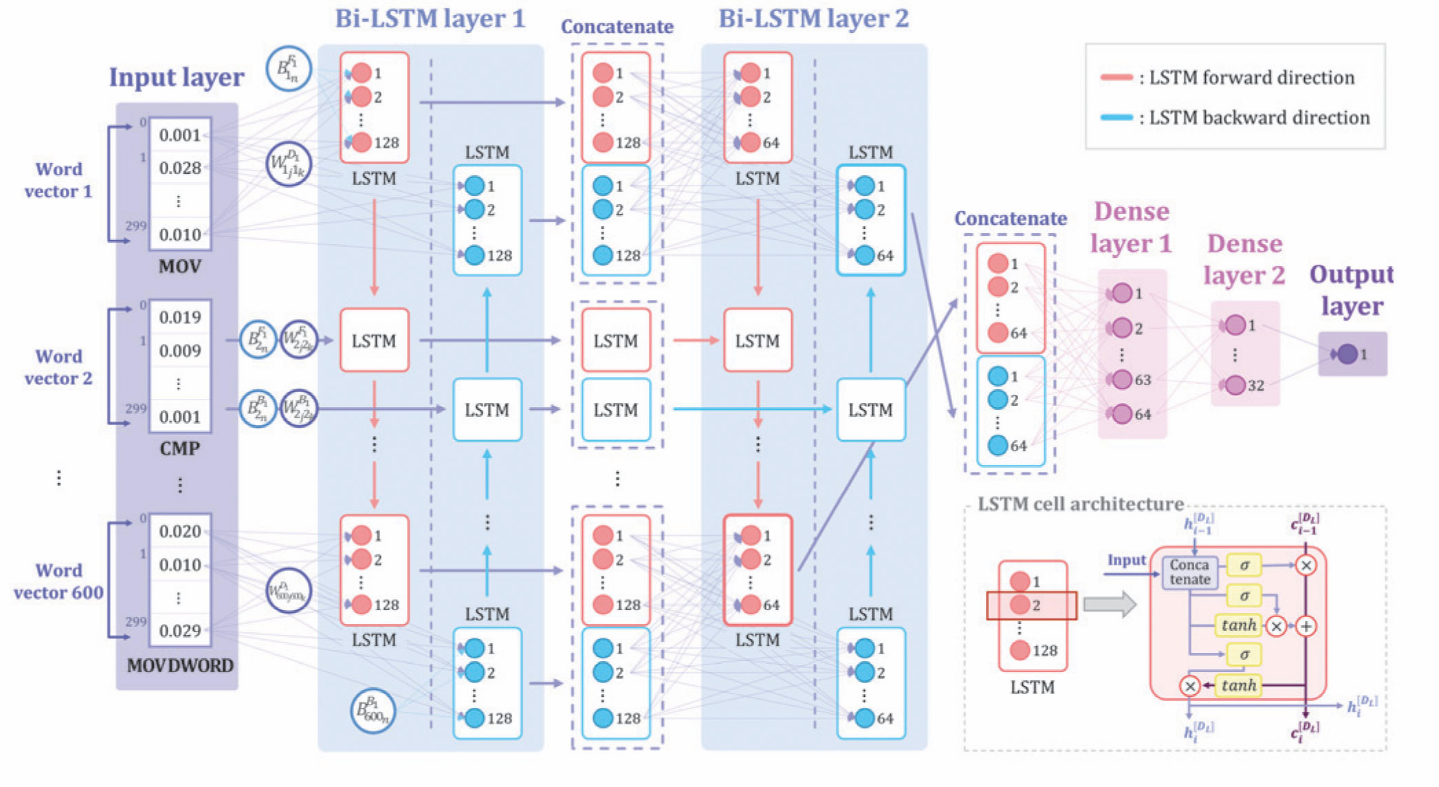
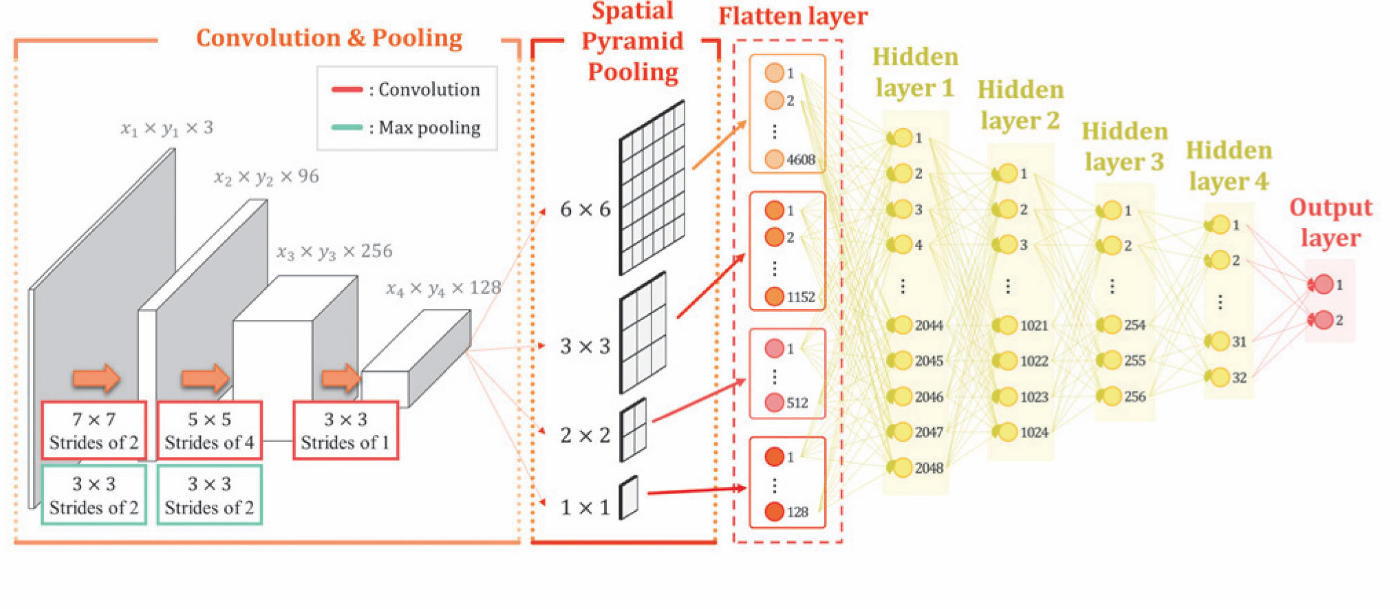


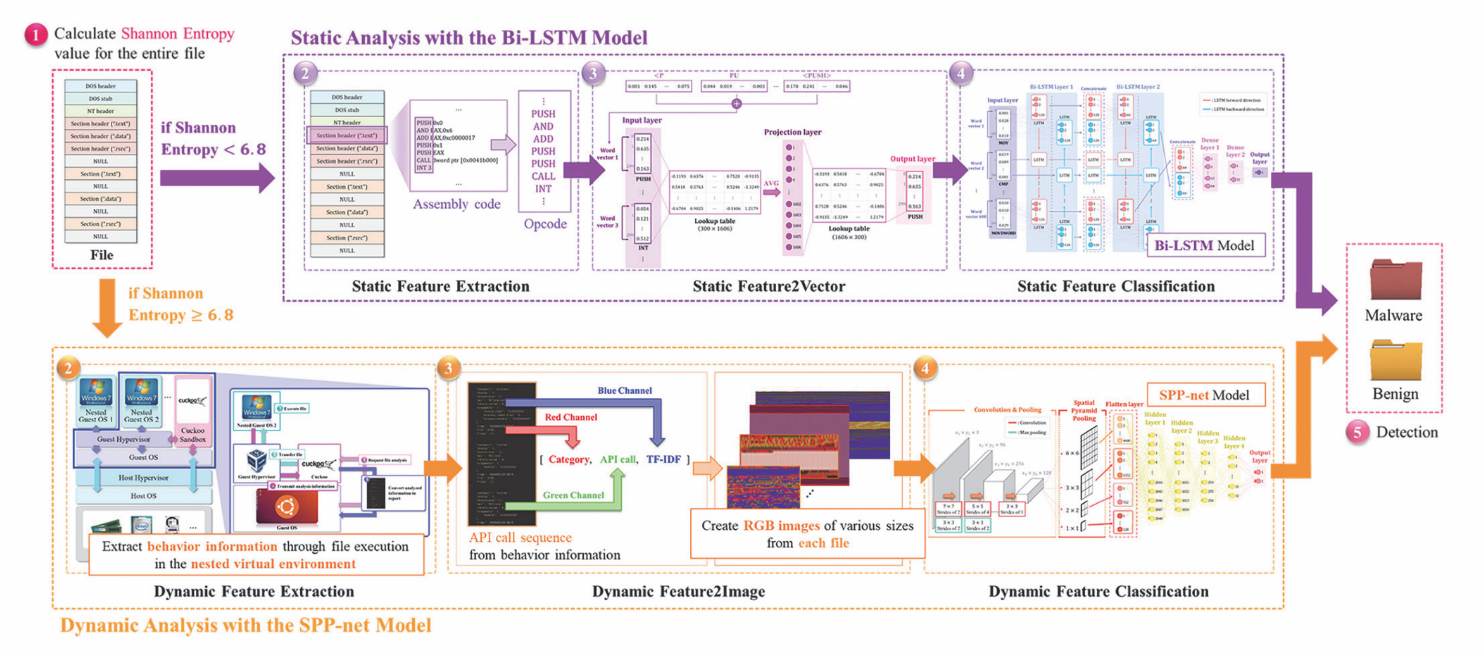


# 13 Hybrid Malware Detection Based on Bi-LSTM and SPP-Net for Smart IoT

Jueun Jeon , Byeonghui Jeong , Seungyeon Baek , and Young-Sik Jeong , Member, IEEE

* Main Idea: multi-model system which uses Shannon Entropy to specify which files are better classified by which model (Bi-LSTM or SPP-Net)
* Details
  + SPP-Net CNN
    - Dynamic feature extraction w/ Cuckoo Sandbox
    - API call sequence data as RGB image
  + Bi-LSTM
    - Static assembly code feature extraction
    - Vector embedding
* Challenges/problems and limitations
  + Data imbalance problem was solved using resampling
    - E.g. More goodware in existence than distinct malware
  + This generates a new problem concerning generalizability -- resampled data does not account for the lack of distinct data but merely artificially expands dataset size
* Evaluation methods and results:
  + Entropy breakpoints tested at 6.8, 7.0 and 7.2
  + Best performance achieved:
    - HyMalD w/ 6.8 entropy breakpoint; acc.: 92.50%
  + 50/50 train/test cross-validation testing of model substructures and cross-reference against alternatives
    - LSTM vs Bi-LSTM
      * Acc.: 87.09% vs 92.09%
    - SPP-Net vs CNN
      * Acc.: 93.3% vs 91.24%
* Source:
  + Code: N/A
  + Data:
    - VirusShare
    - KISA-data challenge 2019-Malware.04, provided by the Korea Internet & Security Agency
* Screenshots:





# 14 CNN-Based Malware Variants Detection Method for Internet of Things

Qi Li, Jiaxin Mi , Weishi Li, Junfeng Wang , and Mingyu Cheng

* Main Idea:
  + Static Features represented as RGB image -> self-attention module to consider global contexts missed by standalone CNN -> 4 convolutional layers using ReLU
* Details
  + [IDA Pro](https://hex-rays.com/ida-pro) malware disassembler used for feature extraction
  + Binary/Opcode/ExtractedStrings used as R/G/B values for constructed images
  + Linear Algebra Covariance matrix used to relate code segments to global code
  + Model uses Keras malware package (Tensorflow backend)
* Challenges/problems and limitations
  + Lossy encoding
    - All bytes which do not map to Assembly Opcodes are encoded as identical
* Evaluation methods and results
  + Cross-validation-- 95.31% accuracy (dataset 1 [IoT only]) / 98.57% accuracy (dataset 2 [other platforms + IoT])
    - Classification of malware families -- benign uncategorized
  + Cross-reference accuracy/precision/recall/F1 with other models in the field
    - LeNet, ResNet, Inception, Xception models tested
    - Also tested different variations on image encoding from cited papers
* Source:
  + Code: N/A (some pseudocode in paper)
  + Data - 10,000+ samples across 2 datasets:
    - <https://github.com/guitmz/mirror-vxheaven.org>
      * Authors Cite: <https://vt.netlux.org/index.html> but it no longer exists
    - <https://virusshare.com/>
    - <https://www.stratosphereips.org/datasets-malware>
* Screenshots:

