International Journal of Computer Trends and Technology
ISSN: 2231–2803 / https://doi.org/10.14445/22312803/IJCTT-V72I1P113

Volume 72 Issue 1, 77-82, January 2024

Review Article

Botnet Detection and Mitigation: A Comprehensive Literature Review

Saurav Bhattacharya[1], Anirudh Khanna[2], Rajat Dubey[3]

[1]*InfoSec Expert, Independent Researcher, Seattle, Washington, United States.*
[2]*Data Recovery Expert, Pacific Gas and Electric Company, San Francisco Bay Area, United States.*
[3]*Cybersecurity Expert, Allianz Commercial, Austin, United States.*

[1]*Corresponding Author : online.saurav@gmail.com*

Received: 25 November 2023 Revised: 04 January 2024 Accepted: 23 January 2024 Published: 31 January 2024

Abstract *- Botnets represent one of the most formidable challenges in cybersecurity, orchestrating a range of malicious activities that threaten individual, organizational, and national security. This article provides a comprehensive review of the evolution of botnets, the methodologies for their detection, and the strategies employed for their mitigation. It traces the journey of botnets from their inception as simple networks of infected devices to their current status as sophisticated, adaptive structures capable of significant disruption. Detection methodologies have evolved from basic signature-based techniques to advanced methods incorporating anomaly detection, behavioral analysis, and machine learning. Yet, they continue to grapple with the increasing sophistication of botnet tactics. Mitigation strategies, encompassing preventive measures, responsive actions, and legal and cooperative efforts, are discussed for their effectiveness and challenges. The article also presents case studies of notable botnet attacks, providing real-world insights into the complexities of combating these threats. Finally, it explores future directions, highlighting the potential advancements in botnet technology and the ongoing need for innovative research, proactive strategies, and international collaboration in the fight against botnets. This review aims to inform and inspire researchers, practitioners, and policymakers as they navigate the ever-evolving landscape of botnet threats and defenses.*

Keywords *- Botnets, Cybersecurity Challenges, Detection Methodologies, Mitigation Strategies, Evolution of Botnets, Machine Learning in Cybersecurity, International Collaboration in Cyber Defense.*

1. Introduction

In the ever-evolving landscape of cyber threats, botnets have emerged as a formidable force, orchestrating a range of malicious activities from distributed denial-of-service (DDoS) attacks to widespread data breaches [26]. Originating from the simple concept of a robot network, botnets have evolved into complex architectures capable of eluding detection and causing significant damage to individuals, organizations, and nations. This review delves into the intricate world of botnets, tracing their evolution from rudimentary networks to sophisticated, distributed entities.

Understanding botnets is paramount in the digital age, as they are not just a threat to security but also a challenge to the economic and social fabric of the digital world [17]. They are the Swiss army knife of the cybercriminal, enabling a variety of attacks with increasing complexity and scale [13]. As technology permeates every aspect of life, the potential for botnets to disrupt, deceive, and damage grows, making it crucial for cybersecurity professionals to stay ahead of these threats.

This article aims to provide a comprehensive review of botnets, encompassing their history, evolution, and the various strategies employed in their detection and mitigation. Specifically, it will cover:

- Historical Overview: Tracing the origins and significant milestones in the development of botnets [10].
- Technical Evolution: Examining the advancements in botnet architecture, communication mechanisms, and attack methodologies [2].
- Detection Techniques: Exploring the various methods employed to detect botnets, including the challenges and limitations faced in effectively identifying them (Binkley & Singh, 2006).
- Mitigation Strategies: Discuss the approaches and best practices in mitigating the impact of botnets, including legal, technical, and cooperative efforts [21].

By dissecting these components, the article will provide a holistic view of botnets, offering insights into their complex nature and the multifaceted approach required to combat them.

2. Evolution of Botnets

The concept of botnets dates back to the early days of the internet when the first malicious bots were simple and primarily focused on vandalism and small-scale disruptions [27]. The infamous Morris Worm in 1988 is often cited as one of the first examples of a botnet, as it used a network of infected devices to propagate itself [12]. These early botnets were limited in scope and sophistication but laid the groundwork for more advanced threats.

As technology advanced, so did botnets. The late 1990s and early 2000s saw a significant evolution in botnet capabilities. Attackers began to use centralized command-and-control (C&C) servers to manage their networks of compromised devices, allowing for coordinated attacks and greater control [11]. This period also saw the introduction of modular botnets that could be updated with new capabilities after deployment, making them more resilient and harder to combat [17].

The sophistication of botnets further increased with the adoption of peer-to-peer (P2P) architecture in the mid-2000s. P2P botnets distributed their control mechanisms across the network, making them more resistant to takedown attempts and enabling large-scale distributed denial-of-service (DDoS) attacks, spam campaigns, and financial theft [19].

Today's botnets are more advanced than ever, utilizing a range of tactics to avoid detection and enhance their impact. They employ domain generation algorithms (DGAs) to dynamically generate domain names for their C&C servers, making them harder to block [3]. Encryption and fast-flux networks are also used to conceal command and control traffic and maintain the botnet's infrastructure [29].

Modern botnets can target a wide range of devices, including not just computers but also IoT devices, smartphones, and other connected technologies. This expansion has led to massive botnets, such as Mirai, which in 2016 managed to take down significant portions of the internet infrastructure through an unprecedented DDoS attack using compromised IoT devices [22].

As botnets have evolved, so have the challenges they present. Their increasing complexity and adaptability make them difficult to detect and dismantle. Botnet operators continuously innovate, using techniques like polymorphism and metamorphism to evade signature-based detection and employing sophisticated obfuscation techniques to hide their presence [32].

The decentralized nature of modern botnets also poses significant legal and jurisdictional challenges, as their infrastructure often spans multiple countries and legal systems. This complexity necessitates a coordinated, international approach to law enforcement and cybersecurity efforts [2].

The evolution of botnets represents a continuous arms race between attackers and defenders. From their humble beginnings to their current state as sophisticated, multifaceted threats, botnets have consistently adapted to new technologies and countermeasures. Understanding their evolution is crucial for developing effective strategies to detect, mitigate, and ultimately prevent these pervasive threats.

3. Detection Methodologies

As botnets have evolved into more sophisticated and elusive entities, the methodologies for detecting them have also advanced. Detection is a critical component in the fight against botnets, as early identification can prevent widespread damage and aid in the dismantling of the botnet infrastructure. This section reviews the primary techniques used in botnet detection, highlighting their methodologies, advantages, and limitations.

3.1. Signature-Based Detection

Signature-based detection is one of the earliest and most straightforward methods for identifying botnets. It involves matching observed activities or malware samples against a database of known signatures or patterns associated with botnets. While effective against known threats, this method struggles with new or modified botnets due to its reliance on pre-existing signatures.

- Advantages: High accuracy for known threats, easy to implement.
- Limitations: Ineffective against new or evolving botnets, requires regular updates.

3.2. Anomaly-Based Detection

Anomaly-based detection methods focus on identifying deviations from normal network or system behavior, which may indicate botnet activity [15]. These techniques use machine learning algorithms and statistical models to detect unusual patterns such as sudden spikes in traffic, irregular communication intervals, or unexpected protocol usage.

- Advantages: Can detect previously unknown botnets, adaptable to new patterns.
- Limitations: Higher false positive rates require extensive training data.

3.3. Behavioral Analysis

Behavioral analysis goes beyond simple pattern matching or anomaly detection by examining the behavior of hosts or networks over time [13]. This method involves analyzing communication patterns, user activity, and other contextual information to identify bot-like behaviors. Behavioral analysis can be particularly effective against bots that exhibit regular, predictable patterns of activity.

- Advantages: Effective against sophisticated and low-volume botnets, provides detailed context.
- Limitations: Resource-intensive, may require manual interpretation.

3.4. Heuristic Analysis

Heuristic analysis uses a set of rules or algorithms to identify botnet characteristics that are not captured by traditional signatures. It is a more flexible approach that can adapt to new and evolving threats by focusing on the properties and actions typical of botnets rather than specific signatures.

- Advantages: Adaptable to new threats, less reliant on updates.
- Limitations: Can produce false positives and require expert knowledge to develop heuristics.

3.5. Challenges in Botnet Detection

Detecting botnets is inherently challenging due to their evolving nature and the increasing use of sophisticated evasion techniques. Some of the primary challenges include:

- Encryption and Obfuscation: Many modern botnets use encryption and obfuscation techniques to hide their traffic and evade detection.
- Peer-to-Peer Architectures: The decentralized nature of P2P botnets makes it difficult to pinpoint a single point of failure or control.
- Polymorphism and Metamorphism: Botnets that frequently change their code or behavior can evade signature-based and heuristic detection methods.
- Scale and Distribution: The vast number of compromised devices and the global distribution of botnets complicate detection and response efforts.

Detecting botnets is a complex task that requires a multifaceted approach. No single methodology is sufficient; rather, a combination of signature-based, anomaly-based, behavioral, and heuristic techniques is often necessary to effectively identify and mitigate botnet threats. As botnets continue to evolve, so too must the strategies and technologies used to detect them. Ongoing research and development in this area are critical to staying ahead of emerging threats.

4. Mitigation Strategies

Mitigating the impact of botnets is a critical aspect of cybersecurity, involving a range of strategies aimed at preventing, containing, and dismantling botnet infrastructure [8]. Effective mitigation not only reduces the immediate threat of a particular botnet but also enhances the overall resilience of networks and systems against future attacks.

4.1. Preventive Measures

Preventive measures are proactive steps taken to reduce the likelihood of botnet infection and proliferation. These include:

- Security Awareness and Training: Educating users about the risks of botnets and safe practices to avoid infection [14].
- Regular Updates and Patch Management: Keeping software and systems updated to patch vulnerabilities that could be exploited by botnets [20].
- Antivirus and Antimalware Solutions: Deploying comprehensive security solutions that can detect and block botnet-related malware [30].
- Network Security Measures: Implementing firewalls, intrusion detection systems, and other network security tools to monitor and control incoming and outgoing traffic [28].

4.2. Response Strategies

Once a botnet infection is detected, response strategies aim to contain and eliminate the threat. Key response strategies include:

- Isolation of Infected Devices: Quickly isolating infected devices to prevent the spread of the botnet within the network [33].
- Removal of Malware: Utilizing specialized tools and techniques to remove botnet malware from infected devices [24].
- Recovery and Restoration: Restoring affected systems and data from backups and ensuring that all traces of the botnet have been removed [23].

4.3. Legal and Cooperative Efforts

Combating botnets often requires cooperation across different sectors and jurisdictions, as well as legal measures to pursue and prosecute those responsible for botnets. These efforts include:

- Law Enforcement Collaboration: Working with law enforcement agencies to track down and prosecute botnet operators [1].
- International Cooperation: Engaging in international efforts to dismantle botnet infrastructure that spans multiple countries [7].
- Public-Private Partnerships: Collaborating with private sector entities, such as ISPs and technology companies, to share information and coordinate responses to botnet threats [16].

4.4. Challenges in Botnet Mitigation

Mitigating botnets presents several challenges, including:

- Evolving Tactics: As botnet operators continue to innovate, mitigation strategies must also evolve to address new tactics and technologies [13].
- Scale and Complexity: The sheer size and complexity of some botnets make it difficult to dismantle their infrastructure fully [10].
- Collateral Damage: Aggressive mitigation efforts, such as taking down botnet command and control servers, can sometimes impact legitimate users and services.

Mitigating the impact of botnets requires a multi-layered approach that includes preventive measures, effective response strategies, and ongoing legal and cooperative efforts. While no single strategy is foolproof, a combination of these approaches can significantly reduce the risk and impact of botnets. Continuous adaptation and collaboration are key to staying ahead of botnet threats and ensuring the security and resilience of digital environments.

5. Case Studies

Examining specific instances of botnet attacks and their countermeasures provides valuable insights into the practical challenges and strategies involved in botnet mitigation. This section presents a series of case studies that highlight significant botnet incidents, the approaches used to combat them, and the lessons learned from each.

5.1. Conficker

Conficker, also known as Downup or Downadup, emerged in 2008 and infected millions of computers worldwide, exploiting vulnerabilities in Microsoft Windows [6]. A coalition of private and public entities formed the Conficker Working Group to combat the spread of the worm. Their efforts included patching vulnerabilities, coordinating with ISPs to reduce the worm's spread, and increasing public awareness [25]. The Conficker case highlighted the importance of timely patch management, international cooperation, and the effectiveness of a coordinated response to widespread botnet threats.

5.2. Mirai

The Mirai botnet, known for its massive DDoS attacks in 2016, primarily infected IoT devices such as cameras and DVRs. It marked a significant shift in botnet capabilities and targets [4]. Efforts to mitigate Mirai included identifying and patching vulnerable devices, taking down C&C servers, and implementing network-level DDoS protection measures [22]. Mirai demonstrated the vulnerabilities in IoT devices and the need for improved security in these devices. It also underscored the potential scale and impact of DDoS attacks facilitated by botnets.

5.3. Storm Worm

Storm Worm was a Trojan horse program that surfaced in 2007, creating a botnet used for various malicious activities, including sending spam emails and conducting DDoS attacks. Researchers and cybersecurity experts analyzed the Storm Worm's behavior, leading to the development of more effective antivirus signatures and behavioral detection techniques. Efforts also focused on disrupting the botnet's communication channels [17]. The Storm Worm case emphasized the need for continuous research and development in detection methodologies and the benefits of understanding botnet communication patterns for effective disruption.

These case studies illustrate the diverse nature of botnet threats and the multifaceted approach required for effective mitigation. They highlight the importance of readiness, resilience, and cooperation among various stakeholders in the cybersecurity ecosystem. By learning from past incidents, the cybersecurity community can better prepare for and respond to future botnet challenges.

6. Future Directions

As technology continues to advance, so do the capabilities and complexity of botnets. This section discusses the potential future directions of botnet development, the ongoing research needs, and the implications for cybersecurity strategies.

6.1. Emerging Threats

- IoT and Botnets: With the proliferation of IoT devices, future botnets may increasingly target these devices due to their often-lax security and the high volume of potential recruits [18].
- AI and Machine Learning: The use of AI and machine learning by attackers could lead to more adaptive and resilient botnets capable of evading detection and automating attack strategies [5].
- Decentralization: Further decentralization of botnet command and control structures could make future botnets more robust against takedown attempts [31].

6.2. Research Needs

- Detection and Attribution: As botnets become more sophisticated, research into new detection methodologies and attribution techniques will be crucial.
- Mitigation Strategies: Developing and refining botnet mitigation strategies, particularly in the context of rapidly evolving technology landscapes, remains a critical area of research [20].
- International Cooperation: Enhancing mechanisms for international cooperation is necessary to combat botnets that operate across borders [7].

6.3. Technological Advancements

- Quantum Computing: The advent of quantum computing could both pose new challenges for botnet defense and offer new tools for disrupting botnet activities.
- Blockchain Technology: While often associated with security and trust, blockchain could also be used by attackers to create more resilient and anonymous botnets [9].

The future of botnets is likely to be characterized by increased sophistication, scale, and impact, posing significant challenges to the cybersecurity community. Staying ahead of these threats will require continuous innovation in detection and mitigation strategies, as well as

a commitment to global cooperation and knowledge sharing. By anticipating future trends and investing in research and development, the cybersecurity community can prepare to meet these challenges head-on.

7. Conclusion

This article has provided a comprehensive review of botnets, including their evolution, the methodologies for their detection, strategies for mitigation, and insightful case studies. Botnets have grown from simple networks of infected devices to sophisticated and resilient structures capable of massive disruption. Detection methodologies have evolved from signature-based to more advanced anomaly and behavioral analysis, yet they continue to face challenges due to the adaptive nature of botnets. Mitigation strategies, while diverse and improving, require ongoing adaptation and international cooperation to be effective. The battle against botnets is ongoing and dynamic. As technology advances, so too do the capabilities of both botnets and the measures designed to combat them. Continued vigilance is necessary to identify and respond to new threats as they emerge. Innovation in technology and strategy is critical to staying ahead of attackers, requiring a proactive and anticipatory approach to cybersecurity.

7.1. Call to Action

- For Researchers: There is a need for continuous research into new and emerging botnet threats, as well as the development of innovative detection and mitigation strategies. Collaboration across academic, industry, and government sectors can drive forward the necessary advancements in this field.
- For Practitioners: Cybersecurity professionals must remain ever-vigilant, updating their knowledge and skills to combat the latest botnet strategies. Implementing best practices, sharing information within the community, and participating in collective defense efforts are all crucial.
- For Policymakers: Supporting and fostering international cooperation, creating robust legal frameworks, and investing in cybersecurity infrastructure are vital steps in the global fight against botnets. Looking to the future, the importance of understanding, detecting, and combating botnets cannot be overstated. The security and stability of our digital world depend on the collective efforts of individuals and organizations across the globe.

References

[1] Ross Anderson et al., *Measuring the Cost of Cybercrime, the Economics of Information Security and Privacy*, Springer, Berlin, Heidelberg, pp. 265-300, 2013. [CrossRef] [Google Scholar] [Publisher Link]

[2] Jason Andress, and Steve Winterfeld, *Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners*, Elsevier Science, pp. 1-324, 2013. [Google Scholar] [Publisher Link]

[3] Manos Antonakakis et al., "From Throw-Away Traffic to Bots: Detecting the Rise of DGA-Based Malware," *21st USENIX Security Symposium*, 2012. [Google Scholar] [Publisher Link]

[4] Manos Antonakakis et al., "Understanding the Mirai Botnet," *26th USENIX Security Symposium*, Vancouver, BC, Canada, pp. 1093-1110, 2017. [Google Scholar] [Publisher Link]

[5] Giovanni Apruzzese et al., "On the Effectiveness of Machine and Deep Learning for Cybersecurity," *2018 10th International Conference on Cyber Conflict (CyCon)*, Tallinn, Estonia, pp. 371-390, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[6] Brian M. Bowen et al., "Baiting Inside Attackers Using Decoy Documents," *International Conference on Security and Privacy in Communication Systems*, pp. 51-70, 2009. [CrossRef] [Google Scholar] [Publisher Link]

[7] James R. Binkley, and Suresh Singh, "An Algorithm for Anomaly-Based Botnet Detection," *2nd Workshop on Steps to Reducing Unwanted Traffic on the Internet*, pp. 43-48, 2006. [Google Scholar] [Publisher Link]

[8] Douglas Maughan, "The Need for a National Cybersecurity Research and Development Agenda," *Communications of the ACM*, vol. 52, no. 2, pp. 29-31, 2009. [CrossRef] [Google Scholar] [Publisher Link]

[9] M.M.R Chowdhury, and A.S Namin, "The Evolution of Botnet Detection and Mitigation," *IEEE Potentials*, vol. 36, no. 5, 2017.

[10] Mauro Conti et al., "A Survey on Security and Privacy Issues of Bitcoin," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 4, pp. 3416-3452, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[11] Evan Cooke, Farnam Jahanian, and Danny McPherson, "The Zombie Roundup: Understanding, Detecting, and Disrupting Botnets," *SRUTI '05 Steps to Reducing Unwanted Traffic on the Internet Workshop*, pp. 39-44, 2005. [Google Scholar] [Publisher Link]

[12] D. Dittrich, "The "Stacheldraht" Distributed Denial of Service Attack Tool," *USENIX Security Symposium*, 2002. [Google Scholar]

[13] M.W Eichin, and J.A Rochlis, "With Microscope and Tweezers: An Analysis of the Internet Virus of November 1988," *IEEE Symposium on Security and Privacy*, Oakland, CA, USA, pp. 326-343, 1989. [CrossRef] [Google Scholar] [Publisher Link]

[14] Maryam Feily, Alireza Shahrestani, and Sureswaran Ramadass "A Survey of Botnet and Botnet Detection," *Third International Conference on Emerging Security Information, Systems and Technologies*, Athens, Greece, pp. 268-273, 2009. [CrossRef] [Google Scholar] [Publisher Link]

[15] Thomas A. Johnson, *Cybersecurity: Protecting Critical Infrastructures from Cyber Attack and Cyber Warfare*, CRC Press, pp. 1-363, 2014. [Google Scholar] [Publisher Link]

[16] P. García-Teodoro et al., "Anomaly-based Network Intrusion Detection: Techniques, Systems and Challenges," *Computers & Security*, vol. 28, no. 1-2, pp. 18-28, 2009. [CrossRef] [Google Scholar] [Publisher Link]

[17] Marc D Goodman, and Susan W Brenner, "The Emerging Consensus on Criminal Conduct in Cyberspace," *International Journal of Law and Technology*, vol. 10, no. 2, pp. 139-223, 2002. [CrossRef] [Google Scholar] [Publisher Link]

[18] Julian B. Grizzard et al., "Peer-to-Peer Botnets: Overview and Case Study," *First Workshop on Hot Topics in Understanding Botnets*, pp. 1-8, 2007. [Google Scholar] [Publisher Link]

[19] Stephen Herwig et al., "Measurement and Analysis of Hajime, a Peer-to-peer IoT Botnet," *Network and Distributed System Security Symposium*, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[20] Thorsten Holz et al., "Measurements and Mitigation of Peer-to-Peer-based Botnets: A Case Study on Storm Worm," *Proceedings of the 1st Usenix Workshop on Large-Scale Exploits and Emergent Threats*, San Francisco California, pp. 1-9, 2008. [Google Scholar] [Publisher Link]

[21] Julian Jang-Jaccard, and Surya Nepal, "A Survey of Emerging Threats in Cybersecurity," *Journal of Computer and System Sciences*, vol. 80, no. 5, pp. 973-993, 2014. [CrossRef] [Google Scholar] [Publisher Link]

[22] Sheharbano Khattak et al., "A Taxonomy of Botnet Behavior, Detection, and Defense," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 2, pp. 898-924, 2014. [CrossRef] [Google Scholar] [Publisher Link]

[23] Constantinos Kolias et al., "DDoS in the IoT: Mirai and Other Botnets," *Computer*, vol. 50, no. 7, pp. 80-84, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[24] Lei Liu et al., *BotTracer: Execution-based Bot-Like Malware Detection, Information Security*, Springer, Berlin, Heidelberg, pp. 97-113, 2009. [CrossRef] [Google Scholar] [Publisher Link]

[25] Niels Provos et al., "The Ghost in the Browser: Analysis of Web-based Malware," *First Workshop on Hot Topics in Understanding Botnets (HotBots 07)*, 2007. [Google Scholar] [Publisher Link]

[26] Seungwon Shin, Haopei Wang, and Guofei Gu, "A First Step toward Network Security Virtualization: From Concept to Prototype," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 10, pp. 2236-2249, 2012. [CrossRef] [Google Scholar] [Publisher Link]

[27] Sérgio S.C Silva et al., "Botnets: A survey," *Computer Networks*, vol. 57, no. 2, pp. 378-403, 2013. [CrossRef] [Google Scholar] [Publisher Link]

[28] L. Spitzner, "Honeypots: Catching the Insider Threat," *19th Annual Computer Security Applications Conference*, Las Vegas, NV, USA, pp. 170-179, 2003. [CrossRef] [Google Scholar] [Publisher Link]

[29] William Stallings, *Cryptography and Network Security: Principles and Practices*, Pearson/Prentice Hall, pp. 1-680, 2007. [Google Scholar] [Publisher Link]

[30] Feamster Nick, Konte Maria, and Jung, Jaeyeon, "*Fast-Flux Service Networks: Dynamics and Roles in Hosting Online Scams*," University of Maryland Institute for Advanced Computer Studies, Technical Report, 2008. [Google Scholar] [Publisher Link]

[31] Symantec, Internet Security Threat Report, vol. 23, 2018. [Publisher Link]

[32] Ping Wang, Sherri Sparks, and Cliff C. Zou, "An Advanced Hybrid Peer-to-Peer Botnet," *IEEE Transactions on Dependable and Secure Computing*, vol. 7, no. 2, pp. 113-127, 2010. [CrossRef] [Google Scholar] [Publisher Link]

[33] Ilsun You, and Kangbin Yim, K. "Malware Obfuscation Techniques: A Brief Survey," *International Conference on Broadband, Wireless Computing, Communication and Applications*, Fukuoka, Japan, pp. 297-300, 2010. [CrossRef] [Google Scholar] [Publisher Link]

[34] Saman Taghavi Zargar, James Joshi, and David Tipper, "A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks," *IEEE Communications Surveys & Tutorials*, vol. 15, no. 4, pp. 2046-2069, 2013. [CrossRef] [Google Scholar] [Publisher Link]