www.ioirp.com

International Journal of Innovative Research in Technology, Science & Engineering (IJIRTSE)
ISSN: 2395-5619, Volume – 4, Issue – 2. April 2018

WIRELESS BROADCASTING AND THEIR SCHEMES

V.Chandru[1] , S.Saravanan[2], P.karthik[3]

1. Assistant Professor, Department of Visual Communications

2. Assistant Professor& Head, Department of Electronics & Communication Systems

3. Assistant Professor, Department of Electronics & Communication Systems
AJK College of Arts & Science, Coimbatore.

Abstract

A secure wireless broadcast network model is investigated, in which a source node broadcasts K confidential message flows to N user nodes, with each message intended to be decoded accurately by one user and to be kept secret from all of other users. a wireless broadcast network, where a single source reliably communicates independent messages to multiple destinations, with the potential aid of relays and cooperation between destinations. The wireless nature of the medium is captured by the broadcast nature of transmissions as well as the superposition of transmitted signals plus independent Gaussian noise at the received signal at any radio. We show that these are inadequate when applied to the broadcast model, and describe new protocols that preserve security with better performance, adequately addressing the requirements of security-critical environments. We provide analytical and some preliminary experimental evidence that our protocols achieve anonymity at a reasonable cost.

Keywords: Wireless, Broadcast, Schemes, Time-Based.

1. Introduction

Wireless broadcast networks constitute one class of basic and important wireless networks, where a source node simultaneously transmits a number of information flows (messages) to different destinations. Three important and challenging issues need to be addressed for wireless broadcast networks: reliability, security and stability. These three issues have been separately studied for wireless broadcast networks in previous work. Reliability requires that each information flow is received correctly at intended corresponding destinations, and the capacity region that includes all achievable rate vectors (rate allocation among users) has been studied. Following the seminal work of secure communication via the physical layer has been applied to study wireless broadcast networks, where reliability and security are jointly studied. A queue length based scheduling algorithm that achieves the network. Subsequently, network stability has also been studied jointly with reliability via the capacity region of wireless networks. Although jointly considering the above three issues has the potential for significant impact in improving network performance and resource efficiency, this perspective has not been examined before. One reason is because the physical layer approach to achieve security, which quantifies the measure of secrecy and greatly facilitates this joint design, has attracted considerable attention only recently.

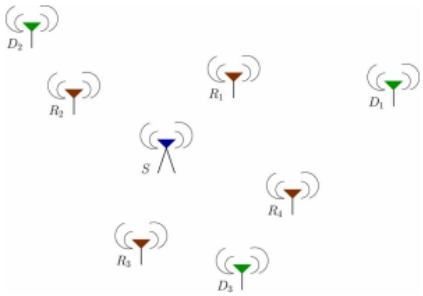

Figure 1: Wireless Broadcast Network

The scenario of study in this paper is a communication network with broadcast traffic, as illustrated in Fig. 1. Broadcast here means that a single source node is reliably communicating independent messages to multiple destination nodes using the help of multiple relay nodes. In the example of a cellular system, the setting represents down-link communication where the base-station is transmitting to multiple terminals with the potential help of relay stations. Note that some of the terminals can themselves act as relays. The term wireless most

commonly refers to the Gaussian network model, where the canonical Gaussian channel model describes the relationship between the transmitted and received symbols of the various nodes in the network.

2. Broadcast Schemes

Before describing different schemes, we make the following assumptions for all the broadcast schemes:

1) There is one source and M > 1 receivers.

2) Data is assumed to be sent in packets, and each packet is sent in a time slot of fixed duration.

3) The source assumes to know which packet from which receiver is lost. This can be accomplished through the use of positive and negative acknowledgments (ACK/NAKs). For simplicity, we assume all the ACK/NAKs are instantaneous, i.e. the source knows (a) whether or not a packet is lost and (b) identity of the receiver with the lost packet instantaneously. This implicitly assumes that ACK/NAKs are never lost. This assumption is not critical as we can incorporate the delay and bandwidth used by ACK/NAKs into the analysis.

4) Packet loss at a receiver i follows the Bernoulli distribution with parameter pi . In addition, the packet loss at different receivers is uncorrelated. This model is clearly insufficient to describe many real-world scenarios. However, this model is only intended for capturing the essence of wireless broadcast. One can develop a more accurate model, albeit complicate analysis.

A. Broadcast Schemes without Network Coding Scheme A (Memoryless receiver).

In this scenario, a receiver sends a NAK immediately whenever there is a packet loss in the current time slot, regardless whether it has received this packet correctly in some previous time slots (hence memoryless). This situation arises when a receiver received a correct packet, but this packet was lost at some other receivers at some previous time slots. Hence, the source has to retransmit this packet. If this packet is now lost in the current time slot, a memoryless receiver would automatically request a retransmission, even though it has correctly received the packet before. This scheme is clearly suboptimal in terms of bandwidth utilization as it implies that the source has to resend a packet until all the receivers receive this packet correctly and simultaneously.

Scheme B.

In this scenario, a receiver sends a NAK immediately only if there is a packet loss in the current time slot and this packet has not been received correctly in any previous time slot. This scheme is clearly superior to scheme A in terms of bandwidth utilization. Consider the following scenario with one source and two receivers R1 and R2. Suppose in the first time slot, a packet is correctly received at R1, but not at R2. So, the source has to rebroadcast this packet. In the second time slot, the packet is received correctly at R2, but not at R1. Using scheme A, the source has to retransmit the packet the third time because of the memoryless receivers. On the other hand, using scheme B, neither R1 nor R2 will send a NAK, and therefore the source can send a different packet, resulting in better bandwidth utilization.

B. Broadcast Schemes with Network Coding Scheme C (Time-based retransmission)

In this scheme, the receiver's protocol is similar to that of the receiver in scheme B in which it sends the NAK immediately if it does not receive a packet correctly. However, the source does not retransmit the lost packet immediately when it receives a NAK. Instead, the source maintains a list of lost packets and the corresponding receivers for which their packets are lost. The retransmission phase starts at a fixed interval of time in terms of number of time slots N, e.g. N = 100. During the retransmission phase, the source forms a new packet by XORing a maximum set of the lost packets from different receivers before retransmitting this combined packet to all the receivers. The combined packets may be lost during the retransmission, and these packets will be retransmitted until all the receivers receive this packet. The source keeps sending out the combined packets until no more lost packets on the list, it then resumes the transmission of a different set of packet. Even though a receiver successfully receives the combined packets, it must be able to recover the lost packets, and it does so by XORing this combined packets with appropriate set of previously successful packets. The information on choosing this appropriate set of packets are included in the packets sent by the source.

Scheme D (Improved time-based retransmission)

Scheme C is suboptimal because the source has to retransmit the same combined packet even though some receivers may receive it. An improved scheme is to have the source dynamically changes the combined packets based on what the receivers have received.

Conclusion

In this paper we propose some network coding techniques to increase the bandwidth efficiency of reliable broadcast in a wireless network. Our proposed schemes combine different lost packets from different receivers in such a way that multiple receivers are able to recover their lost packets with one transmission by the source. The advantages of the proposed schemes over the traditional wireless broadcast are shown through simulations and theoretical analysis. . To the authors' best knowledge, this is the first work that addresses the reliability, security (via a physical layer approach), and stability jointly for wireless broadcast networks. The approach in this paper can be applied to analyze other wireless networks including multi-access, interference and relay networks. This approach also allows the incorporation of public and common message flows for users in the system as well.

References:

[1] A. S. Avestimehr, S. N. Diggavi, and D. N. C. Tse, "Wireless network information flow: A deterministic approach," IEEE Trans. Inf. Theory, vol. 57, no. 4, pp. 1872–1905, Apr. 2011.

[2] M. Anand and P. R. Kumar, "A digital interface for Gaussian relay and interference networks: Lifting codes from the discrete superposition model," IEEE Trans. Inf. Theory, vol. 57, no. 5, pp. 2548–2564, May 2011.

[3] S. Kannan, A. Raja, and P. Viswanath, "Approximately optimal broadcasting in wireless networks," presented at the IEEE Int. Conf. Signal Process. Commun., Bangalore, India, Jul. 2010.

[4] S. Kannan, A. Raja, and P. Viswanath, "Approximately optimal broadcasting-cum-multicasting in wireless networks," presented at the IEEE Int. Symp. Inf. Theory, St. Petersburg, Russia, Aug. 2011.

[5] D. Vasudevan and S. B. Korada, "Polymatroidal flows on two classes of information networks," IEEE Trans. Inf. Theory, vol. 57, no. 1, pp. 227–233, Jan. 2011.

[6] K. Borders, and A. Prakash, "Web tap: Detecting covert web traffic," Proceedings of the 11th ACM Conference on Computer and Communications Security (CCS), pp. 110-120, Oct. 2004.

[7] A. Boukerche, K. E. Khatib, L. Xu, and L. Korba, "A novel solution for achieving anonymity in wireless ad hoc networks," Proceedings of the 1 st ACM International Workshop on Performance Evaluation of Wireless Ad Hoc, Sensor, and Ubiquitous Networks, pp. 30-38, Oct. 2004.

[8] A. Boukerche, K. E. Khatib, L. Xu, and L. Korba, "Performance evaluation of an anonymity-providing protocol for wireless ad hoc networks," Elsevier Performance Evaluation, vol. 63, no. 11, pp. 1094-1109, Nov. 2006.

[9] M. Burnside, and A. D. Keromytis, "Low latency anonymity with mix rings," Proceedings of the 9 th Information Security Conference (ISC), pp. 32-45, Aug./Sep. 2006.

[10] R. Canetti, and A. Herzberg, "Maintaining security in the presence of transient faults," Proceedings of Crypto '94, pp. 425-438, 1994.

[11] R. Canetti, and H. Krawczyk, "Analysis of keyexchange protocols and their use for building secure channels," Proceedings of Eurocrypt '01, pp. 453-474, 2001.

[12] R. Canetti, and H. Krawczyk, "Universally composable key exchange and secure channels," Proceedings of Eurocrypt '02, pp. 337-351, 2002.

[13] D. Chaum, "Untraceable electronic mail, return addresses, and digital pseudonyms," Communications of the ACM (CACM), vol. 24, pp. 84-88, Feb. 1981.

[14] D. Chaum, "The dining cryptographers problem: Unconditional sender and recipient untraceability," Journal of Cryptology, vol. 1, no. 1, pp. 65-75, 1988.

[15] L. Cottrell, The Anonymizer. (http://www.anonymizer.com/)