International Journal of Modern Engineering Research (IJMER)
www.ijmer.com Vol. 3, Issue. 5, Sep - Oct. 2013 pp-3293-3295 ISSN: 2249-6645

An Eavesdropping Model for Securing Communications over Wireless Broadcast Networks

G. Vidya Sagar[1], Syed Gulam Gouse[2]
[1]M.Tech, Nimra College of Engineering & Technology, Vijayawada, A.P, India.
[2]Professor, Dept.of CSE, Nimra College of Engineering & Technology, Vijayawada, A.P., India.

ABSTRACT: *Wireless broadcast networks constitute one class of basic and important wireless networks, in which a source node simultaneously transmits a number of information messages to different destinations. However, broadcast communications make use of the open nature of the wireless medium, which presents a great challenge to achieve the secure communication for individual users. This is because information for all users is contained in one transmitted signal, and hence information destined for one user may be obtained by non- intended users unless special coding is used. In this paper, we study a broadcast network, in which a source node transmits confidential message flows to the user nodes, and each message flow is intended to be decoded accurately by one node while being kept secret from all other nodes. Nodes are thus considered to be eavesdroppers with regard to all other messages but their own. Here we consider two eavesdropping models. The first model is referred to as a collaborative eavesdropping model, in which the eavesdroppers can exchange their outputs to interpret the message. The second model is referred to as a non- collaborative eavesdropping model, in which eavesdroppers do not exchange their outputs.*

Keywords: *Broadcasting, Eavesdropping, Wireless network.*

I. INTRODUCTION

Network-wide broadcasting is a fundamental operation in wireless networks. The goal of broadcasting is to transmit a message from a source to all the other nodes in the network. Several network protocols rely on broadcasting, for example, information dissemination, service/resource discovery, or routing in multihop wireless networks. Given that key applications of multihop wireless networks include disaster relief and rescue operations, military communication, and prompt object detection using sensors, the design of low-latency broadcasting scheme is essential to meeting stringent end-to-end delay requirements for higher-level applications. Interference is a fundamental limiting factor in wireless networks. When two or more nodes transmit a message to a common neighbor at the same time, the common node will not receive any of these messages. In such a case, we say that collision has occurred at the common node. Any communication protocol for wireless networks should contend with the issue of interference in the wireless medium.

One of the earliest broadcast mechanisms proposed in the literature is flooding [1] [2], where every node in the network transmits a message to its neighbors after receiving it. Although flooding is extremely simple and easy to implement,

Ni et al. [3] show that flooding can be very costly and can lead to serious redundancy, bandwidth contention, and collision: a situation known as broadcast storm. Since then, a large amount of research has been directed towards designing broadcast protocols which are collision-free and which reduce redundancy by reducing the number of transmissions.

II. RELATED WORK

Wireless broadcast networks constitute one class of basic and important wireless networks, in which a source node simultaneously transmits a number of information communications make use of the open nature of the wireless medium, which presents a great challenge to achieve secure communication for individual users. This is because information for all users is contained in one transmitted signal, and hence information destined for one user may be obtained by no intended users unless special coding is used. Physical layer security, which uses randomness of a physical communication channel to provide security for messages transmitted through the channel, opens a promising new direction toward solving wireless networking security problems. This approach was pioneered by Wyner in [4] and by Csiszár and Körner in [5], and more recently has been extensively explored in the literature[6].

Physical layer security adopts a precise quantitative measure of security level, i.e., the equivocation rate defined by Shannon [7], which equals the entropy rate of the source message conditioned on the channel output at the eavesdropper. This measure of the secrecy level allows security to be considered under the general Shannon framework of information theory [8], and hence provides an analytical basis with which to characterize the fundamental limits on communication rates given the security level constraints. This measure of security level also makes a unified security design across networking layers possible. The goal of such a design is to maximize network utility (i.e., to maximize overall users' satisfaction of the service rate in a certain fair manner among users) under security, reliability, and stability constraints. This motivates a joint design of rate control at the transport layer, rate scheduling at the medium access control layer, and power control and secure coding at the physical layer.

To achieve reliable and secure communication for users, we adopt the physical layer security approach [4], [5] to employ a stochastic encoder at the source node. The source node allocates its power not only among message flows (i.e., among users) but also dynamically according to the channel state information to improve secrecy communication rates. Hence the source power control operates over the symbol time scale, and determines the service rate allocation among users

at the packet time level. At the packet time level, to maintain the stability of all queues, the source node implements a rate schedule scheme that adapts its service rate allocation dynamically among users based on the queue lengths. Furthermore, rate control is performed also at the packet time level to maximize the network utility function. Our goal is to study how to jointly design rate control and rate scheduling at the packet time scale and power control and secure coding at the symbol time scale to achieve network utility maximization under reliability, security and stability constraints.

III. COLLABORATIVE EAVESDROPPING MODEL

For the collaborative eaves dropping model, we first obtain the secrecy capacity region, within which each rate vector can be achieved by a time-division scheme, i.e., at each channel state, the source transmits only to the user whose channel gain is better than the sum of the channel gains of all other users. It is clear that this user must have the best channel gain at this state. The power control among the channel states thus determines the rate allocation among users, i.e., rate allocation among components of a rate vector. We further show that all arrival rate vectors contained in this region can be stabilized by a throughput optimal queue-length-based scheduling scheme at the packet time level, where queue length determines the service rate allocation among users, and hence determines the corresponding power control to achieve this service rate vector at the symbol time level [9]. Finally, we obtain a distributed rate control policy that Maximizes the overall network utility maximization given that reliability, secrecy, and stability are achieved. This maximization is achieved by joint design of rate control, rate scheduling, power control, and secure coding.

For a given channel state h=(h1,h2,……hk), let p(h) denote the source power allocation for state h. We use p to denote the set that includes all power allocation functions (i.e., power control policies) that satisfy the power constraints, i.e.,

$$\mathcal{P} = \{p(\underline{h}) : E[p(\underline{h})] \leq P\}.$$

Now let Ai be the set of all channel states for which the channel gain of user is larger than the sum of the channel gains of all other users, i.e.,

$$\mathcal{A}_i = \left\{ \underline{h} : |h_i|^2 \geq \sum_{j \neq i, 1 \leq j \leq K} |h_j|^2 \right\}$$

For the collaborative eavesdropping model, the secrecy capacity region of the fading broadcast network is given by

$$\mathcal{C}_s = \bigcup_{p(\underline{h}) \in \mathcal{P}} \left\{ \begin{array}{l} (R_1, \ldots, R_K) : \\ R_i \leq E_{\underline{h} \in \mathcal{A}_i} \left[\log(1 + p(\underline{h})|h_i|^2) \right. \\ \qquad \left. - \log\left(1 + p(\underline{h}) \sum_{j \neq i, 1 \leq j \leq K} |h_j|^2\right) \right] \\ \text{for } 1 \leq i \leq K \end{array} \right\}$$

The secrecy capacity region given in above includes all achievable secrecy rate vectors with each component representing the service rate for one user. It still remains to determine a rate scheduling algorithm to choose a service rate vector at each packet time slot to stabilize all queues and correspondingly to determine a power control policy over the symbol time slots to achieve this service rate vector.

IV. NON- COLLABORATIVE EAVESDROPPING MODEL

For the non collaborative eavesdropping model, we study a time-division scheme, in which the source transmits to one user in each channel state. The secrecy rate region based on this scheme is derived. Although the time-division scheme is suboptimal, it is simple and important from a practical point of view. We also provide and discuss improved secure coding schemes based on non-time-division schemes. Based on a simple achievable secrecy rate region, a queue-length-based rate scheduling algorithm is derived that stabilizes the arrival rate vectors contained in this rate region.
For a given channel allocation scheme A(h), we consider the set of states for transmitting to user , i.e.,

$$\{\underline{h} : A(\underline{h}) = i\}.$$

The channel states in this set may not necessarily satisfy the condition that user i has the best channel state among all users.
The channel corresponding to these states can be viewed as parallel channels to every user with each subchannel corresponding to one state realization h.

Applying this scheme, an achievable rate for user can be obtained and is given by

$$R_i = \min_{j \neq i} E_{\underline{h}:A(\underline{h})=i} \left[\log\left(1 + p(\underline{h})|h_i|^2\right) - \log\left(1 + p(\underline{h})|h_j|^2\right) \right]^+$$

we can obtain the achievable secrecy rates for other users, and hence these rates constitute a rate vector achieved for a given power control scheme and a channel allocation scheme p(h) . An achievable secrecy rate region for the broadcast channel includes achievable secrecy rates obtained for any power control scheme and any possible state allocation scheme A(h).

For the noncollaborative eavesdropping model, an achievable secrecy rate region for the fading broadcast channel is given by

$$\mathcal{R}_s = \bigcup_{p(\underline{h})\in\mathcal{P}, A(\underline{h})\in\mathcal{A}} \left\{ \begin{array}{l} (R_1, \ldots, R_K): \\ R_i = \min_{j\neq i} E_{\underline{h}:D(\underline{h})=i} \left[\log\left(1 + p(\underline{h})|h_i|^2\right) - \log\left(1 + p(\underline{h})|h_j|^2\right) \right]^+ \\ \text{for } 1 \leq i \leq K \end{array} \right\}$$

where the random vector h=(h1,h2,….hk) has the same distribution as the marginal distribution of the random process {hn} at one symbol time instant.

V. CONCLUSION

Wireless telecommunications is the transfer of information between two or more points that are not physically connected. Distances can be short, such as a few meters for television remote control, or as far as thousands or even millions of kilometers for deep-space radio communications. For a collaborative eavesdropping model, in which the eavesdroppers exchange their outputs, the secrecy capacity region is obtained, within which each rate vector is achieved by using a time-division scheme and a source power control policy over channel states. A throughput optimal queue-length-based rate scheduling algorithm is further derived that stabilizes all arrival rate vectors contained in the secrecy capacity region. For a non collaborative eavesdropping model, in which eavesdroppers do not exchange their outputs, an achievable secrecy rate region is derived based on a time-division scheme, and the queue-length-based rate scheduling algorithm and the corresponding power control policy are obtained that stabilize all arrival rate vectors in this region.

REFERENCES

[1] C. Ho, K. Obraczka, G. Tsudik, and K. Viswanath, “Flooding for reliable multicast in multi-hop ad hoc networks,” in Proc. of the Int. Work. On Disc. Alg. and Meth. for Mobile Comp. and Comm., 1999, pp. 64–71.
[2] J. Jetcheva, Y. Hu, D. Maltz, and D. Johnson, “A simple protocol for multicast and broadcast in mobile ad hoc networks,” July 2001.
[3] S.-Y. Ni, Y.-C. Tseng, Y.-S. Chen, and J.-P. Sheu, “The broadcast storm problem in a mobile ad hoc network,” in Proc. of the 5th Ann. ACM/IEEE Int. Conf. on Mobile Comp. and Net., 1999, pp. 151–162.
[4] M. Neely, E. Modiano, and C. Li, “Fairness and optimal stochastic control for heterogeneous networks,” in Proc. IEEE INFOCOM, Miami, FL, Mar. 2005, vol. 3, pp. 1723–1734.
[5] A. Stolyar, “Maximizing queueing network utility subject to stability: Greedy primal-dual algorithm,” Queueing Syst., vol. 50, no. 4, pp. 401–457, Aug. 2005.
[6] A. Eryilmaz and R. Srikant, “Joint congestion control, routing and MAC for stability and fairness in wireless networks,” IEEE J. Sel. Areas Commun., vol. 24, no. 8, pp. 1514–1524, Aug. 2006.
[7] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, “Wireless information-theoretic security,” IEEE Trans. Inf. Theory, vol. 54, no. 6, pp. 2515–2534, Jun. 2008.
[8] E. Ekrem and S. Ulukus, “Degraded compound multi-receiver wiretap channels,” IEEE Trans. Inf. Theory, 2009, submitted for publication.
[9] P. Gopala, L. Lai, and H. E. Gamal, “On the secrecy capacity of fading channels,” IEEE Trans. Inf. Theory, vol. 54, no. 10, pp. 4687–4698, Oct. 2008.