Carnegie Mellon University

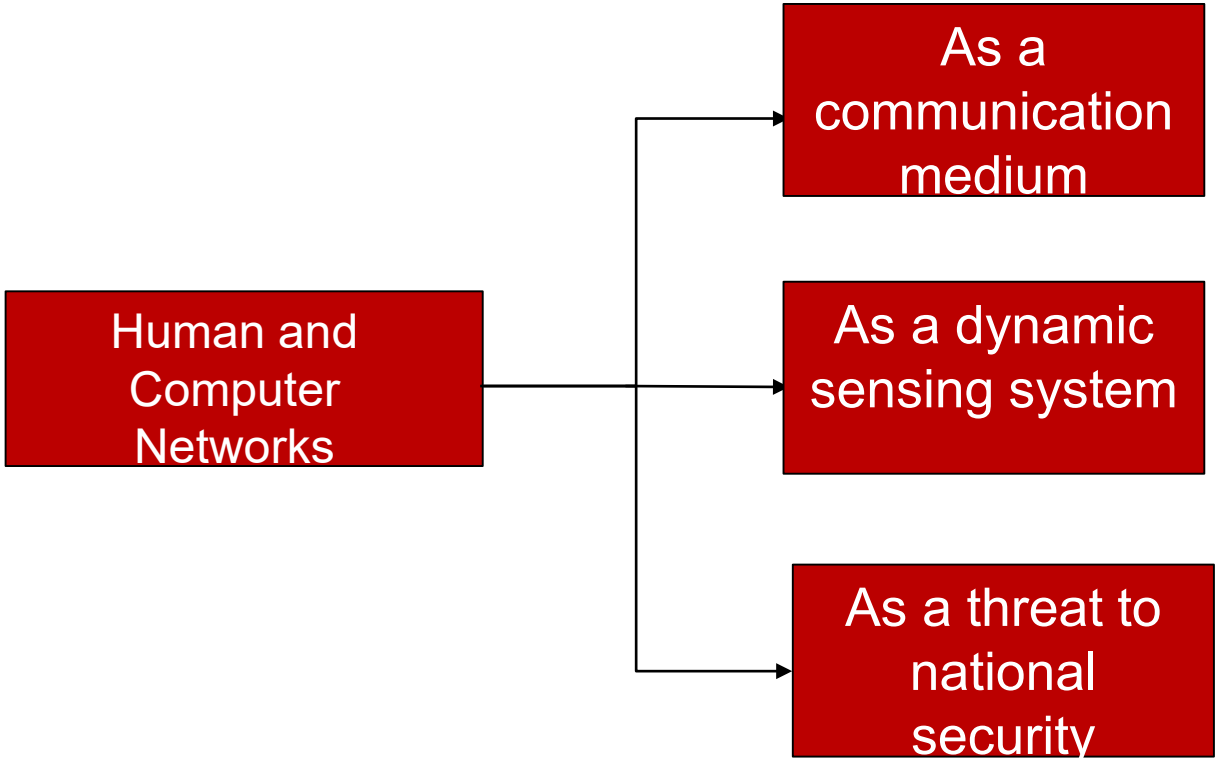
CyLab's Partners Conference

Deep Learning for Enhancing the Robustness of Intrusion Detection Systems

Conrad S. Tucker

Arthur Hamerschlag Career Development Professor,
Mechanical Engineering & Machine Learning (Courtesy)

Ascertaining the Veracity and Security of Data in the Information Age



Carnegie Mellon University

conradt@andrew.cmu.edu

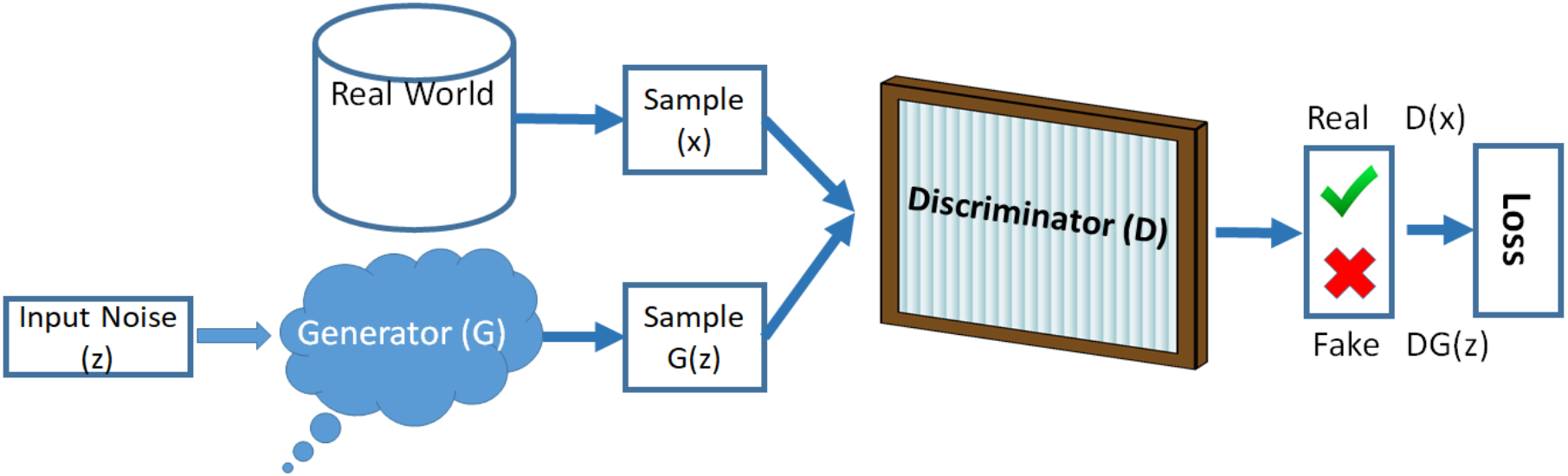
Human Perception and Classification

Carnegie Mellon University

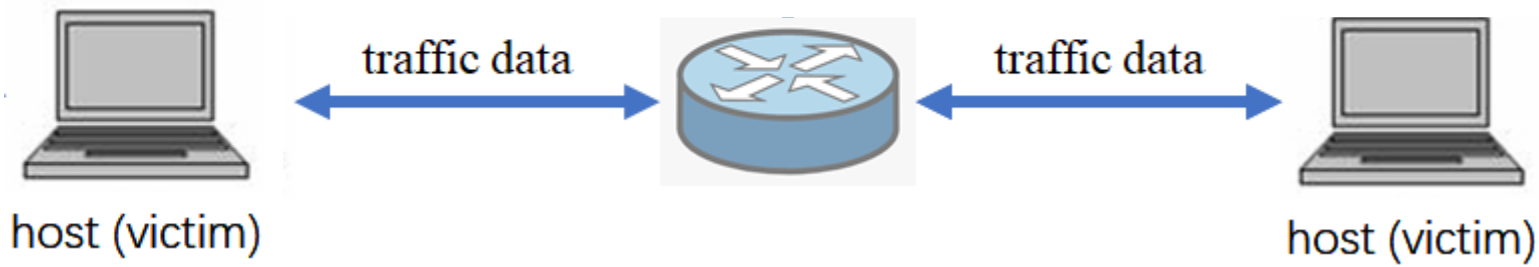
conradt@andrew.cmu.edu

Generative Adversarial Networks (GANs)

(Goodfellow, et al. 2014)

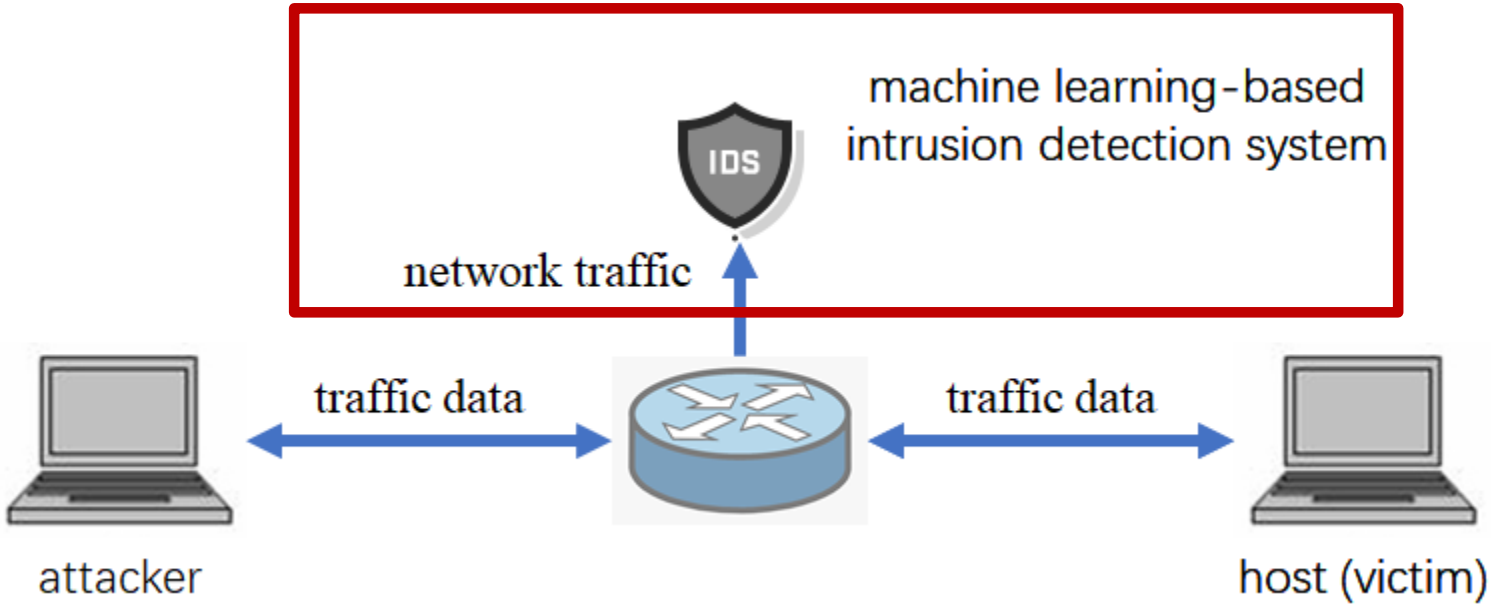


Computer Networks form the Backbone of Modern-Day Communication Systems



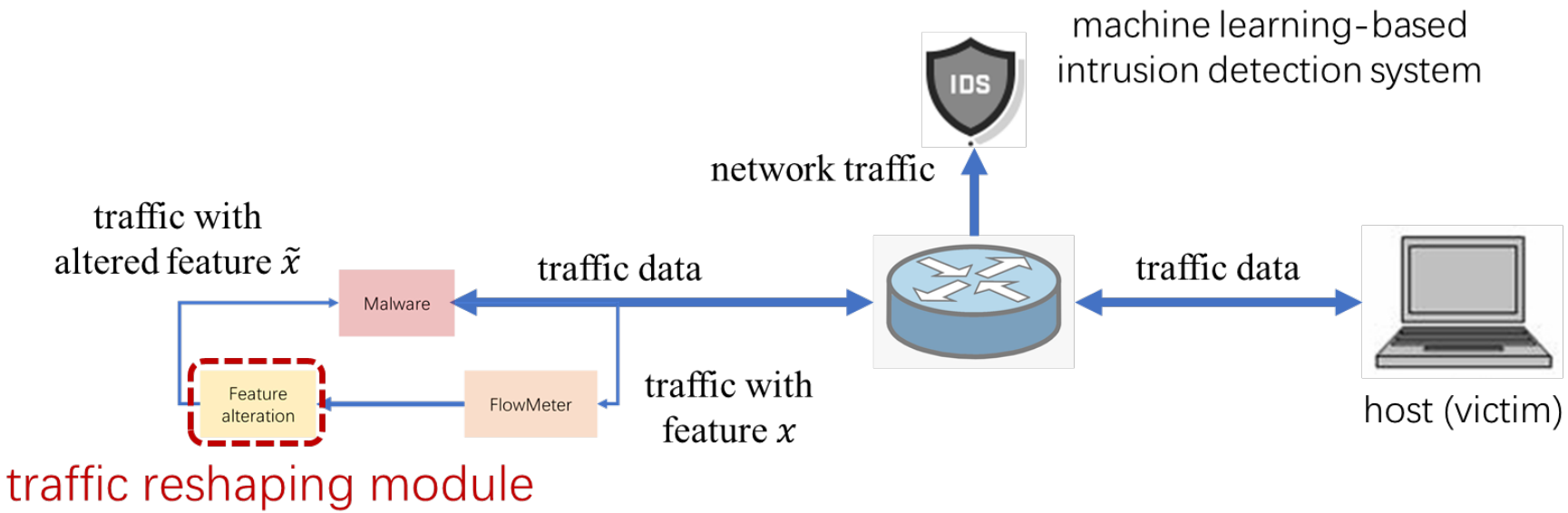
Shu, D., Cong, W., Chai, J., & **Tucker, C. S.** (2020, July). Encrypted rich-data steganography using generative adversarial networks. In Proceedings of the 2nd ACM Workshop on Wireless Security and Machine Learning (pp. 55-60)

Computer Networks are also Susceptible to AI-Based Attacks



Shu, D., Cong, W., Chai, J., & **Tucker, C. S.** (2020, July). Encrypted rich-data steganography using generative adversarial networks. In Proceedings of the 2nd ACM Workshop on Wireless Security and Machine Learning (pp. 55-60)

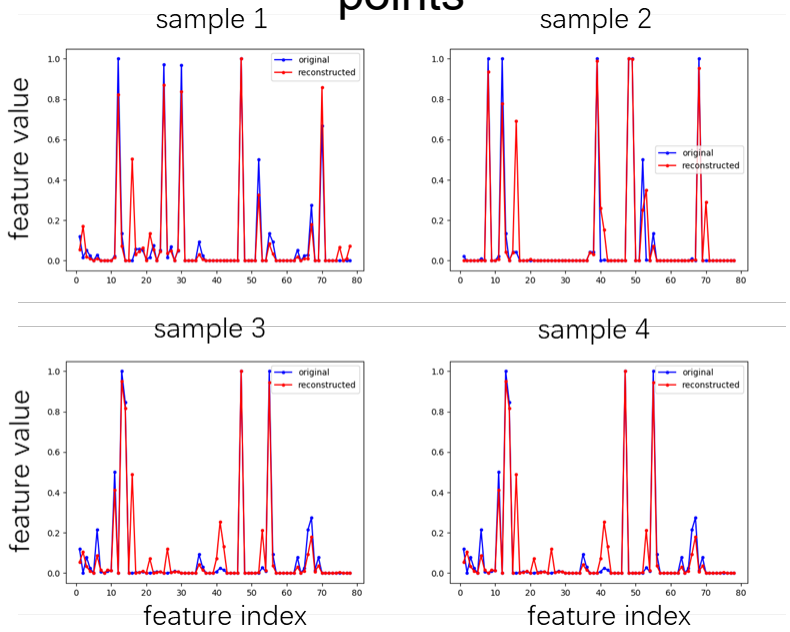
Computer Networks are also Susceptible to AI-Based Attacks



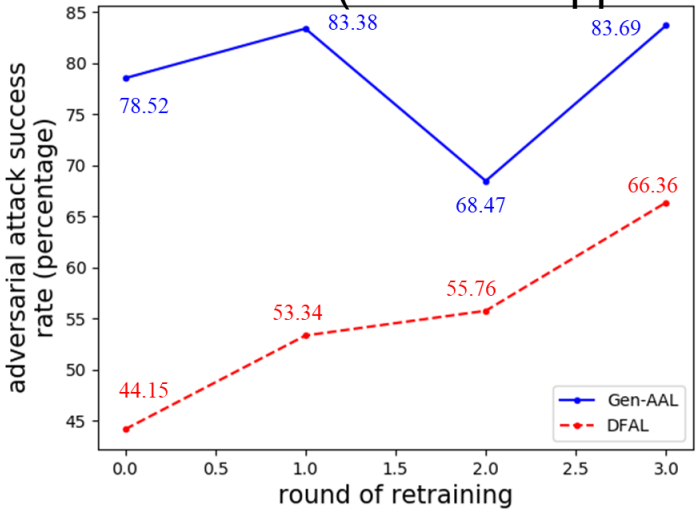
Shu, D., Cong, W., Chai, J., & **Tucker, C. S.** (2020, July). Encrypted rich-data steganography using generative adversarial networks. In Proceedings of the 2nd ACM Workshop on Wireless Security and Machine Learning (pp. 55-60)

Generative Adversarial Active Learning (Gen-AAL)

original and adversarial feature points



attack success rate of Gen-AAL and DFAL (baseline approach)



Shu, D., Cong, W., Chai, J., & **Tucker, C. S.** (2020, July). Encrypted rich-data steganography using generative adversarial networks. In Proceedings of the 2nd ACM Workshop on Wireless Security and Machine Learning (pp. 55-60)

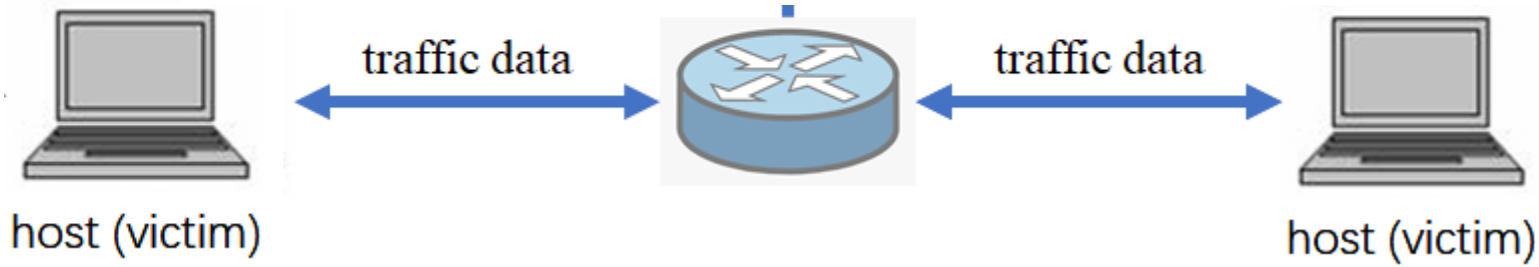
conradt@andrew.cmu.edu

Perturbed Features that Successfully Compromise IDS

Features with largest perturbations	
Feature name	
'Flow IAT Std'	Standard deviation time between two packets sent in the flow
'Flow IAT Min'	Minimum time between two packets sent in the forward direction
'Flow IAT Mean'	Mean time between two packets sent in the forward direction
'Fwd IAT Std'	Standard deviation time between two packets sent in the forward direction
'Flow Packets/s'	Number of flow packets per second
'Fwd Packet Length Max'	Maximum size of packet in forward direction
'Init_Win_bytes_backward'	The total number of bytes sent in initial window in the backward direction
'Destination Port'	Destination port
'min_seg_size_forward'	Minimum segment size observed in the forward direction
'Packet Length Variance'	Variance length of a packet

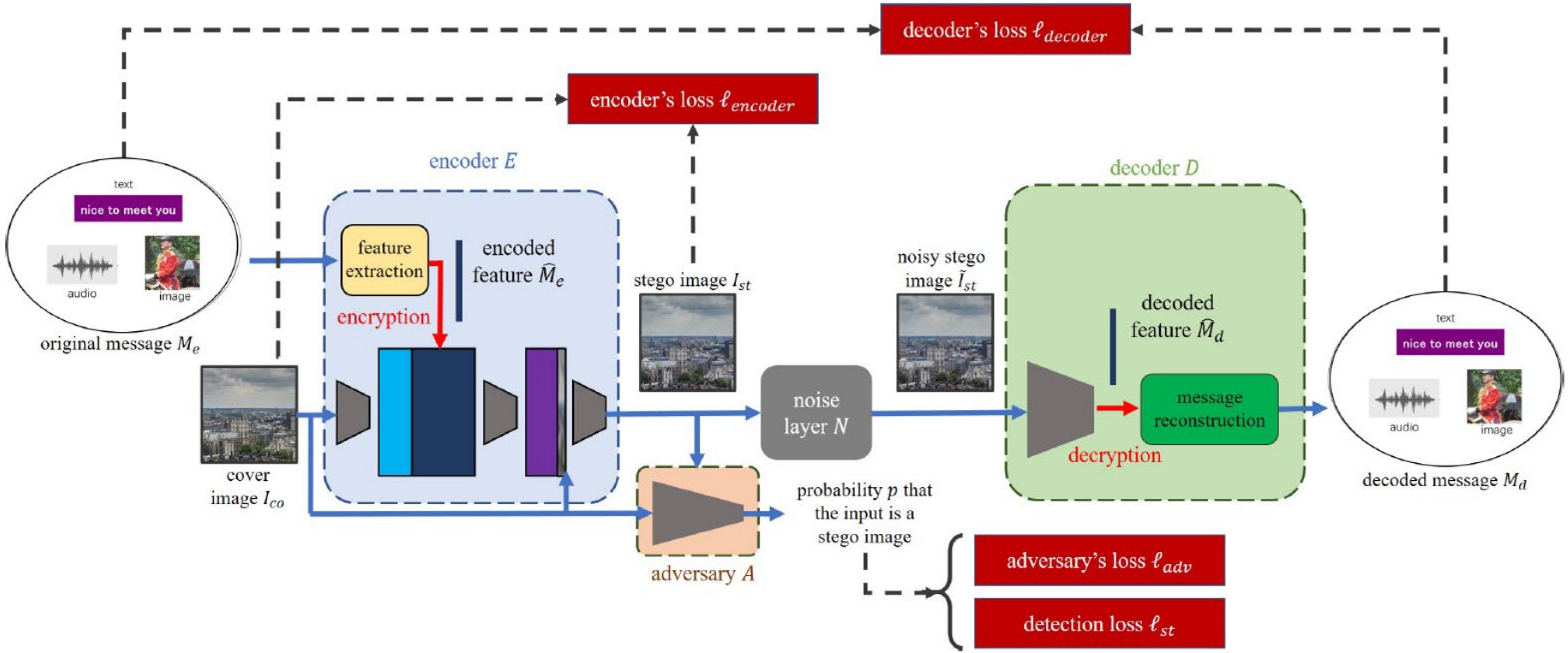
conradt@andrew.cmu.edu

Computer Networks form the Backbone of Modern-Day Communication Systems



Shu, D., Cong, W., Chai, J., & **Tucker, C. S.** (2020, July). Encrypted rich-data steganography using generative adversarial networks. In Proceedings of the 2nd ACM Workshop on Wireless Security and Machine Learning (pp. 55-60)

AI-Encoding of Messages within Network Communications

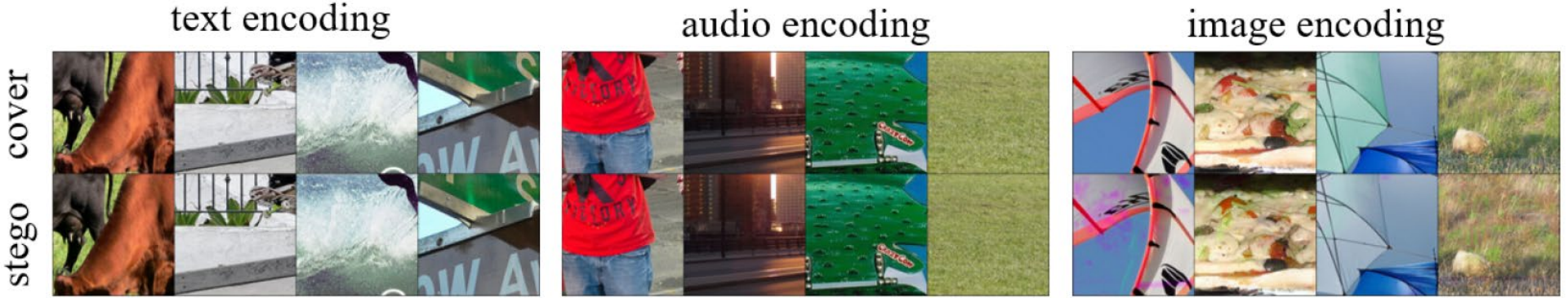


Shu, D., Cong, W., Chai, J., & **Tucker, C. S.** (2020, July). Encrypted rich-data steganography using generative adversarial networks. In Proceedings of the 2nd ACM Workshop on Wireless Security and Machine Learning (pp. 55-60).

conradt@andrew.cmu.edu

Results

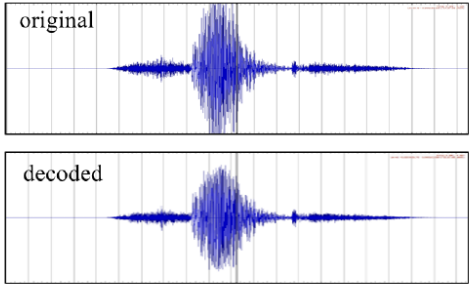
AI-Encoding of Messages within Network Communications



Shu, D., Cong, W., Chai, J., & **Tucker, C. S.** (2020, July). Encrypted rich-data steganography using generative adversarial networks. In Proceedings of the 2nd ACM Workshop on Wireless Security and Machine Learning (pp. 55-60).

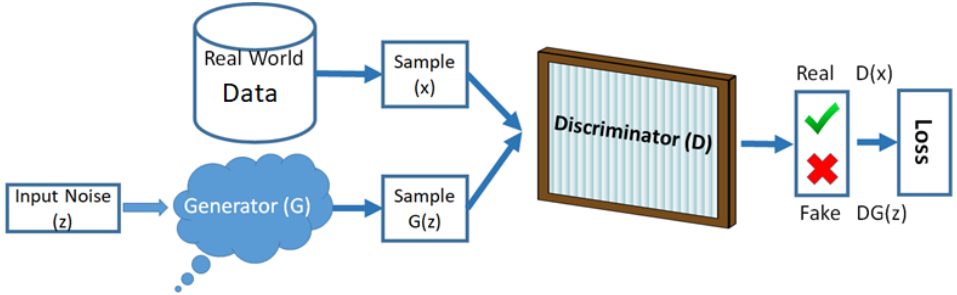
Results

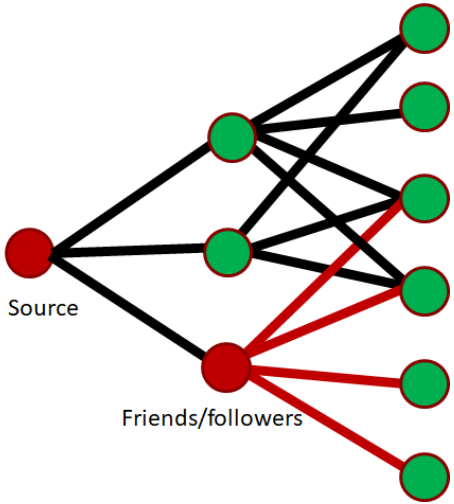
AI-Encoding of Messages within Network Communications

Message type	Decoding error	Example of messages
text	0.017	predict : <start> a beautiful woman sitting on a bench next to a body of water . <end> ground truth: <start> a beautiful woman sitting on a bench next to a body of water . <end> predict : <start> a black bird eating an apple on the ground in the woods . <end> woven ground truth: <start> a black bird eating an apple on the ground in the woods . <end> <pad> predict : <start> a man with a bucket hat riding a hose on a beach . <end> woven ground truth: <start> a man with a bucket hat riding a hose on a beach . <end> <pad> predict : <start> a big bird with a huge coupons looks out of its cage <end> woven woven ground truth: <start> a big bird with a huge beak looks out of its cage <end> <pad> <pad> predict : <start> a dog with a leash on is sitting near a park bench <end> woven woven ground truth: <start> a dog with a leash on is sitting near a park bench <end> <pad> <pad>
audio	0.0003	
image	0.0057	

conradt@andrew.cmu.edu

Research Summary Path Forward





Human and Computer Networks

- As a communication medium
- As a dynamic sensing system
- As a threat to national security

conradt@andrew.cmu.edu

Research Team and Collaborators

Frederica Free-Nelson
VISITING RESEARCHER

Research interests:
vehicular security, machine learning, and intrusion detection methods and techniques to promote cyber resilience and foster research on autonomous active cyber defense

Email:
frederica.f.nelson.civ@mail.mil

James Cunningham
DOCTORATE

Research interests:
Deep Learning/Reinforcement Learning

Email:
jamescun@andrew.cmu.edu

Sakthi Prakash
DOCTORATE

Research interests:
Machine Vision/Machine Learning

Email:
sarulpra@andrew.cmu.edu

Sweta Priyadarshi
DOCTORATE

Research interests:
Machine vision and deep learning

Email:
swetap@andrew.cmu.edu

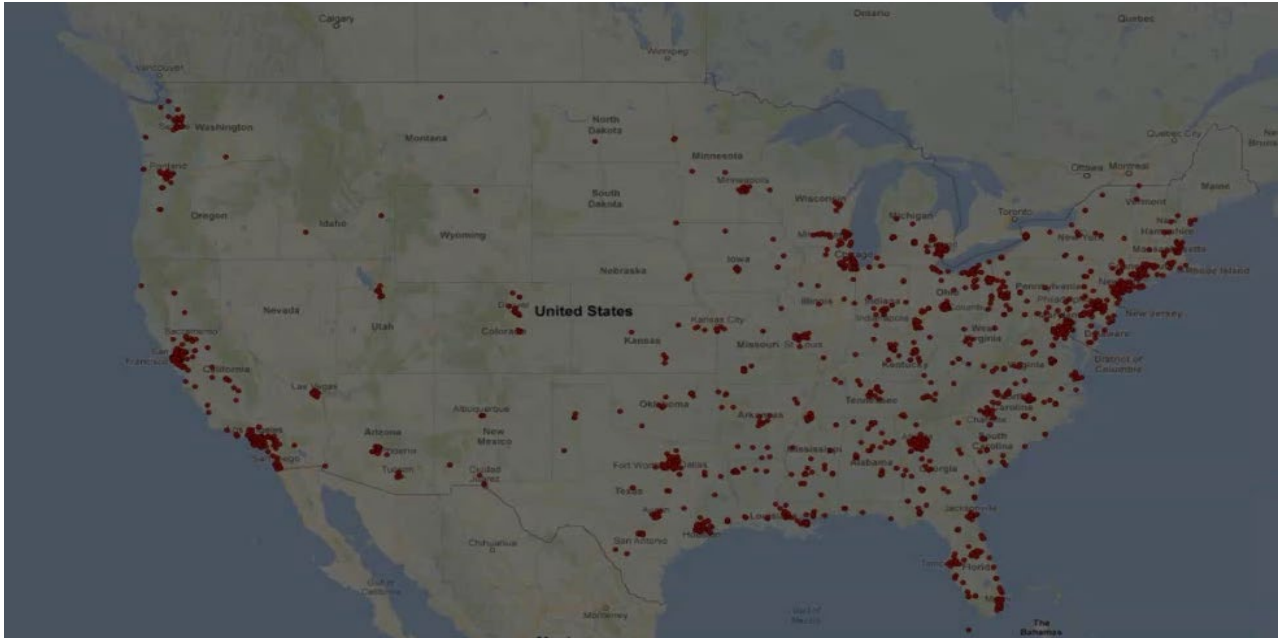
Dule Shu
DOCTORATE

Research interests:
Generative Design, Deep Learning

Email:
dules@andrew.cmu.edu

Questions?

Sponsors/Collaborators



Atlantic Council
BRENT SCOWCROFT CENTER
ON INTERNATIONAL SECURITY

Carnegie Mellon University

conradt@andrew.cmu.edu