Detection of Denial of Service Attacks Using Echo State Networks

Submission 583

IEEE SMC 2021
Melbourne, Australia
17-20 October, 2021

Kamila Bekshentayeva and Ljiljana Trajkovic
{kdagilov, ljilja}@sfu.ca
School of Engineering Science
Simon Fraser University
Vancouver, British Columbia, Canada

Roadmap

- Introduction
- Echo State Networks
- Datasets
- Performance and Results
- Conclusions

Roadmap

Introduction

- Overview of DoS and DDoS Attacks
- Overview of Machine Learning
- Contribution

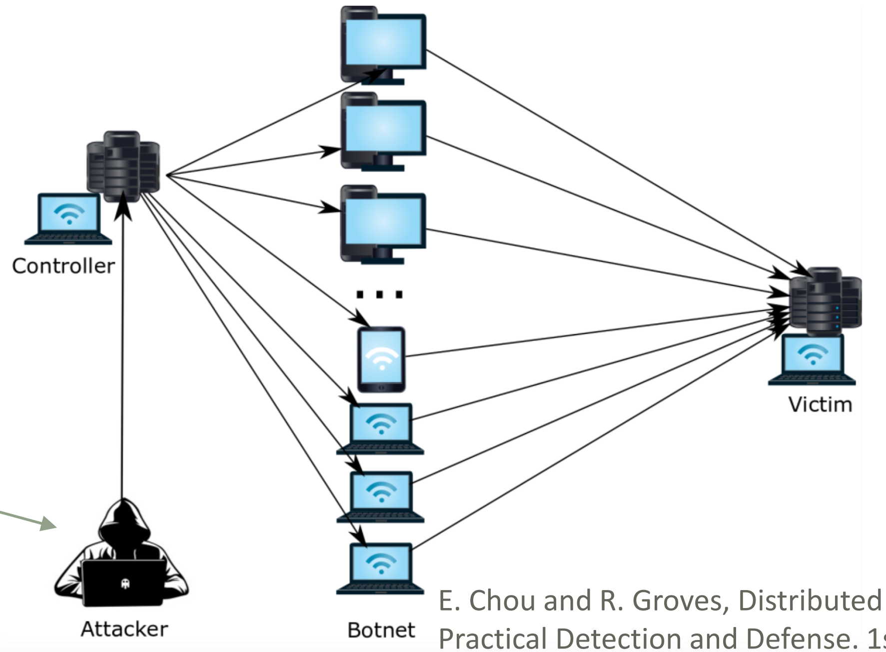
Denial of Service and Distributed Denial of Service (DoS and DDoS): Overview

- **Denial of Service (DoS)** attacks are attempts of an attacker to make services unavailable to legitimate users.
- **Distributed Denial of Service (DDoS)** attacks combine the resources of multiple compromised end systems in a coordinated way to exhaust resources of a target system.

Denial of Service and Distributed Denial of Service (DoS and DDoS): Overview

- **Denial of Service (DoS)** attacks are attempts of an attacker to make services unavailable to legitimate users.
- **Distributed Denial of Service (DDoS)** attacks combine the resources of multiple compromised end systems in a coordinated way to exhaust resources of a target system.

- **ATTACKER**: a cyber criminal, a hacktivist, or a user, who pursues financial gain, prestige, or follows his/her other personal goals.
- He/she **utilizes the best-effort Internet architecture**.



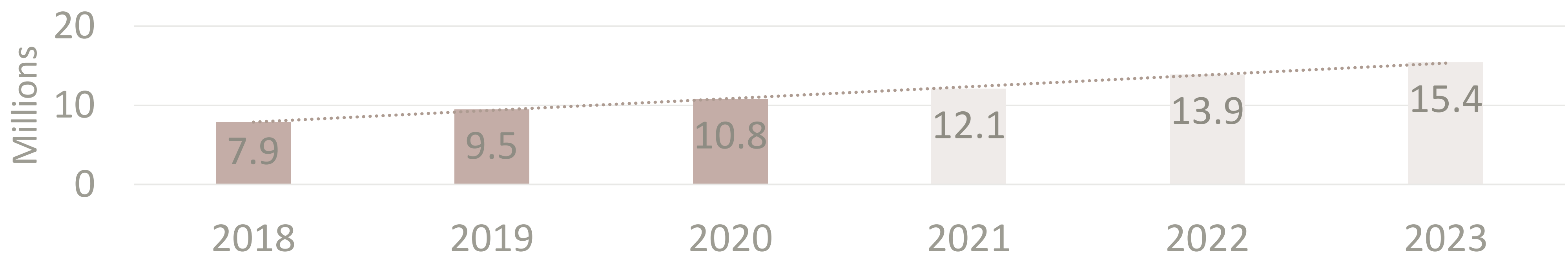
E. Chou and R. Groves, Distributed Denial of Service (DDoS): Practical Detection and Defense. 1st Ed. Sebastopol, CA: O’Reilly Media, 2018.

Motivation: DoS/DDoS are evolving and becoming harder to detect

DoS and DDoS attacks significantly affect the Internet performance

- Continuous growth of vulnerable and interconnected end systems increases occurrences of successful DDoS attacks.
- Defence mechanisms against DoS and DDoS attacks have received considerable attention in the area of cybersecurity.
- Two general intrusion detection approaches: Anomaly-based and signature-based.

Cisco's analysis of DDoS total attacks: history and predictions.



Cisco Annual Internet Report (2018–2023) White Paper. [Online]. Available: https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html.

Machine Learning

Involves the design of learning algorithms that optimize their performance as more data are observed to solve a specific task

Various **network anomaly detection systems** employ **machine learning algorithms**: convolutional neural networks, recurrent neural networks (RNNs), deep belief networks, and autoencoders.

@ SFU Communication Networks Lab:
Support Vector Machines (SVM), Recurrent Neural Networks (LSTM, GRU), Broad Learning System (BLS), deep learning networks, boosting algorithms and decision trees → intrusion detection in network traffic.

C. M. Bishop, Pattern Recognition and Machine Learning. Secaucus, NJ, USA: Springer-Verlag, 2006.

Research Contributions

- Echo state networks (ESNs) are used as a **feasible** reservoir computing approach to **identify intrusions in the network. We show they are/they have:**
  - **Not resource intensive** and **simple** to implement (may be used on devices with limited computational/memory resources)
  - Comparable performance with **short training time**
- Investigating how configuration of **reservoir hyperparameters** influences the performance of ESN models.
- Models are compared based on **accuracy, F-Score, false alarm rate**, and **training time** to bidirectional long short-term memory (**bi-LSTM**).
- **Employed datasets: CIC-IDS2017, CSE-CIC-IDS2018, CICDDoS2019,** and **Border Gateway Protocol** (Slammer, Nimda, Code Red I worms and recent large DDoS events).

Roadmap

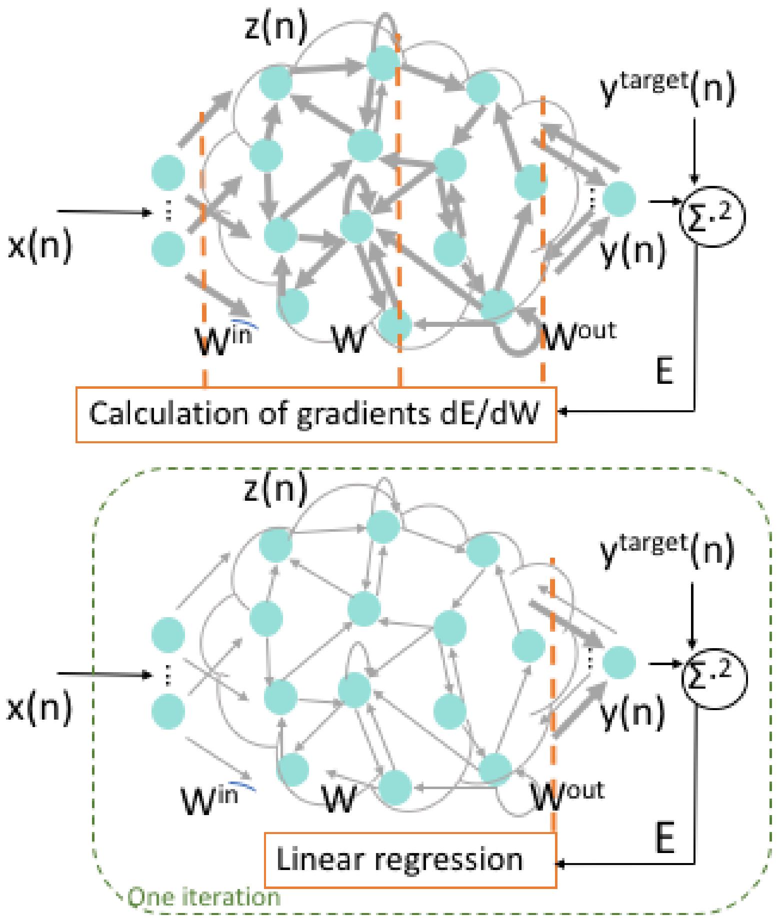
Introduction	Echo State Networks	Datasets	Performance and Results	Conclusions

Roadmap

Echo State Networks

- Reservoir Computing (RC) for training RNNs
- Echo State Networks (ESNs)
- ESN Reservoir Hyperparameters

Reservoir Computing (RC) as a Paradigm for Training Recurrent Neural Networks



- Reservoir is a randomly connected network of nodes excited by input x(n).
- Most common reservoirs are ESN and liquid state machine (LSM*): **training is performed to obtain only optimal output weights** leaving out the supervised adaptation of input and reservoir weights.

*LSM is sparse neural network where activation functions are replaced by threshold levels. Reservoir accumulates values from sequential samples, and emits output only when the threshold is reached, setting internal counter again to zero.

ESN Models

	Reservoir weights	$\rho(W)$	α	N_z
ESN1	Random	0.9	0.2	10
ESN2	**Deterministic**	0.9	0.2	10
ESN3	Random	**0.1**	0.2	10
ESN4	Random	0.9	**1**	10
ESN5	Random	0.9	0.2	**30**

- Deterministic reservoir - with each weight having the same value; known as recursive mechanism.
- $\rho(W)$ – reservoir radius
- α – leaking rate
- N_z – number of reservoir nodes

ESNs: Description (Steps)

Step 1: Generating random reservoir with parameters: $\boldsymbol{W}^{in} \in R^{Nx \times Nz}$, $\boldsymbol{W} \in R^{Nz \times Nz}$, $\alpha \in (0,1]$ – leaking rate

Step 2: Calculating reservoir activation states $\tilde{z}(n) \in R^{N_z}$ from the training set.

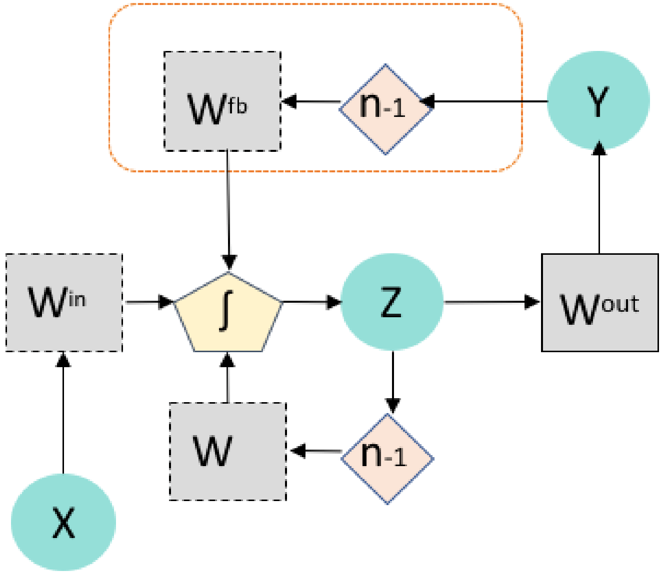
$$\tilde{z}(n) = tanh\left(x(n)\boldsymbol{W}^{in} + z(n-1)\boldsymbol{W}\right) \quad n = 1, \dots, N.$$
$$z(n) = (1-\alpha)z(n-1) + \alpha\tilde{z}(n) \quad n = 1, \dots, N.$$

$\tilde{z}(n) \in R^{N_z}$ vector of reservoir node activations at a timestep n

$z(n) \in R^{N_z}$ the reservoir state update at a timestep n.

N_z is a number of reservoir nodes

In cases where $\alpha = 1$ and $z(n) \equiv \tilde{z}(n)$.



ESN: Description (Steps)

Step 3: Using ridge regression to obtain the output weights.

The vectors $[z(n); x(n)]^T$ are collected into a matrix $Z \in R^{N \times (N_z+N_x)}$ Targets $y^{target}(n) \in R^1$ are collected into a matrix $Y \in R^{N \times 1}$. Z and Y have a row for every training time step n

$$\boldsymbol{W}^{out} = (\boldsymbol{Z}^T \boldsymbol{Z} + \beta \boldsymbol{I})^{-1} \boldsymbol{Z}^T \boldsymbol{Y}^{target}$$

To find the optimal weights – we minimize the loss function:

$$E(\mathbf{y}, \mathbf{y}^{\mathbf{target}}) = \frac{1}{N_y} \sum_{n=1}^{N_y} \sqrt{\frac{1}{N} \sum_{i=1}^{N} (y_i(n) - y_i^{target}(n))^2}.$$

Step 4: Evaluating the network by applying collected output weights with the new input x(n) to compute y(n)

$$y(n) = [z(n); x(n)]\boldsymbol{W}^{out} \quad n = 1, \dots, N.$$

$\boldsymbol{W}^{out} \in R^{(N_z+N_x) \times 1}$ *learned output weight matrix*

Roadmap

Introduction	Echo State Networks	Datasets	Performance and Results	Conclusions

Roadmap

Datasets

- CIC-IDS2017, CSE-CIC-IDS2018, and CIC-DDoS2019 Datasets
- Border Gateway Protocol Datasets
- Feature Selection

CIC-IDS2017, CSE-CIC-IDS2018, and CIC-DDoS2019 Datasets

Datasets

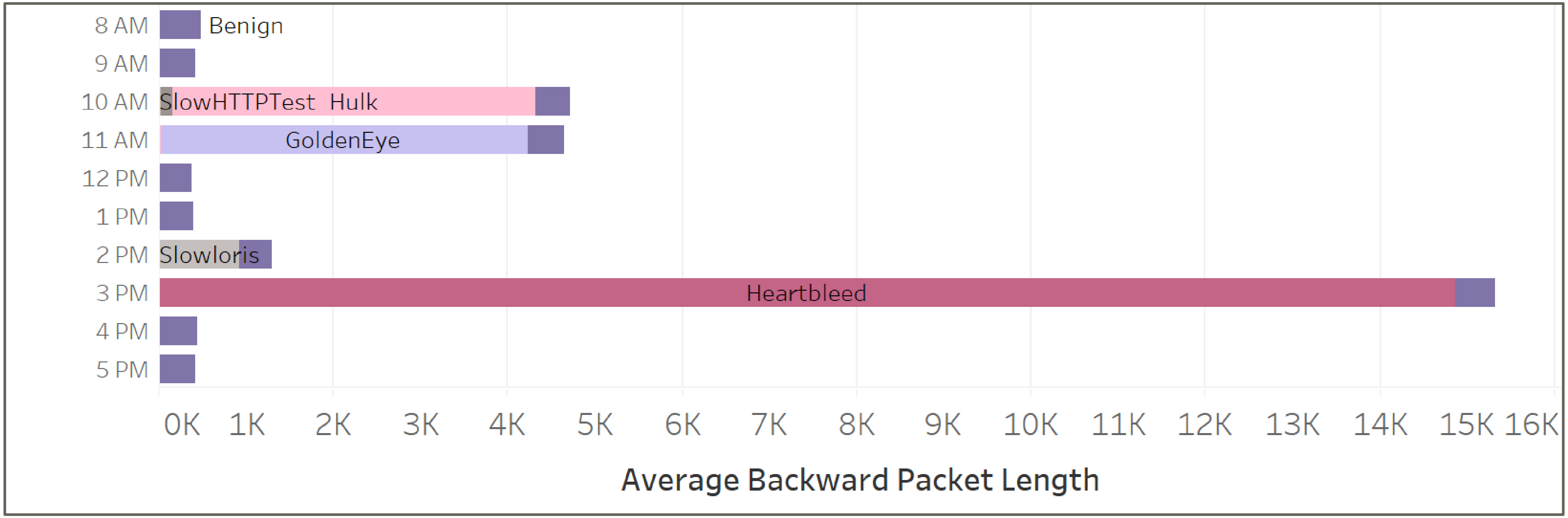
- **Public**
- **Labeled**
- **Diverse traffic and features**

- Canadian Institute for Cybersecurity (CIC) → **CIC-IDS2017**, **CSE-CIC-IDS2018** (colab. Communications Security Establishment (CSE)), and **CIC-DDoS2019** datasets with current network traffic trends
- **B-Profile:** background regular behavior of 25 users
  - Protocols: HTTP, HTTPS, FTP, SSH, SMTP, POP3, and IMAP*
- **M-Profile:** infiltration, DoS, web application, and brute force attacks

*HTTP – Hypertext Transfer Protocol; FTP – File Transfer Protocol; SSH – Secure Shell; SMTP – Simple Mail Transfer Protocol; POP3 – Post Office Protocol; IMAP – Internet Mail Access Protocol

Intrusion Detection Evaluation datasets. [Online]. Available: https://www.unb.ca/cic/datasets.html.

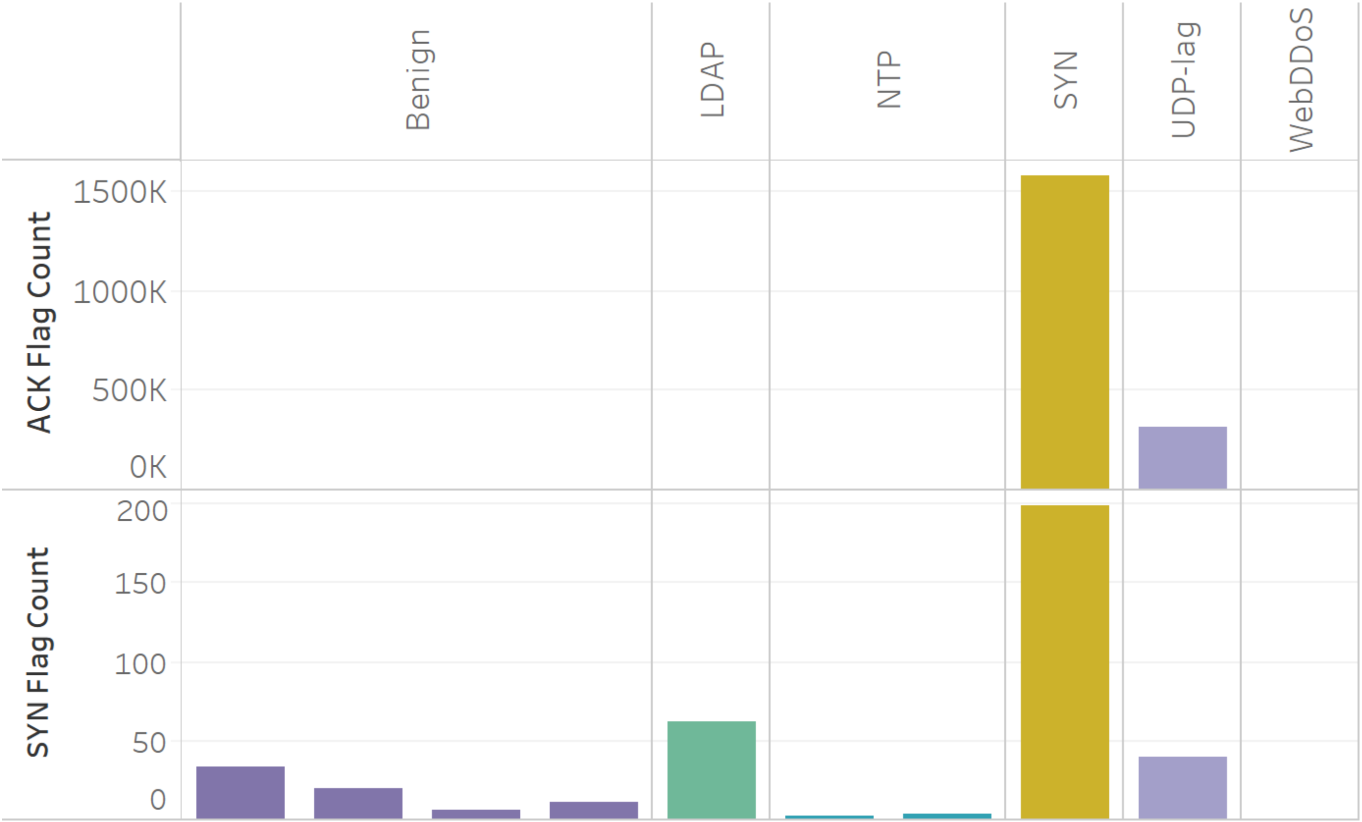
Features



Packet length (CIC-IDS2017):

- Regular packets are generally under 1,000 bytes
- Heartbleed attack packets approximately reach 15,000 bytes on average.

Features



TCP Flags (CICDDoS2019):

- SYN attacker brings down a network connection by requesting for seemingly legitimate connections through a series of TCP requests with TCP SYN, ACK flags set to 1

Border Gateway Protocol Datasets

BGP

- Routing protocol
- Allows Autonomous Systems (ASes) exchange reachability information
- Incremental

BGP collectors

- RIPE (rrc04, Geneva; rrc14, Palo Alto)
- Routeviews (routeviews4, Eugene Oregon)

RIPE NCC: RIPE Network Coordination Center. [Online]. Available: http://www.ripe.net/data-tools/stats/ris/ris-raw-data.

University of Oregon Route Views project. [Online]. Available: http://www.routeviews.org.

Border Gateway Protocol Datasets

Types of messages
- open
- update
- keep alive
- notification

Zebra-dump parser
- MRT - ASCII

C# tool
- 37 features

Feature	Name	Category
1	Number of announcements	*volume*
2	Number of withdrawals	*volume*
3	Number of announced NLRI prefixes	*volume*
4	Number of withdrawn NLRI prefixes	*volume*
5	Average *AS-path* length	*AS-path*
6	Maximum *AS-path* length	*AS-path*
7	Average unique *AS-path* length	*AS-path*
8	Number of duplicate announcements	*volume*
9	Number of implicit withdrawals	*volume*
10	Number of duplicate withdrawals	*volume*
11	Maximum edit distance	*AS-path*
12	Arrival rate	*AS-path*
13	Average edit distance	*volume*
14 – 23	Maximum *AS-path* length, where $n = (11, ..., 20)$	*AS-path*
24 – 33	Maximum edit distance $= n$, where $n = (7, ..., 16)$	*AS-path*
34	Number of Interior Gateway Protocol (IGP) packets	*volume*
35	Number of Exterior Gateway Protocol (EGP) packets	*volume*
36	Number of incomplete packets	*volume*
37	Packet size (B)	*volume*

Border Gateway Protocol Datasets

Event	Beginning	Duration (min)
Slammer	25.01.2003	869
Nimda	18.09.2001	1301
Code Red I	19.07.2001	600
DDoS 2019	22.10.2019	8 hours
DDoS 2020	17.02.2020	3 days

Border Gateway Protocol Datasets

Event	Beginning	Duration (min)
Slammer	**25.01.2003**	**869**
Nimda	**18.09.2001**	**1301**
Code Red I	**19.07.2001**	**600**
DDoS 2019	22.10.2019	8 hours
DDoS 2020	17.02.2020	3 days

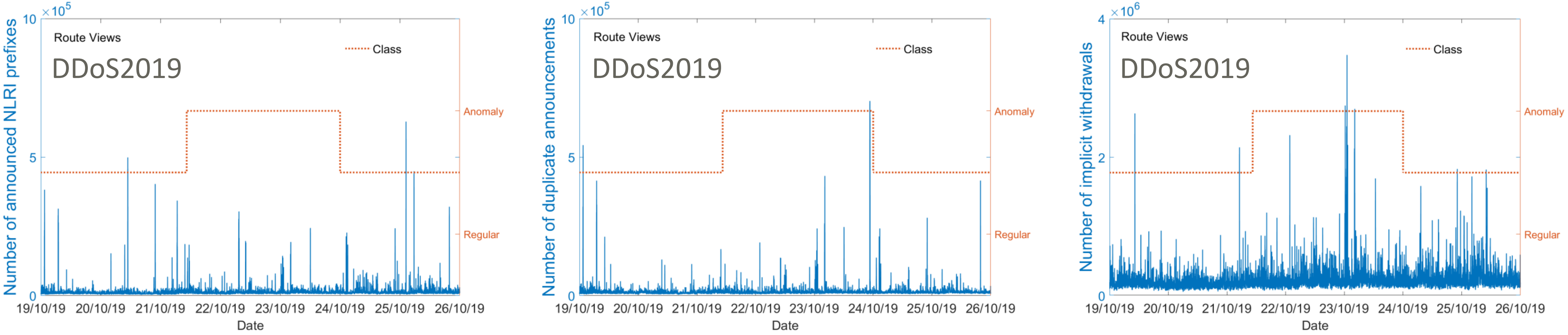
- BGP worms propagated via email messages
- DoS

Border Gateway Protocol Datasets

Event	Beginning	Duration (min)
Slammer	25.01.2003	869
Nimda	18.09.2001	1301
Code Red I	19.07.2001	600
DDoS2019	**22.10.2019**	**8 hours**
DDoS2020	**17.02.2020**	**3 days**

- **DDoS2019: October 2019 DDoS Attack on AWS:** affected the Amazon route 53 DNS webservice leaving thousands of customers not being able to access cloud services, websites, and applications.
- **DDoS2020: February 2020 DDoS Attack on AWS:** largest ever DDoS attack of 2.3 Tbps, CLDAP reflection attack.

Route Views: October 2019 DDoS Attack on AWS



Number of announced NLRI* prefixes (left), number of duplicate announcements (center), and number of implicit withdrawals (right)

- Duplicate announcements are the BGP update packets that have identical NLRI prefixes and the AS-path attributes.
- Implicit withdrawals are prefixes implicitly withdrawn by sending the same prefix with new attributes.

We indicated the 23rd of October, 2019 as a day with network anomalies due to ransom driven DDoS attacks that hit the banking industry in South Africa

*NLRI – Network Layer Reachability Information

Feature Selection

Selecting best features

- Enhances performance
- Reduces training time

Extra trees

- Extremely Randomized Trees
- Tree-based ensemble method generates decision trees from a training set.
- **Parameters**: number of attributes (features) (**K = 20),** minimum sample size (**nmin = 2),** number of decision trees in the ensemble (**M = 100)**, determines the strength of the variance reduction of the ensemble model aggregation.

Ensemble learning

- Overcomes the overfitting by combining the predictions of many varied models into a single prediction

Roadmap

Introduction	Echo State Networks	Datasets	Performance and Results	Conclusions

Roadmap

Performance and Results

- Performance of ESN Models
- Comparing Performance of ESN and Bi-LSTM in Detecting the Denial of Service Attacks

Bi-LSTM model

PyTorch

Open-source Python-based scientific computing package developed by Facebook’s AI Research lab; tensors

Torch.nn

provides building blocks for building neural network architectures of any complexity.

Bidirectional LSTM layer: input nodes = number of features and 16 output nodes, dropout rate = 0.5, batch size = 10, and ReLU activation function

Fully-connected layer with 32 input and 2 output nodes passed to the F.softmax module

nn.CrossEntropyLoss() ; torch.optim.Adam(); learning rate 0.001 , 10 epochs

Performance Results

	CIC-IDS2017			CSE-CICIDS2018			CIC-DDoS2019		
	Acc.	F-Score	FAR	Acc.	F-Score	FAR	Acc.	F-Score	FAR
ESN1	0.927	0.907	0.106	0.983	0.854	0.017	0.994	0.994	0.012
ESN2	0.958	0.945	0.058	0.980	0.828	0.020	0.991	0.992	0.016
ESN3	0.915	0.893	0.120	0.961	0.679	0.032	0.927	0.932	0.146
ESN4	0.919	0.899	0.120	0.979	0.824	0.021	0.981	0.999	0.000
ESN5	0.962	0.950	0.053	0.997	0.973	0.003	0.999	0.999	0.001
Bi-LSTM	0.995	0.994	0.002	0.996	0.962	0.004	1.000	1.000	0.000
Training Time (s)									
ESN5	988			2,335			1,690		
Bi-LSTM	2,200			3,417			2,619		

Performance of ESN and Bi-LSTM models based on accuracy, F-Score, and false alarm rate when evaluated using **CIC-IDS2017, CIC-CSE-IDS2018, and CIC-DDoS2019**

Performance Results

	Slammer			Nimda			Code Red I		
	Acc.	F-Score	FAR	Acc.	F-Score	FAR	Acc.	F-Score	FAR
ESN1	0.907	0.699	0.080	0.805	0.502	0.166	0.910	0.432	0.040
ESN2	0.908	0.710	0.083	0.821	0.470	0.130	0.919	0.424	0.027
ESN3	0.930	0.726	0.036	0.843	0.167	0.024	0.913	0.046	0.002
ESN4	0.927	0.712	0.036	0.841	0.122	0.021	0.901	0.536	0.075
ESN5	0.962	0.950	0.053	0.818	0.516	0.150	0.910	0.547	0.062
Bi-LSTM	0.958	0.827	0.024	0.863	0.375	0.029	0.929	0.491	0.021
Training Time (s)									
ESN5	8			7			6		
Bi-LSTM	34			41			37		

Performance of ESN and Bi-LSTM models based on accuracy, F-Score, and false alarm rate when evaluated using **BGP datasets**: **Slammer, Nimda, Code Red I**

Performance Results

	DDoS2019 (RIPE)			DDoS2019 (RV)			DDoS2020 (RIPE)			DDoS2020 (RV)		
	Acc.	F-Score	FAR	Acc.	F-Score	FAR	Acc.	F-Score	FAR	Acc.	F-Score	FAR
ESN1	0.571	0.502	0.465	0.613	0.433	0.259	0.439	0.610	0.988	0.477	0.609	0.877
ESN2	0.579	0.558	0.527	0.611	0.551	0.406	0.437	0.606	0.994	0.577	0.610	0.565
ESN3	0.481	0.522	0.702	0.615	0.261	0.130	0.437	0.607	0.998	0.437	0.603	0.982
ESN4	0.525	0.505	1.000	0.624	0.193	0.084	0.436	0.607	1.000	0.441	0.604	0.971
ESN5	0.677	0.617	0.371	0.618	0.540	0.373	0.453	0.610	0.955	0.595	0.621	0.536
Bi-LSTM	0.388	0.478	0.837	0.654	0.791	1.000	0.346	0.514	1.000	0.760	0.864	1.000
Training Time (s)												
ESN5	12			6			9			11		
Bi-LSTM	111			99			107			101		

Performance of ESN and Bi-LSTM models based on accuracy, F-Score, and false alarm rate when evaluated using **BGP** datasets collected from **RIPE** and **Route Views**: **DDoS2019 and DDoS2020**

Roadmap

Introduction	Datasets	Echo State Networks	Performance and Results	**Conclusions**

Roadmap

Conclusions

- Conclusion
- Key References

Conclusion

- We evaluated performance of **ESN** and **Bi-LSTM** models to detect various DoS and DDoS attacks by using **CIC-IDS synthetic datasets** as well as **RIPE and Route Views BGP datasets** collected from deployed networks
- A number of ESN models was designed by varying **hyperparameters** of the reservoir network: Increasing the number of reservoir nodes and the radius of the reservoir enhanced the model performance.
- The ESN and Bi-LSTM models evaluated in this paper demonstrated **comparable** accuracy, F-Score, and FAR **while ESN models required shorter training time**.
- Even though performance of the classifiers was influenced by the employed datasets, experimental results illustrated that **ESNs may be used to successfully detect network anomalies**.

Key References

DoS and DDoS Detection:

- E. Chou and R. Groves, Distributed Denial of Service (DDoS): Practical Detection and Defense. 1st Ed. Sebastopol, CA: O'Reilly Media, 2018.
- V. Chandola, A. Banerjee, and V. Kumar, "Anomaly detection: a survey," ACM Comput. Surv., vol. 41, no. 3, pp. 15:1–15:58, July 2009.
- J. Mirkovic and P. Reiher, "A taxonomy of DDoS attack and DDoS defense mechanisms," ACM SIGCOMM Comput. Commun. Rev., 34, 2004, pp. 39–53.

Key References

Machine Learning:

- C. M. Bishop, Pattern Recognition and Machine Learning. Secaucus, NJ, USA: Springer-Verlag, 2006.
- I. Goodfellow, Y. Bengio, and A. Courville, Deep Learning. Cambridge, MA, USA: The MIT Press, 2016.
- M. Lamons, R. Kumar, and A. Nagaraja, Python Deep Learning Projects, Packt Publishing, 2018. [E-book] Available: O’Reilly Online Learning (formerly Safari Books Online).
- K. Greff, R. K. Srivastava, J. Koutnik, B. R. Steunebrink, and J. Schmidhuber, “LSTM: a search space odyssey,” IEEE Trans. Neural Netw. Learn. Syst., vol. 28, no. 10, pp. 2222–2232, Oct. 2017.
- Z. Li, Q. Ding, S. Haeri, and Lj. Trajković, “Application of machine learning techniques to detecting anomalies in communication networks: classification algorithms,” in Cyber Threat Intelligence, M. Conti, A. Dehghantanha, and T. Dargahi, Eds., Berlin: Springer, 2018, pp. 71–92.

Key References

Datasets:

- Intrusion Detection Evaluation dataset (CIC-IDS2017). [Online]. Available: https://www.unb.ca/cic/datasets/ids-2017.html. Accessed: May 28, 2021.
- A Realistic Cyber Defense dataset (CSE-CIC-IDS2018). [Online]. Available: https://registry.opendata.aws/cse-cic-ids2018/. Accessed: May 28, 2021.
- DDoS Evaluation Dataset (CICDDoS2019). [Online]. Available: https://www.unb.ca/cic/datasets/ddos-2019.html. Accessed: May 28, 2021.
- RIPE NCC: RIPE Network Coordination Center. [Online]. Available: http://www.ripe.net/data-tools/stats/ris/ris-raw-data [May 2021].
- University of Oregon Route Views project. [Online]. Available: http://www.routeviews.org [May 2021].

Key References

Echo State Networks:

- H. Jaeger, "The "echo state" approach to analysing and training recurrent neural networks-with an erratum note," German Nat. Res. Center for Inf. Technol. GMD, Bonn, Germany, Tech. Rep. 148, 2001.
- M. Lukoševičius, H. Jaeger, and B. Schrauwen, "Reservoir Computing Trends", KI. Künstliche Intelligenz (Oldenbourg), vol. 26, no. 4, pp. 365–371, Nov. 2012.
- M. Lukosevicius, "A practical guide to applying Echo State Networks," in Neural Networks: Tricks of the Trade (2nd ed.), G. Montavon, G. B.'Orr, and K. -R. Müller, Eds., Berlin, Heidelberg, Springer, 2012, vol. 7700, pp. 659–686.

Key References

- K. Bekshentayeva, M. Canute, Y.-M. Kim, D. Lee, A. Wong, “Network Intrusion Detection Using Various Deep Learning Approaches”, BC Artificial Intelligence Showcase, Vancouver, BC, Dec. 2019.
- L. Gonzalez Rios, Z. Li, K. Bekshentayeva, and Lj. Trajkovic, "Detection of denial of service attacks in communication networks," in Proc. IEEE Int. Symp. Circuits and Systems, Seville, Spain, Oct. 2020 (virtual).
- L. Gonzalez Rios, K. Bekshentayeva, M. Singh, S. Haeri, and Lj. Trajkovic, "Virtual network embedding for switch-centric data center networks," in Proc. IEEE Int. Symp. Circuits and Systems, Daegu, Korea, May 2021 (virtual).
- K. Bekshentayeva and Lj. Trajkovic, “Detection of Denial of Service Attacks using Echo State Networks,” in Proc. IEEE International Conference on Systems, Man, and Cybernetics, Melbourne, Australia, submitted.

Thank you for your attention!

Questions:

kdagilov@sfu.ca
ljilja@sfu.ca