Detecting and Counteracting Adversaries in Wireless Multicast over Fading Channels

Nadieh Moghadam
Assistant Professor of Electrical Engineering
Shiley-Marcos School of Engineering
University of San Diego
5998 Alcalà Park, San Diego, CA 92110-2492
nmoghadam@sandiego.edu

Abstract

The demand for wireless multicast has surged in recent times. Concurrently, ensuring security in these systems presents significant challenges. This paper delves into enhancing throughput in the face of adversarial actions and introduces a moving average approach to address this. Our findings indicate that the multicast system's performance in terms of throughput and delay improved significantly, mirroring the efficiency of a system that operates without any adversaries.

Keywords: Multicast; Moving average; Adversary; Throughput; fading channel

I. Introduction

Wireless communication networks have become a cornerstone of modern society, powering everything from casual conversations to critical infrastructures. As these networks evolve, a particular area of interest and concern has emerged: the efficiency and security of wireless multicast systems, especially when faced with adversarial threats.

One of the primary attractions of wireless communication is its ability to disseminate information widely. Ensuring efficient throughput in multicast scenarios is pivotal for several reasons. For one, it guarantees the most productive utilization of available bandwidth. This translates into faster data dissemination, enabling real-time updates and ensuring a higher quality of service for end-users.

However, the multicast nature of these networks also makes them vulnerable. The presence of an adversary introduces a range of potential challenges. These adversaries, equipped with various malicious tactics, can significantly hamper network operations. They might jam signals, inject spurious data, or even eavesdrop on sensitive communications. Such activities not only reduce the network's effective throughput, leading to lags and service degradation, but they also raise pressing security concerns [1].

The economic implications of these threats are profound. As businesses increasingly lean on real-time data transmission, any delay or disruption can lead to missed opportunities, financial losses, and even reputational damage. This is especially concerning given the explosive growth in the number of wirelessly connected devices, thanks to the proliferation of the Internet of Things (IoT) and the emergence of 5G technologies. In this hyper-connected scenario, ensuring the security and high-throughput of multicast systems is nothing short of essential [2,3].

Research and development geared towards addressing these challenges have never been more critical. Delving into this topic can spur technological innovations, opening up new avenues in the field of wireless communications. Moreover, ensuring secure communication in the face of adversarial threats brings with it legal and ethical considerations, particularly when sensitive or personal information is at stake.

Extensive research has been conducted in this field. [4] present a secure wireless communication method focused on transmitting signals with minimal distortion while maintaining confidentiality from eavesdroppers. Their approach focuses on finite blocklength. They introduced a data-driven, adversarially trained deep coding system which may have limitations in the case of a novel type of adversary. Using Radio Tomographic Imaging (RTI), [5] developed a secure wireless communication model that detects adversaries. This system maintains secrecy even if eavesdroppers adjust their position, achieving rates as if prior path-loss knowledge was available.

In essence, in this paper, we enhanced the wireless multicast throughput, particularly in the face of adversarial conditions where malicious entities can flood the transmitter with illegitimate packets,

979-8-3503-7099-7/24/$31.00 ©2024 IEEE

attempting to mislead and disrupt its normal operations. In Section II, we outline the system model, which is followed by a detailed simulation presented in Section III. We wrap up with conclusions and potential avenues for future research in Section IV.

II. System Model

In a wireless communication multicast system model, robustness and reliability are paramount considerations. This system employs a combination of techniques to ensure effective data transmission, even in the presence of challenging channel conditions, including a Rayleigh channel and Additive White Gaussian Noise (AWGN), while addressing the threat of adversarial interference.

A. Multicast Communication Framework:

At the heart of this model is a multicast communication framework where a single transmitter broadcasts data packets to multiple receivers simultaneously. The objective is to ensure that all receivers reliably receive the transmitted data while mitigating the impact of channel impairments and potential adversarial attacks. Binary Phase Shift Keying (BPSK) modulation is employed to modulate the data before transmission. BPSK is an effective choice for this scenario as it is robust against channel impairments and noise. To enhance data integrity, the system incorporates a parity check error detection method. Before transmission, the transmitter appends parity bits to each data packet. When a receiver receives a packet, it independently computes the parity check based on the received data. If any errors are detected, this affects the acknowledgment (ACK) packet which gets sent to the source after each transmission.

B. SNR-Based Adversary Detection:

A notable innovation in this model is the use of Signal-to-Noise Ratio (SNR) as a crucial metric for detecting adversaries. After receiving a packet, each receiver calculates the SNR associated with its reception. The SNR is a reliable indicator of the signal's quality and validity, and it plays a pivotal role in assessing whether the received packet is legit.

To calculate the SNR after the signal has passed through the Rayleigh channel and has been added noise, you can use:

$$SNR = 10 * \log_{10} \frac{\text{Signal Power}}{\text{Noise Power}} \quad (1)$$

Where:

Signal Power is the power of the faded signal without noise, and it can be calculated by:

$$\text{Signal Power} = \frac{\sum|\text{fadedData}|^2}{\text{length of the data}} \quad (2)$$

Noise Power is the difference between the power of the received signal (after adding noise) and the Signal Power.

C. Dynamic ACK Generation:

Upon detecting a potential error in a received packet based on the computed SNR, the receiver generates an ACK packet. This ACK packet serves a dual purpose: it includes the calculated SNR value and conveys the result of the packet error detection process. Specifically, it indicates whether the received packet is considered to contain errors.

The goal is to label the ACK based on the SNR, particularly because the SNR from the actual receiver's feedback is correlated to the previous one due to the Rayleigh channel, while the adversary's SNR is random. Instead of directly comparing the SNR values, you should track the change or variation in SNR between consecutive feedback. If there is a sudden drastic change or no correlation with previous SNR values, it is likely from the adversary. Conversely, if there is a pattern or correlation in SNR changes, it is probably from the actual receiver.

Here is a possible approach to label packets based on SNR:

- Maintain a history of past SNRs and past error-detected values.
- Compute the difference or variation of the current SNR with the last received SNR.
- Similarly, track if the error_detectedion values have a correlation or pattern.

If both the SNR and error_detectedion show patterns consistent with past values (i.e., not random), label them as "valid", otherwise label them as "adversary".

D. Transmitter Decision and Adversarial Resilience:

The transmitter is responsible for receiving ACK packets from multiple receivers and making informed decisions based on the information provided. It takes into account the SNR data and the error detection results reported by the receivers. This information guides the transmitter in deciding whether it should retransmit the previous packet.

In the presence of potential adversaries, who aim to disrupt the system by sending falsified ACK packets, the inclusion of SNR values in the ACK packets adds an extra layer of resilience. The transmitter can carefully examine the received ACKs, cross-verify SNR values across multiple acknowledgments through the moving average technique for validation. This approach ensures that adversarial interference does not lead to excessive retransmissions and performance degradation.

It's important to highlight that the approach used to differentiate between adversary packets and valid packets involves a blind mechanism. In this context, if the system inadvertently identifies an adversary's ACK packet as a legitimate one, the SNR information from that non-legit packet is stored for future reference. This stored SNR data complicates the differentiation between authentic and adversarial packets in later transmissions.

III. Simulation

To demonstrate the effectiveness of our approach, we conducted simulations involving a wireless multicast packet system. Packet transmissions occurred over a Rayleigh fading channel with AWGN noise. Our code implementation included an acknowledgment feedback mechanism for making retransmission decisions. The acknowledgment contains the SNR value and the error detection result. However, an adversarial entity also sent acknowledgment packets in a similar format to confuse the transmitter. To counteract this interference, we introduced a moving average [6, 7] mechanism to mitigate the impact of false adversary packets within our system. In this simulation, we keep only the last 3 SNR entries as the history. When the size exceeds 3, the oldest entry is discarded. Also, the maximum number of retransmissions is assumed to be 3.

In Figure 1, we present the average throughput as a function of varying Signal-to-Noise Ratio (SNR) values for three scenarios: a baseline system without an adversary, the same system under the presence of an adversary, and the system where we applied the Moving Average Window Technique (MAWT) to counteract adversary packets. As SNR increases, it is evident that throughput improves across all scenarios. Notably, the throughput performance of the system with the applied moving window closely mirrors that of the baseline system without an adversary, both significantly outperforming the system affected by adversarial interference.

Figure 2 depicts the relationship between delay and SNR for all three systems. In this setup, a packet is permitted up to three retransmissions based on the ACK packet before it is discarded. We observe that the system implementing the moving average window (MAWT) exhibits performance comparable to that of the system without any adversary. This finding highlights the effectiveness of our approach in mitigating the impact of adversarial influences on system performance.

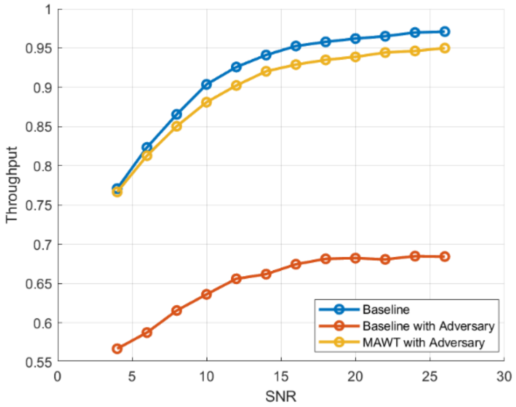

Figure 1: Throughput versus SNR for a Multicast System

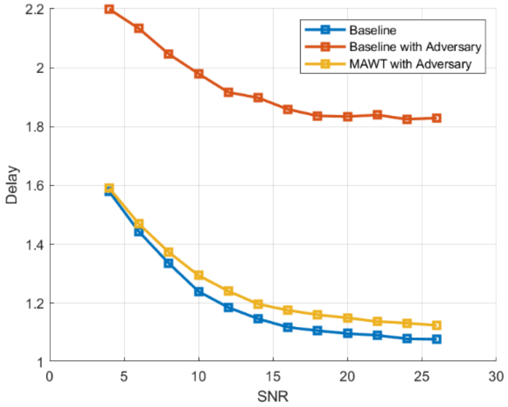

Figure 2: Delay versus SNR for a multicast system

IV. Conclusion and Future Work

In this paper, we present a wireless multicast system that operates over an AWGN Rayleigh channel and is fortified with error detection capabilities. To counteract the detrimental impacts of adversaries on system performance, we incorporated a moving average mechanism. Our findings reveal a substantial enhancement in system performance, bringing it nearly on par with a system free of adversarial interferences. As a prospective endeavor, we aim to integrate Network Coding into the transmitter and assess the resultant performance. We anticipate potential degradation in system efficacy in the face of adversaries, underscoring the need to explore more sophisticated methods for mitigating adversarial effects.

References

[1] T. T. Tran, H. Li, L. Liu and S. U. Khan, "Secure network-coded wireless multicast for delay-sensitive data," 2012 IEEE International Conference on Communications (ICC), Ottawa, ON, Canada, 2012, pp. 1943-1947, doi: 10.1109/ICC.2012.6364369.

[2] L. Ma et al., "Application of Wireless Communication Technology in Ubiquitous Power Internet of Things," 2020 IEEE 3rd International Conference on Computer and Communication Engineering Technology (CCET), Beijing, China, 2020, pp. 267-271, doi: 10.1109/CCET50901.2020.9213170.

[3] F. Ohori, S. Itaya, K. Maruhashi and F. Kojima, "Subdividing One Channel of 5GHz Wireless LAN into Narrow Channels for Factory IoT," 2018 21st International Symposium on Wireless Personal Multimedia Communications (WPMC), Chiang Rai, Thailand, 2018, pp. 632-635, doi: 10.1109/WPMC.2018.8713105.

[4] T. Marchioro, N. Laurenti and D. Gündüz, "Adversarial Networks for Secure Wireless Communications," ICASSP 2020 - 2020 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), Barcelona, Spain, 2020, pp. 8748-8752, doi: 10.1109/ICASSP40776.2020.9053216.

[5] M. Tahmasbi, M. Bloch and A. Yener, "In-Band Sensing of the Adversary's Channel for Secure Communication in Wireless Channels," 2019 IEEE International Symposium on Information Theory (ISIT), Paris, France, 2019, pp. 2184-2188, doi: 10.1109/ISIT.2019.8849506.

[6] "Time Series Analysis: Forecasting and Control" by George E. P. Box, Gwilym M. Jenkins, Gregory C. Reinsel, and Greta M. Ljung.

[7] W. Almuhtadi, B. Cheng, A. Aristama and O. Olafimihan, "Estimation of signal to noise ratio value based on Autoregressive Integrated Moving Average model in Intelligent Satellite System," 2008 Canadian Conference on Electrical and Computer Engineering, Niagara Falls, ON, Canada, 2008, pp. 000937-000940, doi: 10.1109/CCECE.2008.4564674.