Survey Paper Search and Review

Amanul Islam

September 15, 2024

1 Exercises from TWWIST Videos

Chapter 5: Why Does Storytelling Matter in Tactical Writing?
Objective: Recognize how an audience processes information through stories.
Exercise: Write down a list of assumptions and interpretations your audience might make when presented with factual information. Consider how the audience may infer, fill in gaps, or reverse facts.
Learning Outcome: Understand how critical it is to structure stories to guide the audience to our intended interpretation, using characters, goals, and visual elements.
Chapter 6: How to Create Tactical Stories
Objective: Practice using the "Magnificent Seven" cognitive principles (e.g., experience, structure, meaning, gaps, characters, and conflict).
Exercise: Take an existing technical or academic paper you have written and apply each of the "Magnificent Seven" principles to enhance its storytelling quality.
Learning Outcome: Understand how to incorporate storytelling into technical writing by aligning it with cognitive principles that naturally engage readers.

2 Learning Process on the Survey Paper

I began by narrowing down my research focus to anomaly detection in three distinct but interconnected areas: anomaly detection in 5G/6G networks using Variational Autoencoders (VAEs), detection of fake base stations, and anonymous networking detection within cryptocurrency networks.
My initial search targeted papers that explore machine learning techniques, particularly VAE, in detecting anomalies in next-generation wireless networks. These networks are expected to handle vast amounts of data, making them prone to sophisticated cyberattacks and network anomalies. The literature highlights VAEs as a powerful tool due to their ability to model complex distributions and detect rare or unusual patterns.
In the area of fake base station detection, I scanned papers that discuss the vulnerabilities of 5G and 6G networks to spoofing attacks. These attacks exploit

base stations to intercept communications or inject malicious traffic. Most papers emphasize the importance of real-time detection techniques using machine learning models trained on network traffic patterns.
For the third focus, I explored survey papers related to anomaly detection in cryptocurrency, focusing on how anonymity features, such as those found in blockchain-based networks, can be used to obscure illicit activities. The literature on cryptocurrency detection methodologies is evolving, with increased attention on how machine learning models can identify suspicious behaviors in otherwise anonymous transactions.

3 Research Direction

3.1 Initial Research Direction

I am exploring anomaly detection in three interconnected fields: 5G/6G networks, fake base stations, and cryptocurrency networks. My research direction will focus on these core areas: This involves using machine learning techniques, specifically VAEs, to detect anomalies in high-speed, large-scale 5G and upcoming 6G networks. These networks are prone to security threats due to their decentralized nature and the increased complexity of data.With the rise of 5G/6G, fake base stations have become a significant threat. Detecting these stations involves analyzing network traffic and identifying anomalies that indicate spoofing or unauthorized access.Cryptocurrency networks, especially those that provide anonymity, pose challenges for detecting malicious behavior without violating privacy. I will investigate how machine learning models can detect abnormal transactions or behaviors in such networks.

3.2 Survey Paper Search

I focused on searching for relevant survey papers related to the above areas. I targeted papers from the last 7 years that provide comprehensive overviews of:

- Anomaly detection in 5G/6G networks
- Machine learning approaches, especially VAEs, in network security
- Detection of fake base stations and security issues in mobile networks
- Security and anomaly detection in cryptocurrency networks, particularly focusing on anonymous networking

Below is the list of survey papers that I have found, which are relevant to these topics and published within the last 7 years:

Paper 1: `http://dx.doi.org/10.14257/ijsia.2018.12.4.02`
Ibor, A. E., Oladeji, F. A., & Okunoye, O. B. (2018).*A survey of cyber security approaches for attack detection prediction and prevention.* International Journal

of Security and its Applications, 12(4), 15-28.

Paper 2: https://doi.org/10.1109/COMST.2018.2871866
Husák, M., Komárková, J., Bou-Harb, E., & Čeleda, P. (2018). *Survey of attack projection, prediction, and forecasting in cyber security.* IEEE Communications Surveys & Tutorials, 21(1), 640-660.

Paper 3: https://doi.org/10.3390/info10040122
Berman, D. S., Buczak, A. L., Chavis, J. S., & Corbett, C. L. (2019). *A survey of deep learning methods for cyber security.* Information, 10(4), 122.

Paper 4: https://doi.org/10.1109/ICCCI.2019.8821951
Tirumala, S. S., Valluri, M. R., & Babu, G. A. (2019, January). **A survey on cybersecurity awareness concerns, practices and conceptual measures**. In 2019 International Conference on Computer Communication and Informatics (ICCCI) (pp. 1-6). IEEE.

Paper 5: https://doi.org/10.1109/ACCESS.2020.3041951
Shaukat, K., Luo, S., Varadharajan, V., Hameed, I. A., & Xu, M. (2020).**A survey on machine learning techniques for cyber security in the last decade** . IEEE access, 8, 222310-222354.

Paper 6: https://doi.org/10.1109/HORA49412.2020.9152899
Alabadi, M., & Celik, Y. (2020, June). **Anomaly detection for cyber-security based on convolution neural network: A survey**. In 2020 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA) (pp. 1-14). IEEE.

Paper 7: https://doi.org/10.1109/ICICCS51141.2021.9432210
Parkar, P., & Bilimoria, A. (2021, May). **A survey on cyber security IDS using ML methods**. In 2021 5th International Conference on Intelligent Computing and Control Systems (ICICCS) (pp. 352-360). IEEE.

Paper 8: https://doi.org/10.1109/JAS.2021.1004261
Zhang, J., Pan, L., Han, Q. L., Chen, C., Wen, S., & Xiang, Y. (2021).**Deep learning based attack detection for cyber-physical system cybersecurity: A survey**. IEEE/CAA Journal of Automatica Sinica, 9(3), 377-391.

Paper 9: https://doi.org/10.1016/j.neucom.2022.06.002
Pawlicki, M., Kozik, R., & Choraś, M. (2022). **A survey on neural networks for (cyber-) security and (cyber-) security of neural networks**. Neurocomputing, 500, 1075-1087.

Paper 10: https://doi.org/10.1007/978-981-16-8012-0_2
Pandey, A. B., Tripathi, A., & Vashist, P. C. (2022). **A survey of cyber security trends, emerging technologies and threats**. Cyber Security in

Intelligent Computing and Communications, 19-33.

Paper 11: `https://doi.org/10.3390/electronics12061333`
Aslan, Ö., Aktuğ, S. S., Ozkan-Okay, M., Yilmaz, A. A., & Akin, E. (2023). **A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions**. Electronics, 12(6), 1333.

Paper 12: `https://doi.org/10.1016/j.csa.2023.100031`
Admass, W. S., Munaye, Y. Y., & Diro, A. (2023). **Cyber security: State of the art, challenges and future directions**. Cyber Security and Applications, 100031.

Paper 13: `https://doi.org/10.1145/3657647`
Mvula, P. K., Branco, P., Jourdan, G. V., & Viktor, H. L. (2024). **A Survey on the Applications of Semi-supervised Learning to Cyber-security**. ACM Computing Surveys, 56(10), 1-41.

Paper 14: `https://doi.org/10.1016/j.comnet.2024.110695`
Kumar, N., & Chaudhary, A. (2024). **Surveying cybersecurity vulnerabilities and countermeasures for enhancing UAV security**. Computer Networks, 252, 110695.

Paper 15: `https://doi.org/10.1002/9781394213948.ch5`
Nair, M. M., Deshmukh, A., & Tyagi, A. K. (2024). **Artificial intelligence for cyber security: Current trends and future challenges**. Automated Secure Computing for Next-Generation Systems, 83-114.

4 Critical Review of Survey Papers

I scanned five of the most relevant survey papers and provided brief notes on each, focusing on their structure, contributions, and citations.

Paper 1: `http://dx.doi.org/10.14257/ijsia.2018.12.4.02`
Ibor, A. E., Oladeji, F. A., & Okunoye, O. B. (2018). *A survey of cyber security approaches for attack detection prediction and prevention.* International Journal of Security and its Applications, 12(4), 15-28.

Notes: This paper surveys different approaches for detecting, predicting, and preventing cyber-attacks, focusing on both reactive and proactive techniques. The work highlights the importance of machine learning models in attack prediction and discusses future trends in the field.

Story: "This paper provides a comprehensive overview of traditional and machine learning-based cybersecurity techniques, aiming to offer a roadmap for

attack prediction and prevention."

Why it's not highly cited: The paper lacks depth in discussing cutting-edge technologies like deep learning, which may explain its moderate citation count.

Paper 2: `https://doi.org/10.1109/COMST.2018.2871866`
Husák, M., Komárková, J., Bou-Harb, E., & Čeleda, P. (2018). *Survey of attack projection, prediction, and forecasting in cyber security.* IEEE Communications Surveys & Tutorials, 21(1), 640-660.

Notes: This highly cited paper focuses on attack prediction and forecasting techniques in cybersecurity, offering a detailed analysis of various methods, including machine learning and statistical models.

Story: "This paper reviews attack prediction and forecasting methods in cybersecurity, focusing on both traditional and machine learning-based approaches to provide a framework for proactive threat detection."

Why it's highly cited: The paper's appeal lies in its thorough examination of predictive models, making it relevant to academic research and practical cybersecurity.

Paper 3: `https://doi.org/10.3390/info10040122`
Berman, D. S., Buczak, A. L., Chavis, J. S., & Corbett, C. L. (2019). *A survey of deep learning methods for cyber security.* Information, 10(4), 122.

Notes: This paper offers an in-depth review of deep learning methods for cybersecurity, covering intrusion detection, malware detection, and anomaly detection. It is highly relevant to my focus on anomaly detection using machine learning in 5G/6G networks and cryptocurrency.

Story: "The paper reviews the state-of-the-art deep learning methods in cybersecurity, highlighting their application in anomaly detection, intrusion detection, and malware identification."

Why it's moderately cited: Deep learning is a popular topic, but the paper may not introduce groundbreaking new methodologies, limiting its citation count compared to more innovative works.

Paper 4: `https://doi.org/10.1109/ICCCI.2019.8821951`
Tirumala, S. S., Valluri, M. R., & Babu, G. A. (2019, January). *A survey on cybersecurity awareness concerns, practices and conceptual measures.* In 2019 International Conference on Computer Communication and Informatics (ICCCI) (pp. 1-6). IEEE.

Notes: This paper focuses on the human aspect of cybersecurity, specifically on

awareness and training. Although it is not directly related to technical anomaly detection, it provides insights into broader cybersecurity practices.

Story: "This paper examines the human factors in cybersecurity, with a focus on awareness programs and training initiatives aimed at reducing vulnerabilities in organizations."

Why it's not highly cited: The human aspect of cybersecurity, while important, is often overshadowed by the technical aspects, resulting in fewer citations.

Paper 5: `https://doi.org/10.1109/ACCESS.2020.3041951`
Shaukat, K., Luo, S., Varadharajan, V., Hameed, I. A., & Xu, M. (2020). *A survey on machine learning techniques for cyber security in the last decade.* IEEE Access, 8, 222310-222354.

Notes: This paper provides a broad survey of machine learning techniques applied to cybersecurity over the last decade. It includes anomaly, intrusion, and malware detection, making it highly relevant to my research.

Story: "This paper surveys machine learning techniques in cybersecurity over the past decade, offering a detailed review of their application in anomaly detection and malware identification."

Why it's moderately cited: The paper covers a wide range of techniques but may not offer specific solutions, limiting its direct applicability for researchers focusing on niche areas.

4.1 Highly Cited Paper

Reference:
Husák, M., Komárková, J., Bou-Harb, E., & Čeleda, P. (2018). *Survey of attack projection, prediction, and forecasting in cyber security.* IEEE Communications Surveys & Tutorials, 21(1), 640-660. `https://doi.org/10.1109/COMST.2018.2871866`

Notes:
This paper is highly cited because it comprehensively covers various methods for attack projection, prediction, and forecasting in cybersecurity. The breadth and depth of the paper make it relevant to both academic researchers and industry professionals. It includes a detailed analysis of machine learning and statistical models used for threat detection and forecasting.
Story:
"This paper reviews attack prediction and forecasting methods in cybersecurity, focusing on both traditional and machine learning-based approaches to provide a framework for proactive threat detection."

4.2 Cited Paper (3+ years old)

Reference:
Ibor, A. E., Oladeji, F. A., & Okunoye, O. B. (2018). *A survey of cyber security approaches for attack detection, prediction, and prevention.* International Journal of Security and its Applications, 12(4), 15-28. `http://dx.doi.org/10.14257/ijsia.2018.12.4.02`

Notes:
This paper surveys various cybersecurity approaches for attack detection, prediction, and prevention. It covers both traditional and machine learning-based techniques but lacks in-depth coverage of cutting-edge technologies such as deep learning. Despite being moderately cited, the paper remains useful for understanding foundational approaches in cybersecurity.
Story:
"This paper provides a comprehensive overview of traditional and machine learning-based cybersecurity techniques, aiming to offer a roadmap for attack prediction and prevention."

5 Identifying Gaps

Upon scanning the references of the selected papers, I identified several potential gaps in the existing surveys. These gaps suggest areas where further research could be beneficial:

- Gap 1: Limited coverage on **anomaly detection using VAEs specifically for decentralized 5G/6G networks**. While the current surveys cover anomaly detection techniques, there is a lack of focus on VAEs in the context of next-generation decentralized wireless networks.
- Gap 2: Insufficient exploration of **fake base station detection using machine learning models** in newer network architectures (e.g., 5G/6G). Most papers discuss detection in 4G or earlier systems, with less emphasis on the complexities introduced by advanced architectures.
- Gap 3: A gap in addressing **privacy-preserving anomaly detection methods** in cryptocurrency networks. Although several papers discuss anomaly detection in cryptocurrencies, there is limited attention on methods that maintain user privacy while still identifying malicious behaviors.
- Gap 4: Lack of integration between **cross-domain anomaly detection**for both wireless networks and blockchain systems. The existing literature does not fully explore the potential benefits of shared techniques between these domains.

6 Potential Survey Paper Stories

Based on the gaps identified, I generated 3-4 potential survey paper stories that could address these areas:

- **Story 1:** "This survey explores the application of Variational Autoencoders (VAEs) for anomaly detection in decentralized 5G/6G networks, highlighting the challenges and benefits of using VAEs in a highly decentralized environment."
- **Story 2:** "This paper surveys fake base station detection methods in 5G/6G networks, with a focus on machine learning-based approaches that address the unique challenges posed by advanced network architectures."
- **Story 3:** "This survey examines privacy-preserving anomaly detection techniques in cryptocurrency networks, offering a comprehensive review of methods that balance privacy concerns with security needs."
- **Story 4:** "This survey integrates anomaly detection techniques from both wireless networks and blockchain technologies, identifying common approaches and challenges in securing cross-domain systems."

By identifying gaps in the existing literature and generating potential survey paper stories, I have outlined several directions for future research that could contribute to the fields of anomaly detection in 5G/6G networks, fake base station detection, and privacy-preserving techniques in cryptocurrency.