Nuclear Security and Emerging Disruptive Tech: The Impact of Cyber and AI,
March 22, 2018

Intrusion Detection Based on Deep Learning

Overview and Further Challenges

Prof. Kwangjo Kim

Cryptology and Information Security Lab

KAIST School of Computing

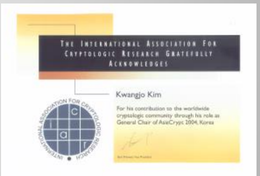
Graduate School of Information Security

Contents

Speaker

- **Contact Information**
  - Room 901@N1, 042-350-3550, 010-9414-1386
  - E-mail: kkj@kaist.ac.kr Home page: http://caislab.kaist.ac.kr/kkj
- **Career**
  - '79 ~ '97 : Section Head of Coding Tech. #1 in ETRI
  - '99 ~ '00 : Visiting Professor at Univ. of Tokyo, Japan
  - '99 ~ '05 : Director of IACR / Institute for IT-gifted Youth
  - '98 ~ '09 : Professor / Dean of School of Engineering in ICU
  - '02 : 1000 World Leaders of Scientific Influence by ABI
  - '05 ~ '06 : Visiting Scholar at MIT/UCSD
  - '09.1~12 : President of KIISC
  - '09.3 ~ : Professor in CSD@ KAIST, Honorable President of KIISC
  - '12.1~8 : Visiting Professor at KUSTAR, UAE
  - '13.1(7)~2(8) : Visiting Professor at ITB, Indonesia
  - '14 : Who's who in the world (ABI) & 2000 Outstanding Intellectuals of the 21st Century (IBC)
  - '15 : H. President of KIISC, Korean Representative to IFIP TC11
  - '17 : Fellow of IACR


- **Academic Activities**
  - More than 100 Program Committee Members of Crypto and Security Conferences
  - General Chair of Asiacrypt2004, and CHES2014
  - More than 20 invited talks to international conferences
  - Editor-in-Chief, Cryptography, MDPI online Journal

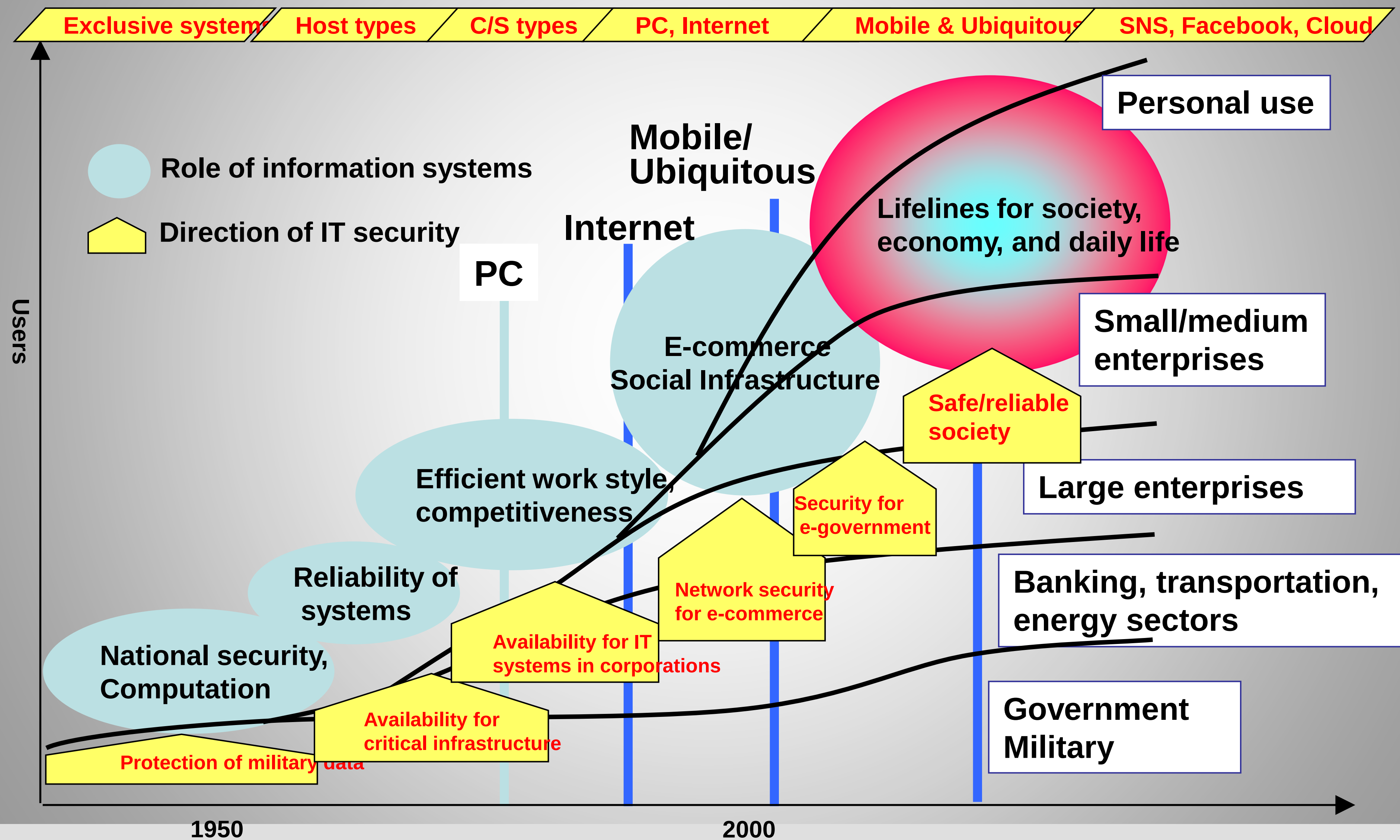


- **Course offered / Fluent Language**
  - CS448, CS548 / English, Japanese, Korea
- **Awards**
  - Presidential Appreciation('02.),Presidential Citation ('09.9), Minister of NIS ('09.12)


- **Hobby**
  - Driving, Mountain Climbing, Cycling, Skiing, Rafting, etc.




Trends of ICT Security



KAIST

History of Cyber Attacks in Korea (in Part)

2009
- 77DDoS happened

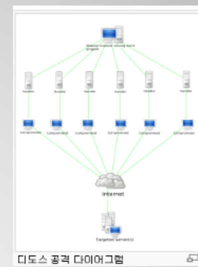
2010
- Military HQ for Cyber Security established

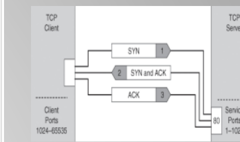
2011
- Law on Personal Privacy enforced
- 34DDoS happened

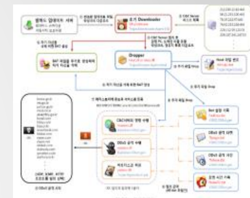
2012
- Information Security day, 2nd Wed. in July

2013
- 320 Cyber terror to Korean Banks, etc
- 625 Cyber terror to Web page@BH. etc

2014
- 100 Million personal informations leaked in 3 major credit cards
- KEPCO hacking

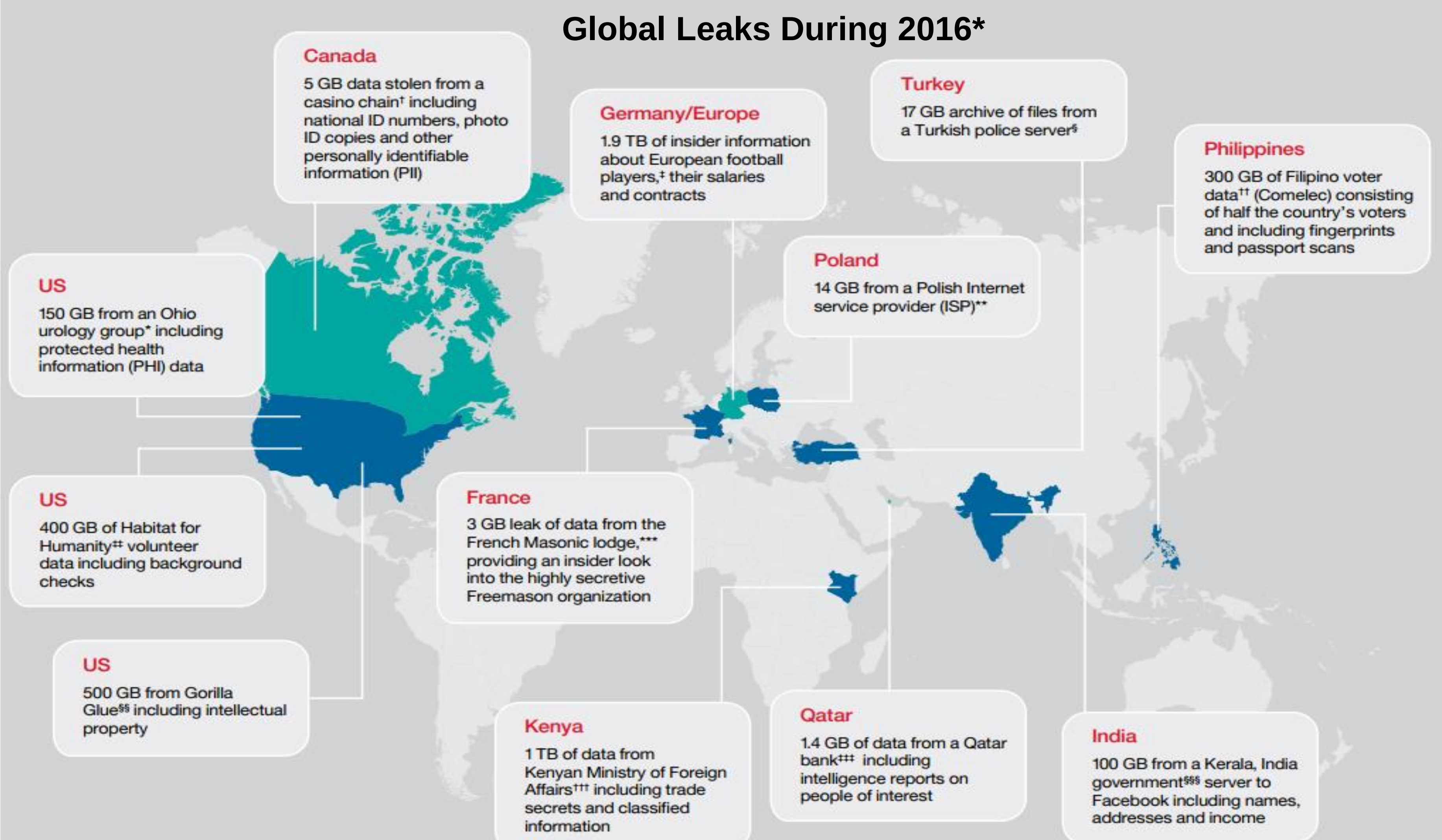






3rd Asiacrypt2011 in Korea

Global Attacks in 2016 (1/2)

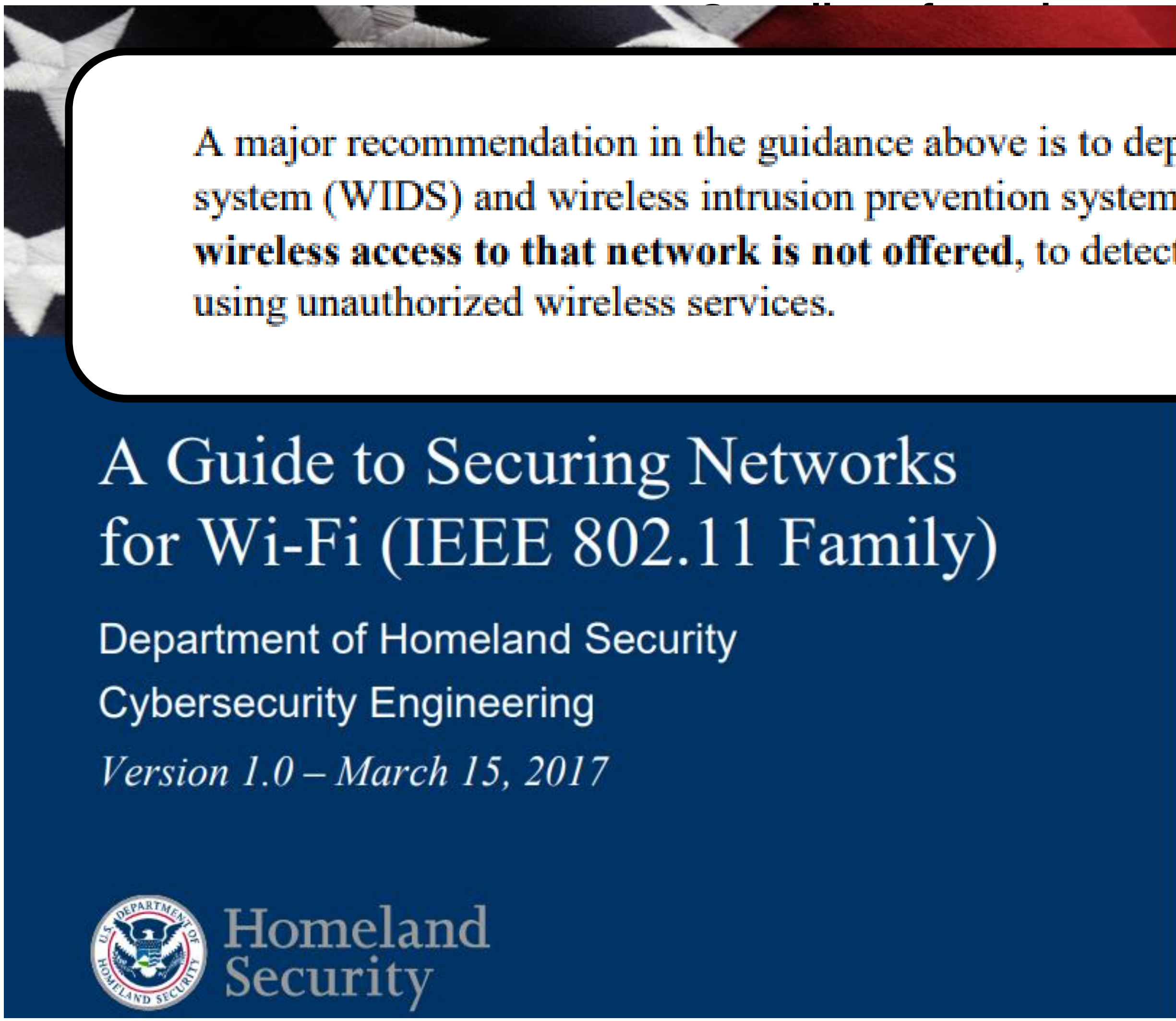


https://www-01.ibm.com/marketing/iwm/dre/signup?source=urx-13655&S_PKG=ov57325

KAIST

Global Attack in 2016 (2/2)

A major recommendation in the guidance above is to deploy a wireless intrusion detection system (WIDS) and wireless intrusion prevention system (WIPS) on every network, **even when wireless access to that network is not offered**, to detect and automatically disconnect devices using unauthorized wireless services.

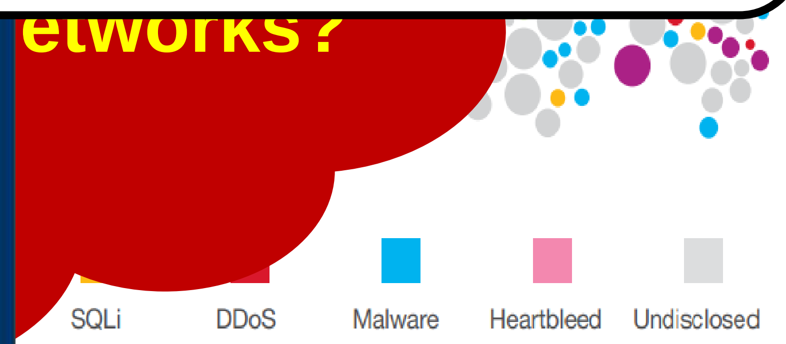


A Guide to Securing Networks for Wi-Fi (IEEE 802.11 Family)

Department of Homeland Security
Cybersecurity Engineering

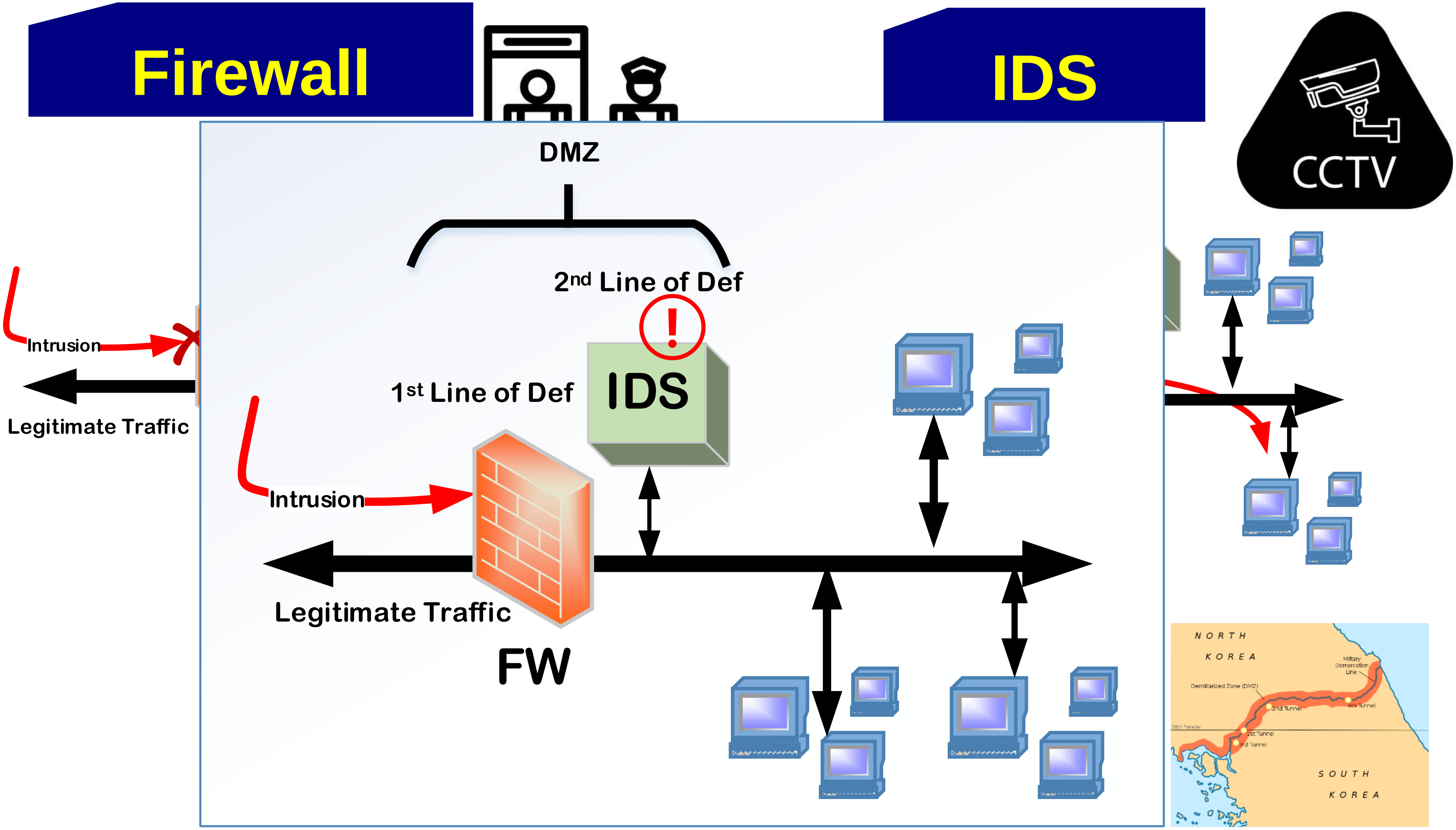
Version 1.0 – March 15, 2017

Homeland Security



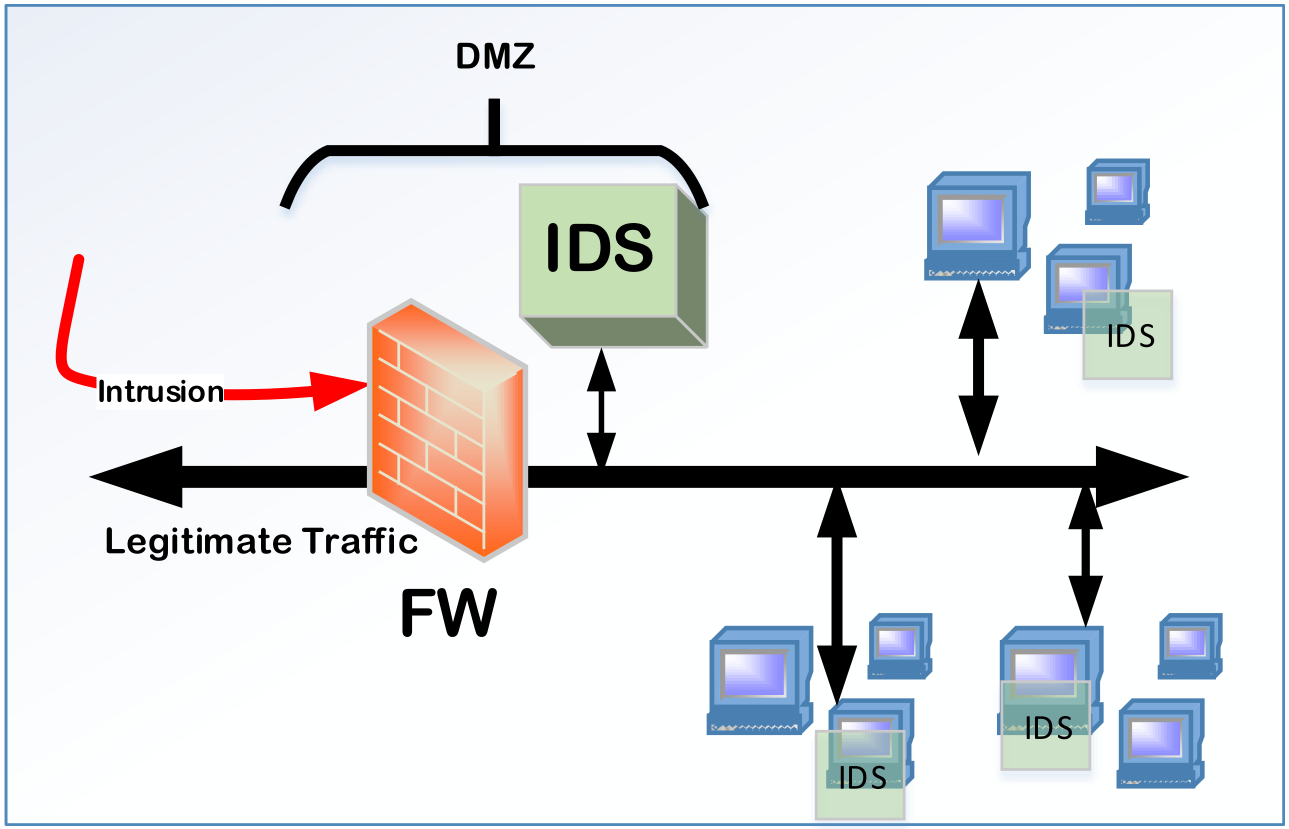
_PKG=ov57325

KAIST


Firewall
IDS
CCTV
DMZ
2nd Line of Def
1st Line of Def
IDS
Intrusion
Legitimate Traffic
Intrusion
Legitimate Traffic
FW
NORTH KOREA
SOUTH KOREA

Types of IDS (location) (1/2)

- Network-based
- Host-based
- Hybrid



KAIST

Types of IDS (methodology) (2/2)

- *Misuse-based*: detects any attack by checking whether the attack characteristics match previously stored signatures or patterns. This also known as signature-based IDS.

- *Anomaly-based*: identifies malicious activities by profiling normal behavior and then measuring any deviation from it. It leverages s tatistical analysis or machine-learning.

- *Specification-based*: manually defines a set of rules and constrain ts to express the normal operations. Any violation of the rules and constraints during execution is flagged as an attack.

Comparion of IDS

	Misuse-based	Anomaly-based	Specification-based
Method	Identify known attack patterns	Identify unusual activity patterns	Identify violation of pre-defined rules
Detection Rate	High	Low	High
False Alarm Rate	Low	High	Low
Unknown Attack Detection	Incapable	Capable	Incapable
Drawbacks	Updating signatures is burdensome	Computing any statistical or machine-learning is heavy	Relying on expert knowledge to define rules is undesirable

Learning : Supervised vs Unsupervised

- Unknown attack detection: Detects new attacks without prior knowledge

	Supervised	**Unsupervised**
Definition	The data are labeled with pre-defined classes.	The data are labeled **without** pre-defined classes
Method	Classification	Clustering
Example	• Support Vector Machine (SVM) • Decision Tree (DT) • Fuzzy Inference System (FIS)	• *k*-means Clustering, • Density-based Spatial Clustering of Applications with Noise (DBSCAN) • Ant Clustering Algorithm (ACA)
Known Attack DR	High	Low
Unknown Attack DR	Low	High

KAIST

Tree of Deep Learning

- ANN, SAE, RBM, DBN, CNN, *etc*

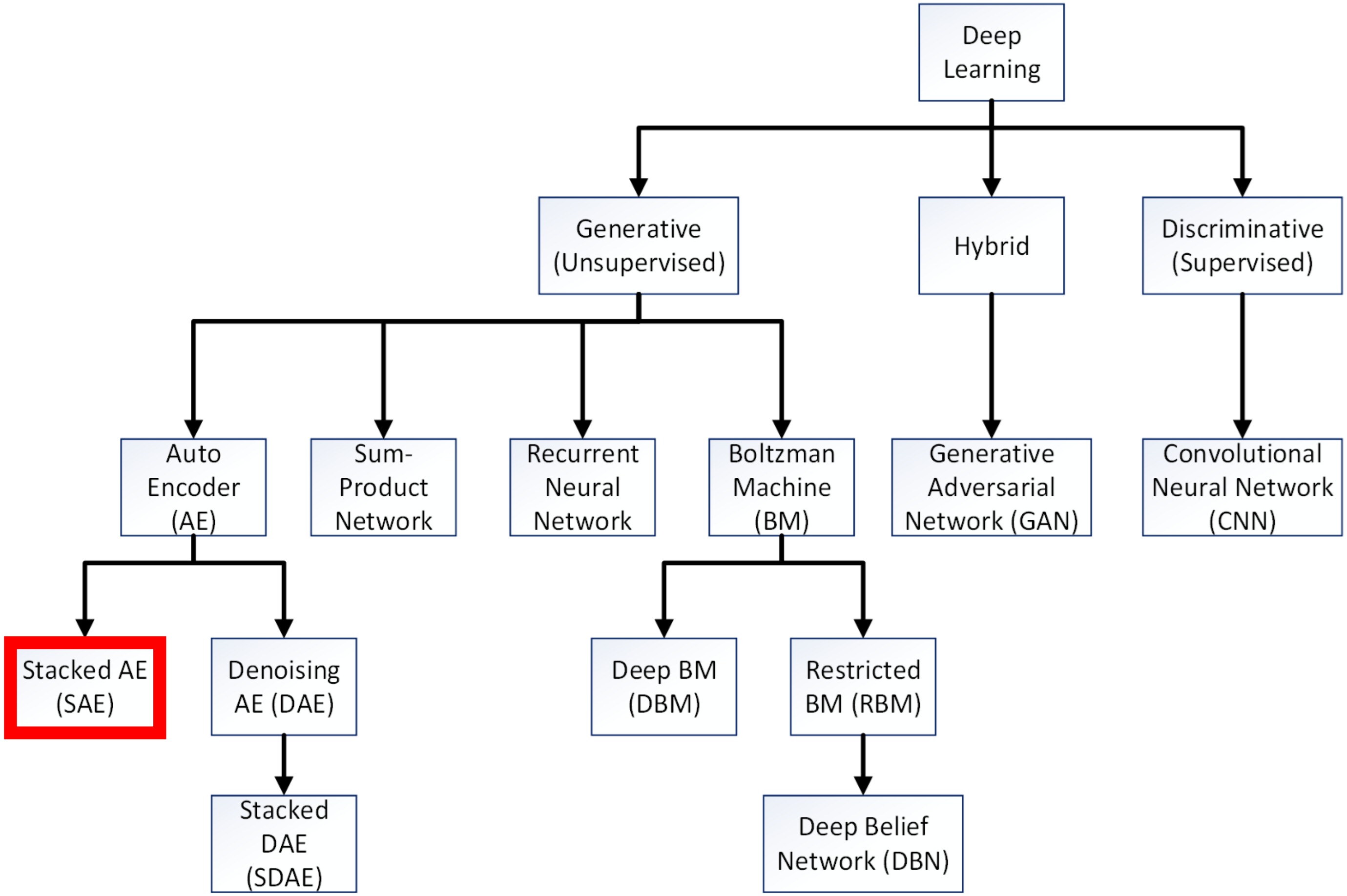


Figure from Aminanto, M.E. and Kim, K.J., "*Deep Learning in Intrusion Detection System: An Overview*", International Research Conference on Engineering and Technology-IRCET 2016, Jun. 28-30, 2016, Bali, Indonesia.

Deep Learning-Based IDSs (1/6)

- DNN (Deep Neural Network)

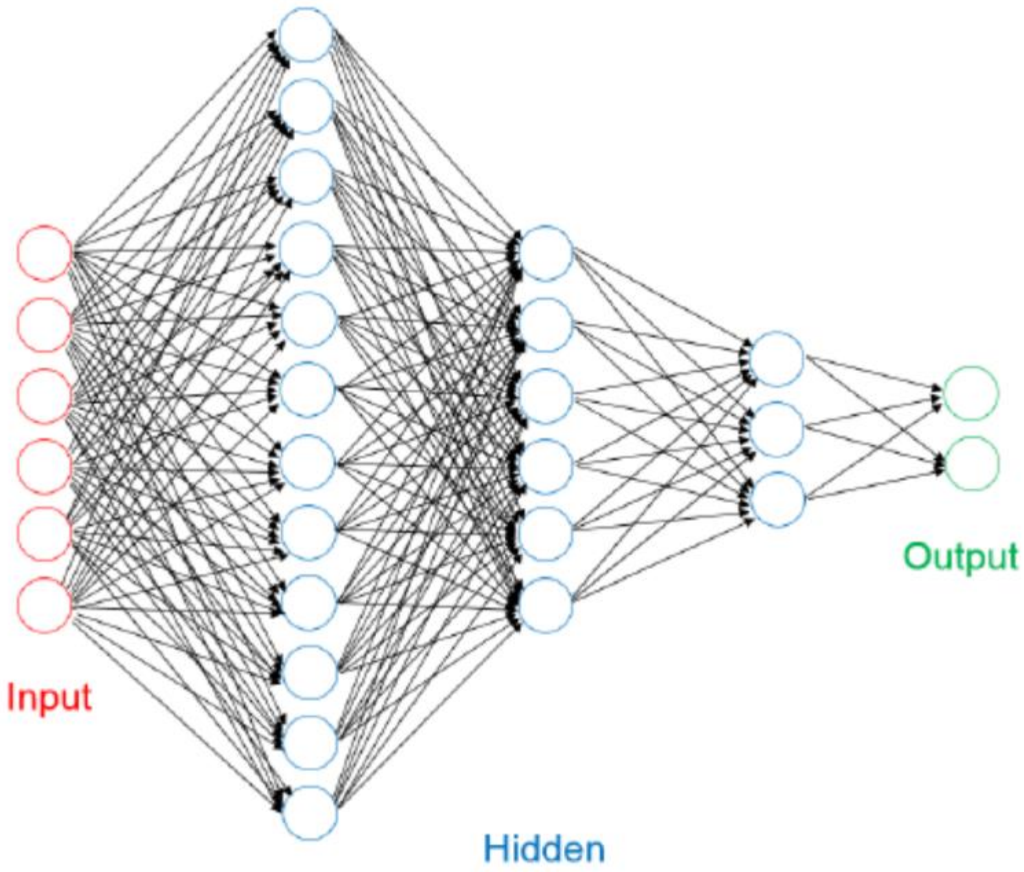


Figure from T. A. Tang, L. Mhamdi, D. McLernon, S. A. R. Zaidi, and M. Ghogho, "Deep learning approach for network intrusion detection in software defined networking," in Wireless Networks and Mobile Communications (WINCOM), 2016 International Conference on. IEEE, 2016, pp. 258–263.

1. T. A. Tang, L. Mhamdi, D. McLernon, S. A. R. Zaidi, and M. Ghogho, "Deep learning approach for network intrusion detection in software defined networking," in Wireless Networks and Mobile Communications (WINCOM), 2016 International Conference on. IEEE, 2016, pp. 258–263.
2. S.S. Roy, A. Mallik, R. Gulati, M.S. Obaidat, and P. Krish-na, "A deep learning based artificial neural network approach for intrusion detection," in International Conference on Mathematics and Computing. Springer, 2017, pp. 44–53.
3. S. Potluri and C. Diedrich, "Accelerated deep neural networks for enhanced intrusion detection system," in Emerging Technologies and Factory Automation (ETFA), 2016 IEEE 21st International Conference on. IEEE, 2016, pp. 1–8.

- LSTM-RNN (Recurrent NN)

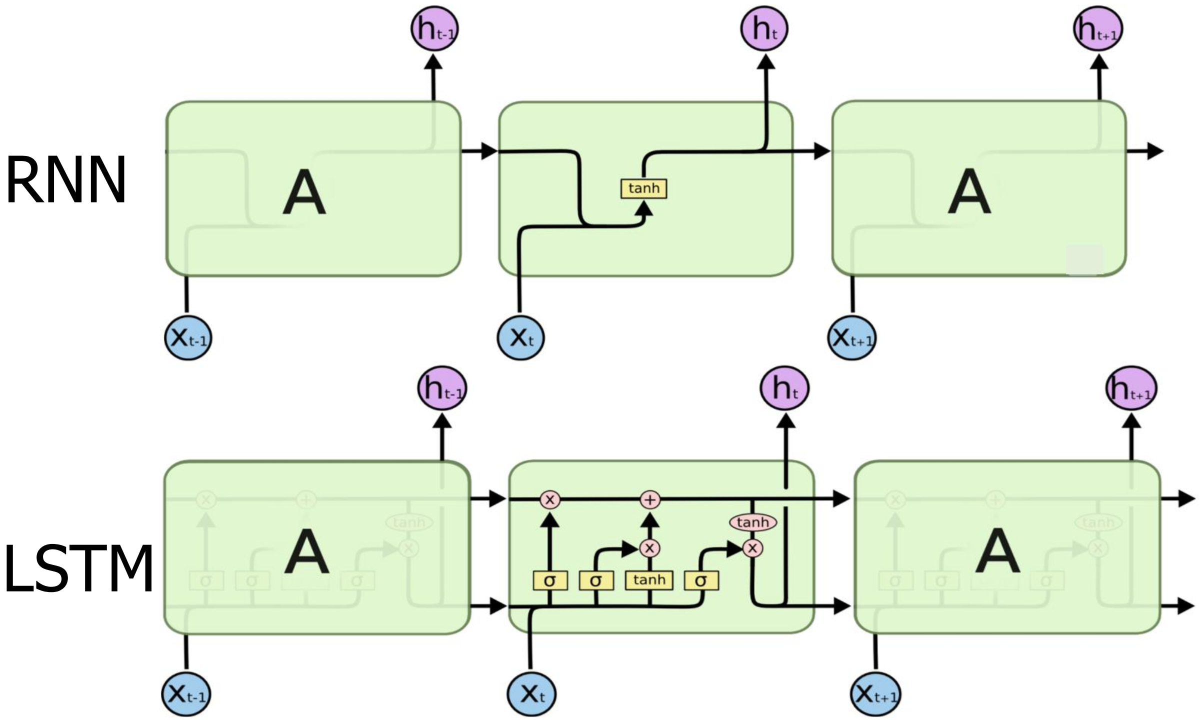


Figure from C. Olah, “Understanding LSTM networks,” http://colah.github.io/posts/2015-08-Understanding-LSTMs/, 2015, [Online; accessed 20-February-2018].

1. J. Kim, J. Kim, H. L. T. Thu, and H. Kim, “Long short term memory recurrent neural network classifier for intrusion detection,” in Platform Technology and Service (PlatCon), 2016 International Conference on. IEEE, 2016, pp. 1–5.
2. Y. LIU, S. LIU, and Y. WANG, “Route intrusion detection based on long short term memory recurrent neural network,” DEStech Transactions on Computer Science and Engineering, no.cii, 2017.
3. C. Yin, Y. Zhu, J. Fei, and X. He, “A deep learning approach for intrusion detection using recurrent neural networks,” IEEE Access, vol. 5, pp. 21 954–21 961, 2017.
4. R. C. Staudemeyer, “Applying long short-term memory recurrent neural networks to intrusion detection,” South African Computer Journal, vol. 56, no. 1, pp. 136–154, 2015.
5. L. Bontemps, J. McDermott, N.-A. Le-Khac et al., “Collective anomaly detection based on long short-term memory recurrent neural networks,” in International Conference on Future Data and Security Engineering. Springer, 2016, pp. 141–152.
6. M. K. Putchala, “Deep learning approach for intrusion detection system (ids) in the internet of things (iot) network using gated recurrent neural networks (gru),” Ph.D. dissertation, Wright State University, 2017.
7. P. K. Bediako, “Long short-term memory recurrent neural network for detecting ddos flooding attacks within tensorflow implementation framework.” 2017.

- CNN (Convolutional Neural Network)

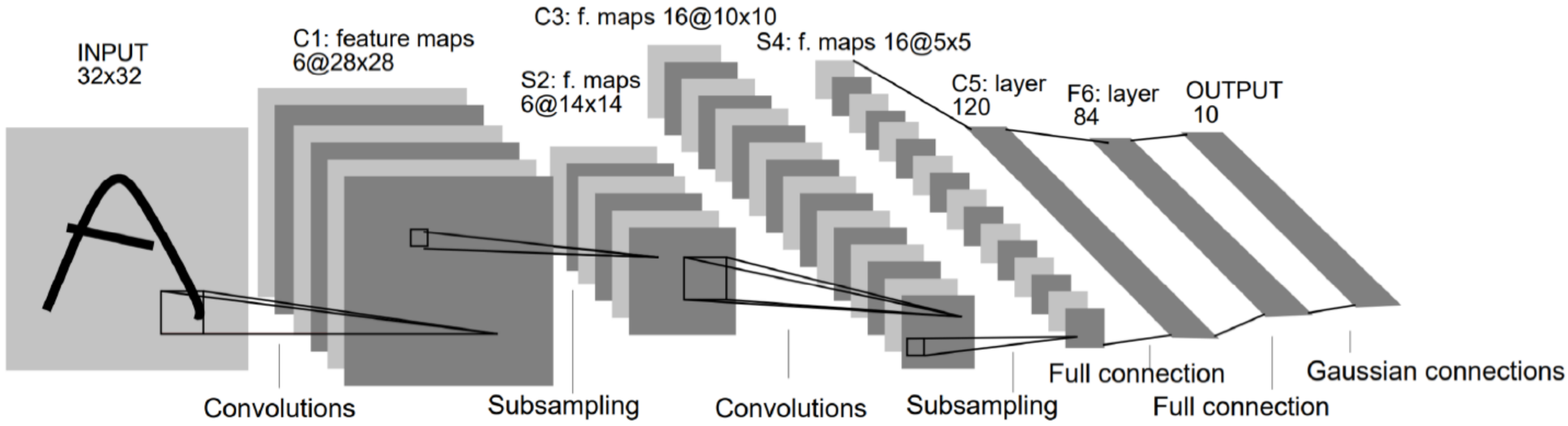
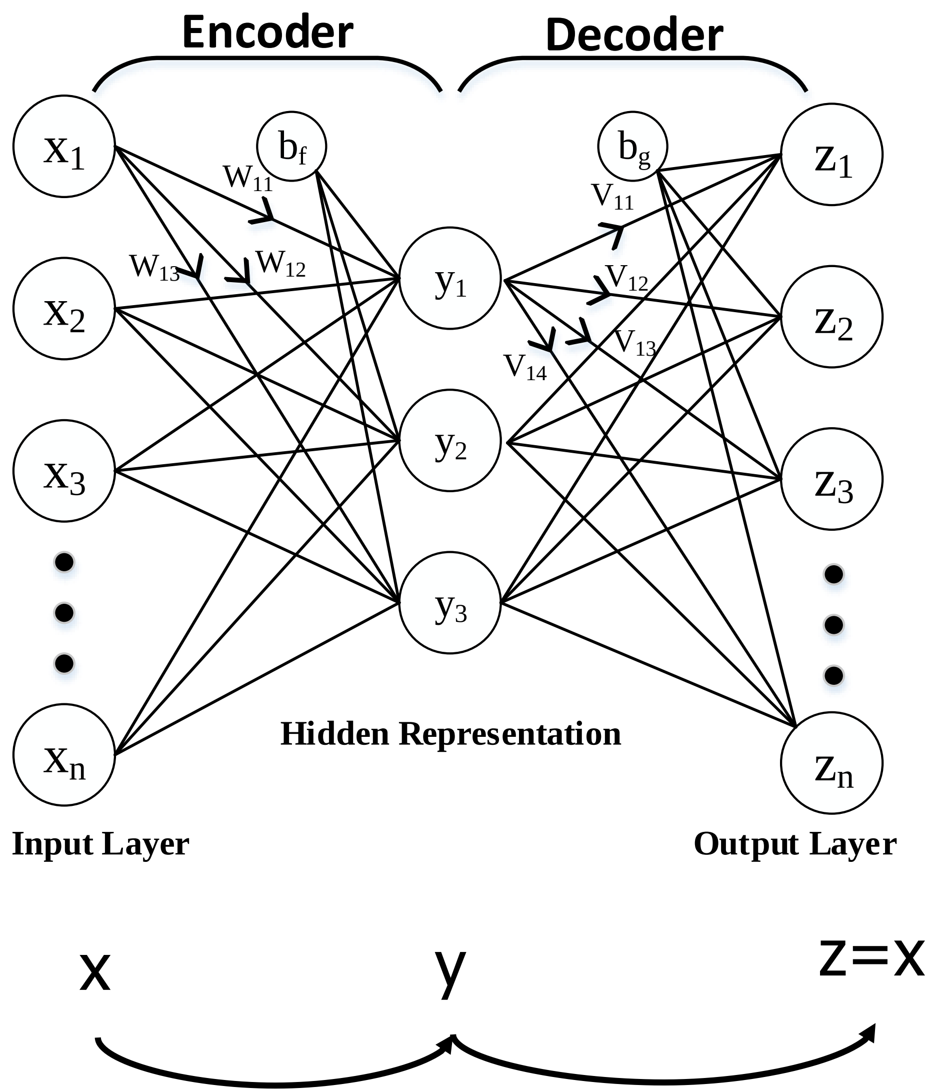


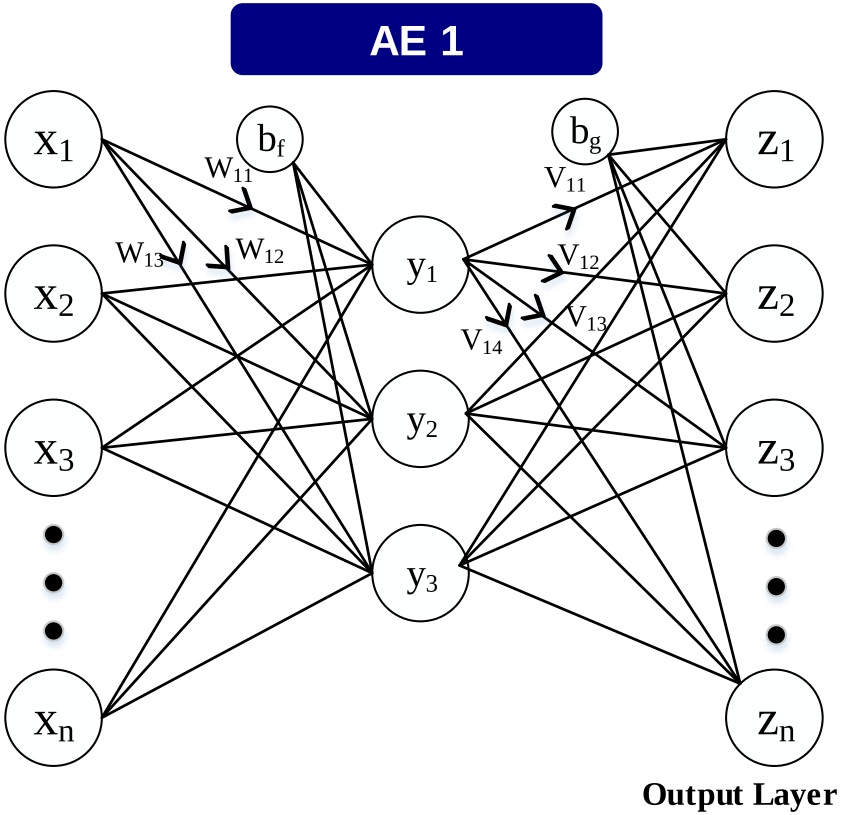
Figure from Y. LeCun, L. Bottou, Y. Bengio, and P. Haffner, "Gradient-based learning applied to document recognition," Proceedings of the IEEE, vol. 86, no. 11, pp. 2278–2324, 1998.

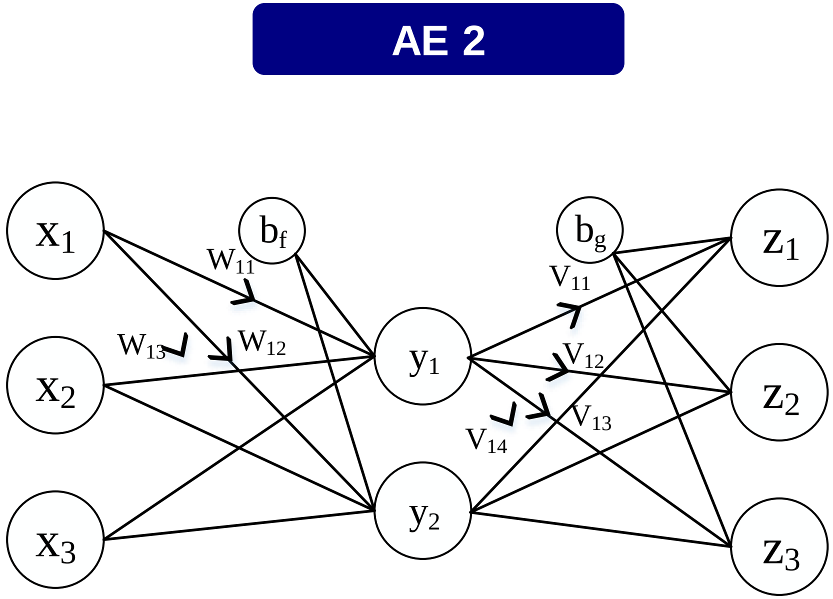
1. Z. Li, Z. Qin, K. Huang, X. Yang, and S. Ye, "Intrusion detection using convolutional neural networks for representation learning," in International Conference on Neural Information Processing. Springer, 2017, pp. 858–866.

- AE (Auto-Encoder)

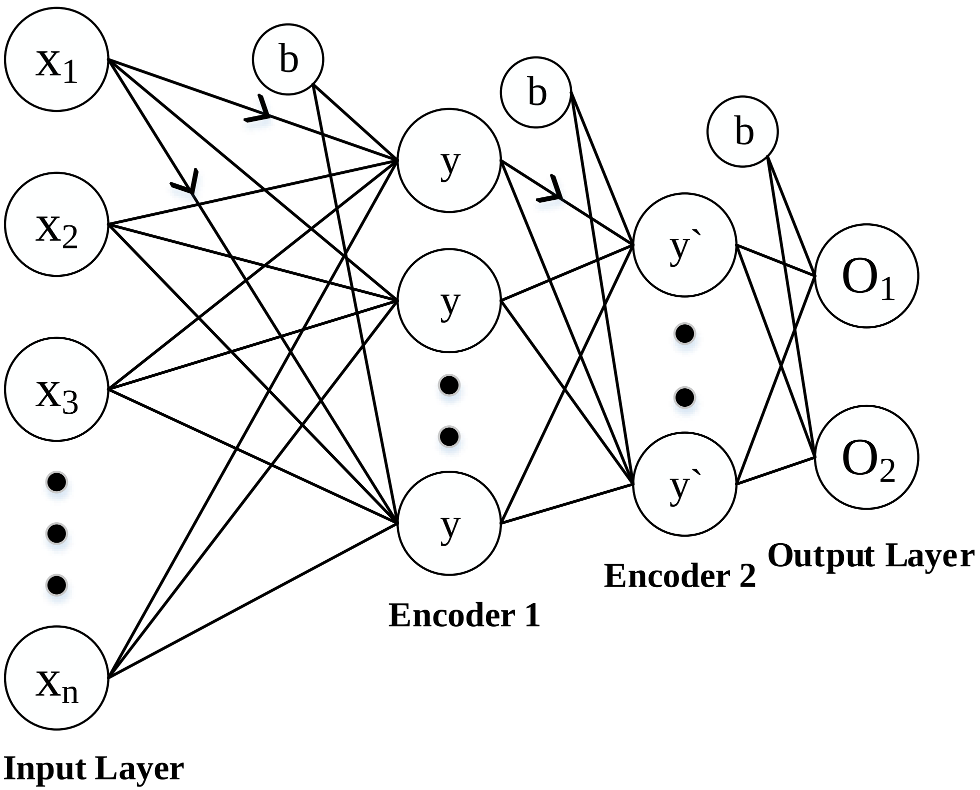


- SAE (Stacked Auto-Encoder)





- SAE (Stacked Auto-Encoder)



1. A. Javaid, Q. Niyaz, W. Sun, and M. Alam, "A deep learning approach for network intrusion detection system," in Proceedings of the 9th EAI International Conference on Bio-inspired Information and Communications Technologies (formerly BIONETICS). ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), 2016, pp. 21–26.
2. Y. Yu, J. Long, and Z. Cai, "Session-based network intrusion detection using a deep learning architecture," in Modeling Decisions for Artificial Intelligence. Springer, 2017, pp. 144–155.
3. M. E. Aminanto, R. Choi, H. C. Tanuwidjaja, P. D. Yoo, and K. Kim, "Deep abstraction and weighted feature selection for Wi-Fi impersonation detection," IEEE Transactions on Information Forensics and Security, vol. 13, no. 3, pp. 621–636, 2018.
4. M. E. Aminanto and K. Kim, "Detecting impersonation attack in Wi-Fi networks using deep learning approach," Information Security Applications: 17th International Workshop, WISA 2016, 2016.
5. M. E. Aminanto and K. Kim, "Improving detection of Wi-Fi impersonation by fully unsupervised deep learning," Information Security Applications: 18th International Workshop, WISA 2017, 2017.

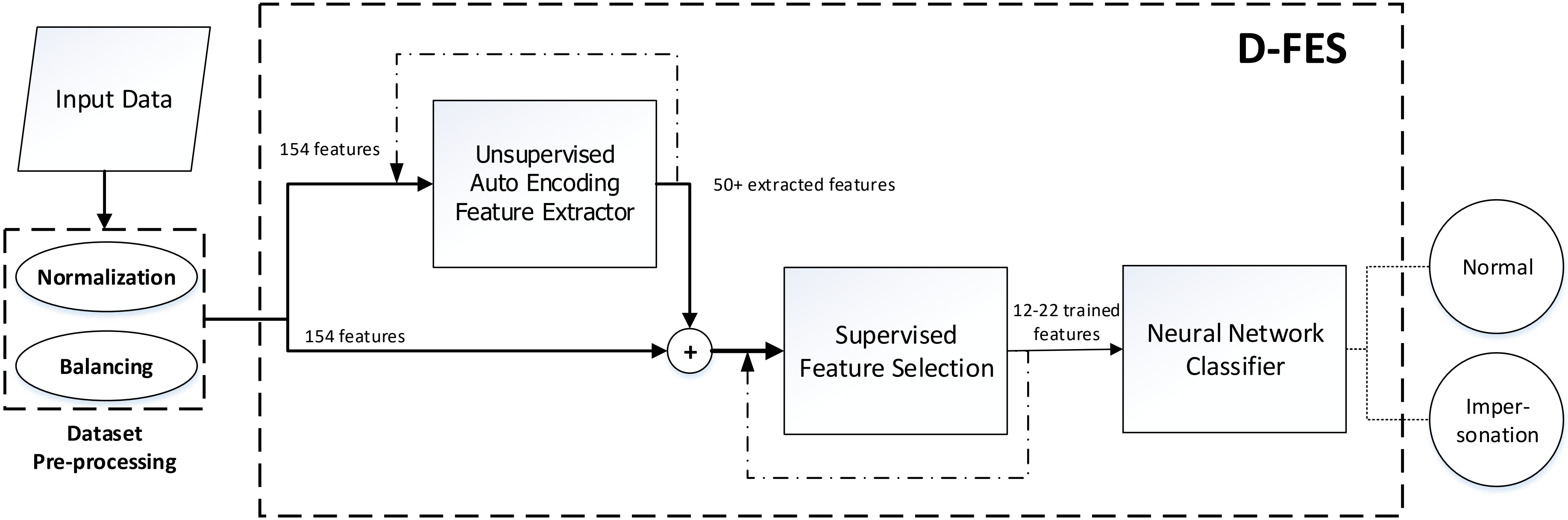
Our SAE Applications

- SAE as a classifier [1]
- Combination of feature extraction and selection [2]
- SAE as a clustering method [3]

1. M. E. Aminanto and K. Kim, “Detecting impersonation attack in Wi-Fi networks using deep learning approach,” Information Security Applications: 17th International Workshop, WISA 2016, 2016.
2. M. E. Aminanto, R. Choi, H. C. Tanuwidjaja, P. D. Yoo, and K. Kim, “Deep abstraction and weighted feature selection for Wi-Fi impersonation detection,” IEEE Transactions on Information Forensics and Security, vol. 13, no. 3, pp. 621–636, 2018.
3. M. E. Aminanto and K. Kim, “Improving detection of Wi-Fi impersonation by fully unsupervised deep learning,” Information Security Applications: 18th International Workshop, WISA 2017, 2017.

Deep-Feature Extraction and Selection

M. E. Aminanto, R. Choi, H. C. Tanuwidjaja, P. D. Yoo, and K. Kim, “Deep abstraction and weighted feature selection for Wi-Fi impersonation detection,” IEEE Transactions on Information Forensics and Security, vol. 13, no. 3, pp. 621–636, 2018.



Comparison

1. SAE as a classifier (WISA16)
2. Combination of feature extraction and selection (IEEE IF&S18)
3. SAE as clustering method (WISA17)

Method	DR (%)	FAR (%)
1	65.178	0.143
2	99.918	0.012
3	92.180	4.400
Kolias *et al.**	22.008	0.021

AWID Dataset

	Normal	Impersonation	Flooding	Injection
	Balanced			
Train	163,319	48,522	48,484	65,379
Test	53,078	20,079	8,097	16,682
	Unbalanced			
Train	1,633,190	48,522	48,484	65,379
Test	530,785	20,079	8,097	16,682

*) Kolias, Constantinos, *et al*., "Intrusion detection in 802.11 networks: empirical evaluation of threats and a public dataset," IEEE Communications Surveys & Tutorials, vol:18.1, pp: 184-208, 2015.

Summary

- ✓The principle of DL is to process hierarchical features of the provided input data, where the higher-level features are composed by lower-level features.

- ✓DL can discover sophisticated underlying structure and feature from abstract aspects.

- ✓The goal of DL is to learn and output feature representation which makes more suitable for feature engineering.

Future Challenges

- ✓Huge training load in the beginning,
- ✓How to apply DL in constrained-computation devices.
- ✓Incorporating DL models as a real-time classifier.
- ✓IDS detecting zero-day attacks with high detection rate and low false alarm rate.
- ✓Comprehensive measure not only detection but also prevention
- ✓*etc.*

KAIST School of Computing

KAIST Graduate School of Information Security

KAIST School of Computing

KAIST Graduate School of Information Security

The End

Comparison

KDD Cup'99 Dataset

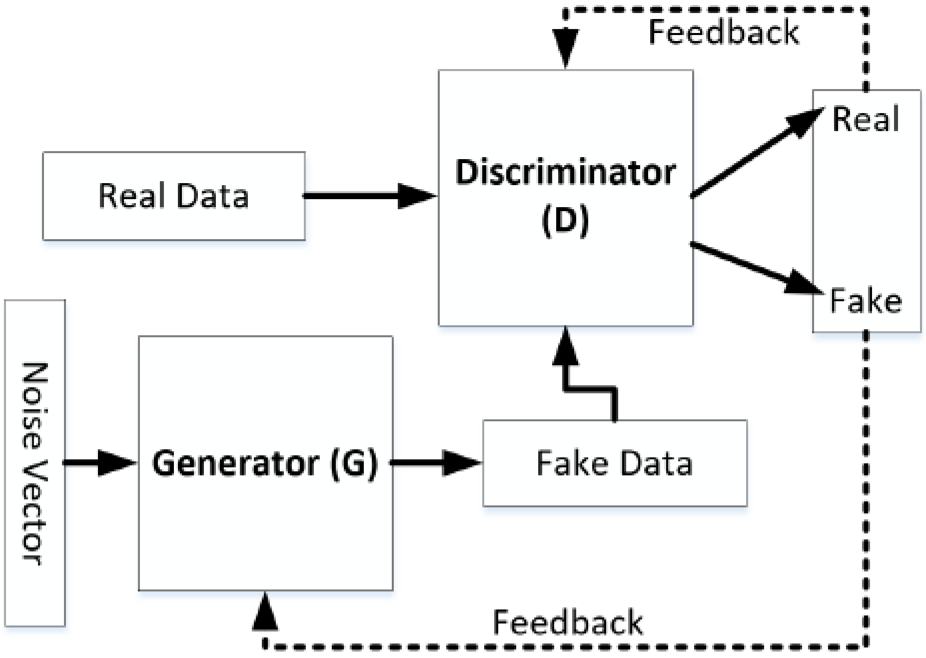
Method	Feature Extractor	Classifier	Accuracy (%)
DNN [1]	FF-NN	Softmax	99.994
LSTM-RNN-K [2]	LSTM-RNN	Softmax	96.930
LSTM-RNN-L [3]	LSTM-RNN	Softmax	98.110
LSTM-RNN-S [4]	LSTM-RNN	LSTM-RNN	93.820
GRU [5]	GRU	GRU	98.920

NSL KDD Dataset

Method	Feature Extractor	Classifier	Accuracy (%)
STL [6]	AE	Softmax	79.10
DNN-SDN [7]	NN	NN	75.75
RNN [8]	RNN	RNN	81.29
CNN [9]	CNN	CNN	79.14

1. S.S. Roy, A. Mallik, R. Gulati, M.S. Obaidat, and P. Krish-na, "A deep learning based artificial neural network approach for intrusion detection," in International Conference on Mathematics and Computing. Springer, 2017, pp. 44–53.
2. J. Kim, J. Kim, H. L. T. Thu, and H. Kim, "Long short term memory recurrent neural network classifier for intrusion detection," in Platform Technology and Service (PlatCon), 2016 International Conference on. IEEE, 2016, pp. 1–5.
3. Y. LIU, S. LIU, and Y. WANG, "Route intrusion detection based on long short term memory recurrent neural network," DEStech Transactions on Computer Science and Engineering, no.cii, 2017.
4. R. C. Staudemeyer, "Applying long short-term memory recurrent neural networks to intrusion detection," South African Computer Journal, vol. 56, no. 1, pp. 136–154, 2015.
5. M. K. Putchala, "Deep learning approach for intrusion detection system (ids) in the internet of things (iot) network using gated recurrent neural networks (gru)," Ph.D. dissertation, Wright State University, 2017.
6. A. Javaid, Q. Niyaz, W. Sun, and M. Alam, "A deep learning approach for network intrusion detection system," in Proceedings of the 9th EAI International Conference on Bio-inspired Information and Communications Technologies (formerly BIONETICS). ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), 2016, pp. 21–26.
7. T. A. Tang, L. Mhamdi, D. McLernon, S. A. R. Zaidi, and M. Ghogho, "Deep learning approach for network intrusion detection in software defined networking," in Wireless Networks and Mobile Communications (WINCOM), 2016 International Conference on. IEEE, 2016, pp. 258–263.
8. C. Yin, Y. Zhu, J. Fei, and X. He, "A deep learning approach for intrusion detection using recurrent neural networks," IEEE Access, vol. 5, pp. 21 954–21 961, 2017.
9. Z. Li, Z. Qin, K. Huang, X. Yang, and S. Ye, "Intrusion detection using convolutional neural networks for representation learning," in International Conference on Neural Information Processing. Springer, 2017, pp. 858–866.

- GAN



1. A. Dimokranitou, "Adversarial autoencoders for anomalous event detection in images," Ph.D. dissertation, Purdue University, 2017.

KAIST