IJCTA, 10(02), 2017, pp. 45-48

Defective and Impeccable Mystery InCmac With Confidential Message

Bharathi. S* and G. Premnath*

Abstract : In this paper, we study about the secret communication between the communication channels with compound multiple access channel(CMAC).In this channel the messages sent by one channel can be decoded by its corresponding receiver and kept secret from other receiver.A multiple access channel is considered and in which the messages from the encoders is confidential. Confidential messages are to be transmitted with perfect secrecy, as measured by equivocation at the other encoder. the upper bounds and the achievable rate for this communication situation are analyzed.

Keywords : Wiretap channel, rate-equivocation, CMAC.

1. INTRODUCTION

The wire-tap channel was first introduced by Wyner in 1975. His model consisted of a transmitter, a receiver and an eavesdropper. In the Wyner model, the eavesdropper channel was degraded version of the legitimate receiver channel. We consider a two-user discrete multiple-access channel in which one user wishes to communicate confidential messages to a common receiver while the other user in permitted to eavesdrop. This approach was introduced by Wyner for the wiretap channel, a scenario in which a single source-destination communication is eavesdropped. Under the assumption that the channel to the wire-tapper is a degraded version of that to the receiver, Wyner determined the capacity secrecy tradeoff. In addition, for the Gaussian case, we show that using cooperative jamming strategy can increase the achievable secrecy rate between the legitimate transmitter and the receiver.

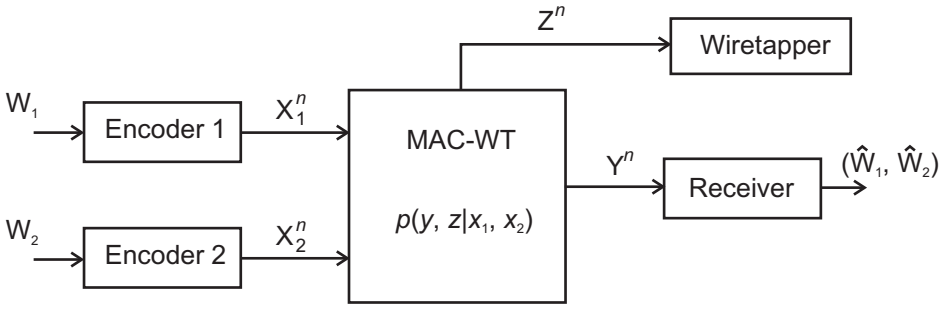

Figure 1

In fact, in terms of information the users can be divided into legitimate and illegal users. Legitimate users are allowed to decoded all the transmitted information (including common private messages of all the transmitters), while illegal users are allowed to decode only the messages of their intended transmitters.

* Department of computer science and engineering Vel tech Multi tech Dr.Rangarajan Dr.sakunthala Engineering College, Avadi, Chennai-62. *shabaru94@gmail.com, gpremnath@veltechmultitech.org*

2. PROPOSED SYSTEM

In this cooperative jamming (CJ) strategy, one of the transmitters that has a stronger channel to the eavesdropper than the legal user can send Gaussian noise signals that may result in a net gain for the legitimate user. Consider a scenario (*e.g*. Base stations) are allowed to decode all the transmitted information, while illegal users (eavesdroppers) are allowed to decode only the messages of their respective transmitters. We study the problem of secret communication over the compound MAC, that up to our best knowledge it has not been studied before. We investigate compound MAC with a confidential message (CMAC-CM) for both imperfect and perfect secrecy conditions at the eavesdropper (receiver-2). We show that if one of the receivers has access to the extremely noisy channel, secrecy condition can help increase the rate region. Also, we show that the use of cooperative jamming strategy can increase the achievable secrecy rate at the legitimate receiver.

3. SYSTEM MODEL

Consider a discrete memoryless CMAC-CM with four terminals as shown in Fig. 1. The finite sets X1, X2, Y1, Y2 and the transition probability distribution $p(y1; y2jx1; x2)$ are the constitutive components of this channel. Here, X1 and X2 are the channel inputs from the transmitters. Also Y1 and Y2 are the channel outputs at the receiver 1 and receiver 2, respectively. Throughout this paper, the random variables are denoted by capital letters *e.g*., X, Y, and their realizations by lower case letters *e.g*., *x, y*. The set of strongly jointly typical sequences of length *n*, on joint distribution $p(x:y)$ is denoted by An" (PX;Y). We use X*ni* , to indicate vector (X*i*;1;X*i*;2; : : : ;X*i*;*n*), and X*ki*;*j* to indicate vector (X*i*;*j* ;X*i*;*j* + 1; : : : ;X*i*;*k*). Before discussing the achievability rate, we first define a code for the channel.

4. THE GENERAL GAUSSIAN MULTIPLE-ACCESS WIRE-TAP CHANNEL

This is a scenario where the users communicate with a common base station in the presence of an eavesdropper, where both channels are modeled as Guassian multiple-access channels as shown in Figure 2.

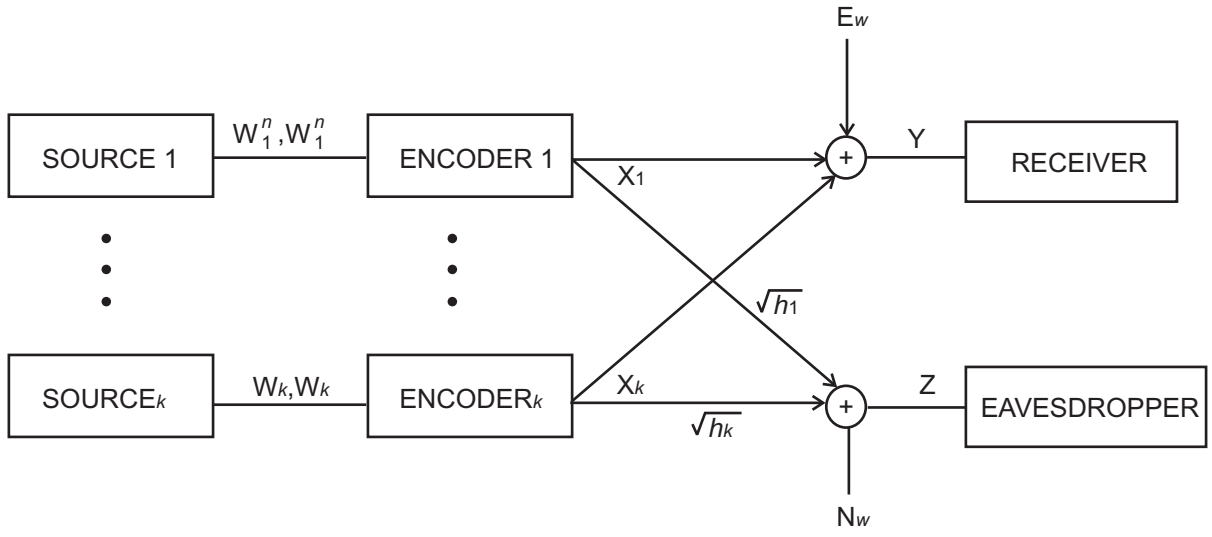

Figure 2

We would like to communicate with the receiver with arbitrarily low probability of error, while keeping the wire-tapper (eavesdropper) ignorant of the secret messages.

5. THE GAUSSIAN TWO-WAY WIRE-TAP CHANNEL

In this scenario, two transmitter/receiver pairs communicate with each other over a common channel. Communicate the open and secret messages with arbitrarily low probability of error, while maintaining secrecy of the secret messages.

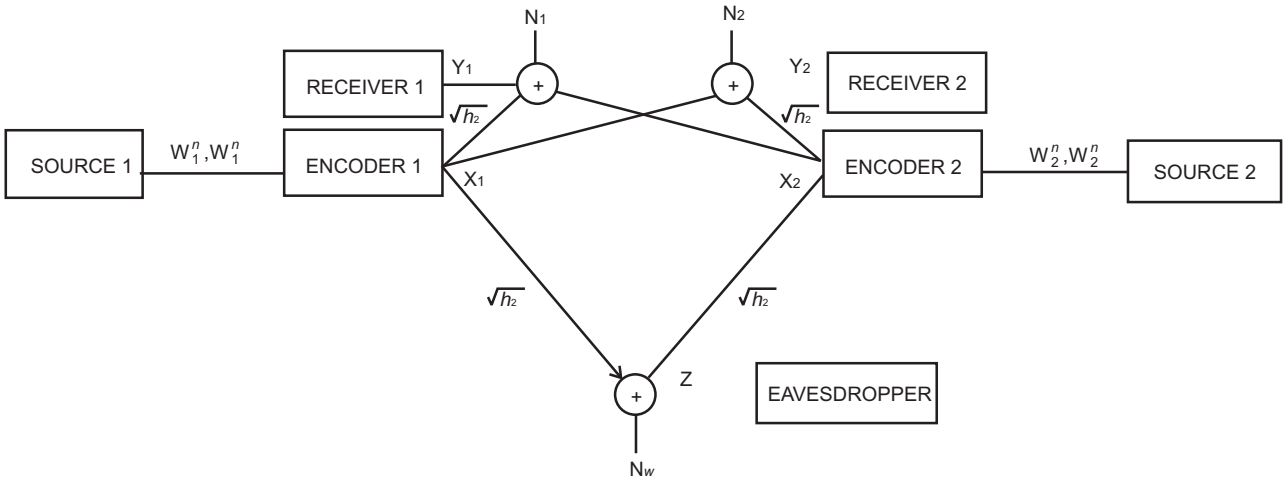

Figure 3

This gives the first set of terms in the achievable region. The key here is that since each transmitter knows its own code word, it can subtract its self-interference from the received signal and get a clear channel. Therefore, the Gaussian two-way channel decomposes into two parallel channels.

6. COMPOUND MULTIPLE ACCESS CHANNEL AND WIRE-TAP CHANNEL

In this channel, we assume that one of the transmitted messages is confidential that is only decoded by its corresponding receiver and kept secret from other receivers. Wire-tap channels evaluation is of the rate-equivocation region is simpler. We show that if the wiretap channel is more capable, is optimal and the boundary of the rate-equivocation region is achieved by varying rate splitting alone. Conversely, we show under a mild condition that if the wiretap channel is not more capable, then is strictly suboptimal. Next, we focus on the class of cyclic shift symmetric wiretap channels. We provide a special class of cyclic shift symmetric wiretap channels for which is optimal. We apply our results to the binary-input cyclic shift symmetric wiretap channels and thoroughly characterize the rate-equivocation regions of the BSC-BEC and BEC-BSC wiretap channels.

7. CONCLUSION

We proposed ascheme termed cooperative jamming, where a disadvantaged user may help improve the secrecy rate jamming the eavesdropper. We found the optimum power allocations for the transmitting and jamming users, and showed that significant rate gains may be achieved, especially when the eavesdropper has much has much higher SNR than the receivers and normal secret communications is not possible. The gains can be significant for both the GGMAC-WT and gtw-wt. This cooperative behavior is useful when the maximum secrecy sum-rate is of interest. We have also contrasted the secrecy rates of the two channels we considered, nothing the benefit of the two-way channels where the fact that each receiver has perfect knowledge of its transmitted signal brings an advantage with each user effectively encrypting the communications of other user.

Finally, we note that the results provided are of mainly theoretical interest, since as of yet there are no currently known practical codes for multiple-access wire-tap channel. Furthermore, accurate estimates of the eavesdropper channel parameters are required for code design for wire-tap channels where the channel model is quasi-static, as in our models considered in this paper.

8. FUTURE WORK

Investigating this possibility and determining the MACC capacity are the subjects of our future work. Moreover, the formulation of this problem of this problem in which the objective is to maximize rate under the secrecy constraint follows the definition of Wyner. However, difficult objectives can be envisioned in which user is more interested in eavesdropping than in maximizing its rate. It would be interesting to compare the conclusions that follow from the two problem formulations.

9. REFERENCES

1. A.D. Wyner, “The wire-tap channel” Bell System Technical journal, vol 57, no.8,oct 1975
2. M.Wiese and H. Boche, “An a achievable region for the wiretap multiple access channel with common message,” in Proc.IEEE Int.Symp. On Info. Theory (ISIT), Cambridge,MA,july 2012,pp.249-253
3. E. Tekin, S.S. erbetli, and A.Yener, “on secure signaling for the Guassian multiple access wire-tap channel,” in proc. Asilomar conf.sig., Syst., Comp., Asilomar, CA, oct 28- nov 1 2005
4. A. Thamgaraj, S.Dihidar, A.R. Calderbank, S.McLaughlin and J-M. Mero;;a. “Application of LDPC codes to the wiretap channel,” IEETrans,Inform. Theory, vol.53, no.8, pp. 2933-2945, Aug 2007.
5. Y. Liang and V. Poor, “Secure communication over fading channels,”in*Proc.Allerton Conf. Commun., Contr., Comput.*, Monticello, IL, Sep27-29 2006.
6. L. Zang, R. Yates, and W. Trappe, “Secrecy capacity of independent parallel channels,” in *Proc. Allerton Conf. Commun., Contr., Comput.*,Monticello, IL, Sep 27-29 2006.
7. U. Maurer and S. Wolf, “Secret-key agreement over unauthenticated public channels - part I: Definitions and a completeness result,” *IEEETrans. Inform. Theory*, vol. 49, no. 4, pp. 822–831, Apr 2003.
8. A.El Gamal and Y. H-Kim, Network information Theory, !st ed.cambridge, U.K: cambridege university prss,2012.
9. “The common randomness capacity of a network of discrete memoryless channels,” *IEEE Trans. Inform. Theory*, vol. 46, no. 2, pp.367–387, Mar 2000.
10. U. M. Maurer and S. Wolf, “Information-theoretic key agreement: From weak to strong secrecy for free,” in *Proc. EUROCRYPT*, 2000, pp. 351–368.
11. J. Barros and M. R. D. Rodrigues, “Secrecy capacity of wirelesschannels,” in *Proc. IEEE Int. Symp. Inform. Theory (ISIT)*, Seattle, WA,Jul 9-14 2015.
12. M. Salehi, Cardinality bounds on auxiliary variables in multiple user theory via the method of Ahlswede and Körner Stanford Univ... Stanford,CA, Aug. 1978, Tech. Rep. 33.
13. M. van Berg, O. Cheong, M. van Kreveld, and M. Overmars, *Computational Geometry: Algorithms and Applications*. NewYork:Springer-Verlag,2008.
14. B. Xie and R. Wesel, “A mutual information invariance approach to symmetry in discrete memoryless channels,”in*Proc. Inf.TheoryAppl.Workshop*,Feb.2008,pp.444–448.
15. O. Ozel and S. Ulukus, “Wiretap channels: Roles of rate splitting and channel prefixing,” in *IEEE Int. Symp. Inf. Theory*, Jul. 2011, pp. 628–632.