Network Coding for Physical Layer Secrecy

Shahriar Etemadi Tajbakhsh, Justin P. Coon *Senior Member, IEEE*, and Gaojie Chen *Member, IEEE*

***Abstract*—Physical layer secrecy is highly costly in terms of achievable data rates if perfect secrecy is considered. However, in many practical systems this level of secrecy is not required. In this paper, we introduce a secrecy system based on network coding and physical layer secrecy which is throughput efficient while maintaining a practical level of secrecy. In this system, a set of linear combinations of the original messages are protected with a physical-layer secrecy scheme and another set of linear combinations are freely transmitted over the wireless broadcast channel. This will allow the designer to tune the system for a desired level of secrecy and throughput. We discuss three variants of this coding scheme; The first two use random linear network codes (RLNC) and hence, highly efficient in terms of throughput. The third variant is based on instantly decodable network codes (IDNC) and designed for delay sensitive applications.**

I. Introduction

A large fraction of the information transmitted over communication networks has a confidential nature and should be protected against unauthorised access by eavesdroppers. Hence, secrecy has been in the center of attention of the communications researchers for several decades. Wyner in his seminal work [1] shows that it is possible to exploit the noise in the channel between the transmitter and eavesdropper to hide secret information from the eavesdropper. More precisely, suppose the capacities of the channels between the transmitter and the legitimate receiver and also between the transmitter and eavesdropper are C_b and C_e, respectively. It is shown in [1] that for memoryless channels it is possible to securely transmit at the rate $C_s = C_b - C_e$, if the legitimate receiver enjoys a better channel than the eavesdropper. This is the basis for physical layer secrecy[1] which has been widely studied particularly for wireless communications [2].

The study of wiretap channels has been extended to networked communication systems [3–6] in the context of network coding. Suppose we have an acyclic multicast network with a source and a set of receiver nodes where each channel between any two nodes has a capacity of 1 unit. Moreover, assume that the maximum possible transmission rate between the source and these destinations is h (which is specified by the size of min-cut between the source and the set of receiver nodes). In [3] it is shown that if k edges in such a network are wiretapped by the eavesdroppers, it is possible to securely transmit $h - k$ units of information.

In the previously mentioned scenarios, perfect secrecy is the requirement, i.e. no information about the intended messages should leak to the eavesdropper. A looser but highly practical secrecy condition, i.e. weakly security, is introduced in [4] where the eavesdropper is not able to obtain any *meaningful* information about the 'individual messages' of the source (but possibly some information about their joint distribution). With this level of secrecy requirement, [4] shows that unlike [3], without any sacrifice of network throughput, one can weakly securely transmit from the source to the receivers as long as the number of wiretapped links is less than h. As an example, suppose that an eavesdropper has wiretapped an XOR combination of two messages x_1 and x_2, i.e. $x_1 \oplus x_2$. Although some information about the collection of the two messages has been leaked, the eavesdropper will not obtain any information about the individual messages x_1 and x_2 (see e.g. [7] for storage and [8] in cooperative wireless networks, where weakly security has been adopted as the secrecy condition).

A more general definition of secrecy is established by Harada and Yamamoto [9], where a transmission is called *strongly* r-secure if the eavesdropper cannot obtain any information about any subset of $s \leqslant r$ messages if $h - r$ links are wiretapped by the eavesdropper. Therefore, weakly security is a special case of r-security where $r = 1$. Parameter r can be used to define the level of secrecy ranging from weakly security to perfect secrecy. Random linear network coding [9] is shown to be strongly secure if the operating field size is sufficiently large.

In this paper, we introduce a general coding scheme for weakly secure and r-secure network coded transmissions over a broadcast wireless channel. The introduced system basically protects a fraction of the linear combinations of the source messages by an extra layer of physical layer perfect secrecy scheme and the rest of combinations are transmitted freely. The fundamental advantage of the proposed scheme is its efficiency in terms of data rate while maintaining secrecy at the level that is desirable for many wireless applications. The proposed system also allows the designer to tune the system for a desired level of secrecy by changing the value of r.

II. System Model

We assume a transmitter is willing to deliver a vector of N messages $\mathbf{X} = [x_1 \dots x_N]$ (vectors represented in bold fonts) to a group of K legitimate wireless receivers over a symbol erasure broadcast channel (SEC) in the presence of a group of M eavesdroppers. Each message $x_i \in \mathbb{F}_q$ is an element from a finite Galois field of size q. The transmitter generates and broadcasts linear *combinations* of these messages over the same finite field (or larger field sizes) using the methods which will be described later. Each combination is received by the legitimate user i with probability p_i and with probability q_j by the eavesdropper j. We assume that the eavesdroppers are capable of exchanging the messages they have received with each other over an error free secure channel. The same

This work was supported by EPSRC grant number EP/N002350/1 ("Spatially Embedded Networks"). S. E. Tajbakhsh, J. P. Coon, and G. Chen are with the Department of Engineering Science, University of Oxford, Parks Road, Oxford, UK, OX1 3PJ, Emails: {shahriar.etemaditajbakhsh, justin.coon, and gaojie.chen}@eng.ox.ac.uk.

[1] In this paper, we use the terms secrecy and security interchangeably.

assumption applies to the legitimate receivers[2]. Given this assumption, the union of the eavesdroppers and the union of legitimate users successfully receive a linear combination with the probabilities $\beta = 1-\prod_{j=1}^{M}(1-q_j)$ and $\alpha = 1-\prod_{i=1}^{K}(1-p_i)$, respectively. It should be noted that we use this abstraction of wireless channel model for tractability of the analysis. However, the behavior of real wireless channels are far more complicated. There exist methods in the literature to derive the probability of block errors given the parameters of a fading channel [10].

The objective of the proposed system is to deliver the messages to the legitimate users while a certain level of secrecy is maintained with high probability. The level of secrecy is defined based on the amount of information made available to the eavesdroppers. We use the definition in [4] to specify the level of information leakage. Suppose U is a subset of the original messages set (denoted by X) and V is a subset of the transmitted combinations (encoded messages). Perfect secrecy means that if V is the set of received combinations at the eavesdropper and $U = X$, then $I(X;V) = 0$, i.e. the received combinations contain no information about the entire set of messages. Weakly security is a looser condition where the eavesdropper obtains no information about any of the individual messages, i.e $I(x_i;V) = 0,\ \forall i = 1,\ldots,N$. A more general definition of secrecy allows us to apply several levels of secrecy. A coding system is called strongly r-secure if $I(U;V) = 0,\ \forall U \subseteq X,\ |U| \leqslant r$.

III. Hybrid Secrecy Method

The underlying principle of the proposed system for holding a certain level of secrecy is to assure that a given number of linear combinations are missed by the union of the eavesdroppers with high probability. Therefore, a fraction of the random linear combinations of the source will go through an extra layer of coding to be prepared for a physical-layer based perfect secrecy scheme. The remaining combinations will be transmitted freely without any further coding. This coding system has been illustrated in Fig. 1.

The outer encoder, using the methods developed in [4, 5, 11] for coding at the source, generates N combinations of the messages such that no subset of these combinations with at least one missing combination is decodable for the eavesdropper. It should be noted that the methods in [5, 11] can operate in the same field size as the original messages whereas the method in [4] should be performed in a larger field size. In [9] it is shown that random linear networks can be also strongly secure if the field size is sufficiently large. Therefore, the outer encoder can be removed and a RLNC encoder operating in a larger field size (as the NC in Fig. 1) applied instead.

The NC encoder generates random linear combinations of its input elements (the N original messages or the N outputs of the outer encoder). The output of the RLNC encoder is split to two subsets of N_s' and N_w linear combinations. The first subset is given to an extra layer of physical-layer based perfect secrecy encoder (PLPS) where its output will be $N_s > N_s'$ encoded elements from the finite field. This output is transmitted over the channel. Such encoders typically use a channel coding method, e.g. LDPC or polar code to combine some random messages with the original messages, to prevent the eavesdropper (whose channel is not as good as the legitimate user) from decoding the messages even if the encoder is known to the eavesdropper [12]. The remaining N_w combinations will be directly transmitted to the receiver. At the receiver side the combinations received from the PLPS are decoded to obtain the N_s' linear combinations. Also a subset of the network coded combinations will be successfully received at the receiver. The collection of these two sets of combinations are decoded by the NC decoder (obviously N independent linear combinations should have been received). In the following, different variants of the proposed scheme are discussed.

A. Semi-Adaptive Approach

If an outer encoder (using one of the methods established in [4, 5, 11]) is considered, $\mathbf{Z}_{N\times 1}$ will be the output. Otherwise $\mathbf{Z} = \mathbf{X}$. The NC component in this method would be a RLNC encoder [13]. The RLNC component generates two sets of linear combinations. The first set includes $N_s' = r$ combinations which are sent to the PLPS encoder to be processed for physical layer secrecy using one of the methods described in [12]. The input to the PLPS encoder, $\mathbf{Y}^2_{N_s'\times 1} = \mathbf{A}^2_{N_s'\times N}\mathbf{Z}_{N\times 1}$, is mapped to $\mathbf{W}_{N_s\times 1}$ where $N_s > N_s'$ (the PLPS rate is discussed later in this section). The second set of combinations (denoted by $\mathbf{Y}^1_{N_w\times 1} = \mathbf{A}^1_{N_w\times N}\mathbf{Z}_{N\times 1}$) is transmitted over the channel without any further coding. $\mathbf{A}^1$ and $\mathbf{A}^2$ are the RLNC coefficient matrices. At the decoder side, once the PLPS unit decodes and obtains $\mathbf{Y}^2$, the RLNC encoder begins generating linear combinations and transmitting them over the channel until the receiver receives sufficient number of independent linear combinations to decode. In other words, the collection of $\mathbf{Y}^2$ combinations and the subset of $\mathbf{Y}^1$ which is successfully received at the receiver form a set of N independent linear combinations and hence decodable. Therefore, the value of N_w is adaptively decided based on an acknowledgement by the receiver.

The average number of required transmissions with this method is given by

$$N_T = \frac{N-r}{\alpha} + \frac{r}{\alpha-\beta} \tag{1}$$

where N_T is the average total number of transmissions. The first term relates to the direct transmissions by the RLNC encoder. The second term is the rate by the PLPS. This is because the capacity of secure transmission using physical layer secrecy is $\alpha-\beta$. This is followed from the Wyner capacity of memoryless wiretap channels [1] and that the capacities of the legitimate and eavesdropper SEC channels are α and β (symbols per channel use), respectively [14]. If $r = 1$, the system is weakly secure. Also, one can observe that for a fixed r, if $N \to \infty$, the system achieves the capacity of non-secure transmissions.

It should be noted that the achievable rate for the hybrid secrecy scheme, denoted by C_h, in its general form and for a fixed ratio $\rho = \frac{r}{N}$, is the weighted sum of the physical layer

[2]If the legitimate receivers are incapable of such collaboration, each user can be treated individually as an instance of the proposed scheme.

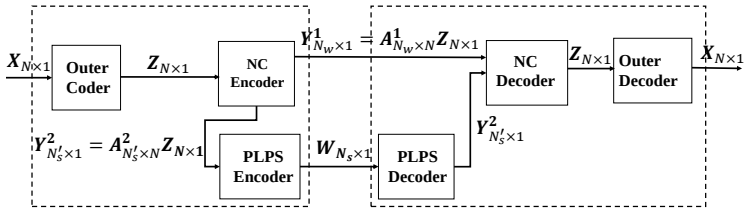

Fig. 1: Hybrid coding system.

secrecy transmissions and free transmissions achievable rates, which is as follows.

$$\begin{aligned} C_h &= \rho C_s + (1-\rho)C_e = \rho(C_b - C_e) + (1-\rho)C_b \\ &= C_b - \rho C_e \end{aligned} \tag{2}$$

Hence, the gain of the proposed scheme in terms of achievable rate is upper bounded by $G = \frac{C_b - \rho C_e}{C_b - C_e}$.

It should be noted that selecting the appropriate level of secrecy in a practical system, will be depending on the application, the computational resources of the eavesdropper, and the coding system and its operating field size. For instance, in [4], it is discussed that if the eavesdropper can *guess g* linear combinations of messages, then the system will be weakly secure if $g < h - k$. An incautiously low level of secrecy (e.g. $r \ll N$) might make the system vulnerable against brute-force or other computational attacks (because any independent linear combination of the messages reduces the linear span of solutions' space).

B. Adaptive Approach

The building blocks of this approach is identical to the semi-adaptive approach. If the difference between α and β is considerable, one can expect that with high probability, the legitimate receiver might receive N independent combinations and decode before the eavesdroppers receive $N - r$ combinations, if all the RLNC combinations are transmitted without PLPS coding. If we denote the random variables representing the number of received linear combinations by the legitimate user and the eavesdropper by N_L and N_E, we have

$$P(N_L \leqslant N-1) = \sum_{\ell=0}^{N-1} \binom{N_w}{\ell} \alpha^\ell (1-\alpha)^{N_w-\ell} = I_{1-\alpha}(N_w - N + 1, N)$$

and

$$P(N_E \leqslant N-r) = \sum_{\ell=0}^{N-r} \binom{N_w}{\ell} \beta^\ell (1-\beta)^{N_w-\ell} = I_{1-\beta}(N_w - N + r, N).$$

where $I_p(\cdot)$ is the regularised incomplete beta function (CDF of a binomial distribution with parameter p). It should be noted that we assumed the field size to be large such that every combination received by the receivers is independent of the others. Therefore, N_L and N_E follow binomial distributions.

The objective would be to check if there are any values of N_w such that $P(N_L \leqslant N-1) \leqslant \epsilon$ for N_w^0 and $P(N_E \leqslant N-r) \leqslant 1-\delta$ for N_w^0, denoted by N_w^0 and N_w^*, for arbitrarily small values of ϵ and δ. If N is large, central limit theorem (CLT) can be used to approximate the binomial distributions of N_L and N_E. Using central limit theorem we have

$$Z = \frac{N_E - N_w\beta}{\sqrt{N_w\beta(1-\beta)}} \to \mathcal{N}(0,1)$$

where $\mathcal{N}(0,1)$ is the standard normal distribution. We would like to find the value of z_0 for which $P(Z \leqslant z_0) = \delta$. Therefore, we have

$$z_0 = \sqrt{2}\,\mathrm{erf}^{-1}(2\delta - 1).$$

Solving the following equation gives the desired value of N_w.

$$\sqrt{2}\,\mathrm{erf}^{-1}(2\delta-1) = \frac{N_{E_0} - N_w\beta}{\sqrt{N_w\beta(1-\beta)}}$$

where $N_{E_0} = N - r$ for the eavesdropper. For the legitimate user, we replace N_{E_0} by $N_{L_0} = N - 1$, β with α and δ with ϵ. By solving the quadratic equation, we have:

$$N_w^* = \frac{1}{\alpha}\Big[N - r \pm A\sqrt{2(1-\alpha)\big(N - r + A^2(1-\alpha)\big)} + A^2(1-\alpha)\Big]$$

where $A = \mathrm{erf}^{-1}(2\delta - 1)$. The smaller value is selected in the case of N_w^* whereas the larger value is selected in the case of N_w^0.

Once for a given δ the value of N_w^* is derived, it can be used as a threshold for the transmissions by the RLNC unit. At the first phase the RLNC generates linear combinations of the original messages. If the legitimate receiver obtains N independent linear combinations before that the total of transmissions exceed N_w^*, with a probability larger than $1 - \delta$ the system will be r-secure. Otherwise, the RLNC transmissions are stopped as soon as the total number of transmissions reach to N_w^* and the remaining number of independent linear combinations required by the legitimate user are encoded by the PLPS unit and transmitted over the channel. It should be noted that this scheme is sensitive to the choice of δ. This dependency will be discussed in Section IV.

C. Instantly Decodable Approach

RLNC in general is throughput efficient. However, it imposes considerable delay to the system. This is because the receiver has to wait until it receives sufficient number of linear combinations to be able to decode and obtain the original messages. For delay sensitive applications, instantly decodable network coding (IDNC) is an efficient alternative. The simplest form of IDNC is described in the canonical example of network coded relaying in [15], where the two receivers Alice and Bob hold two messages x_1 and x_2, respectively. Therefore, the combination $x_1 \oplus x_2$ transmitted by the relay is instantly decodable for both of them. We incorporate the same principle into the current scheme. The first message x_1 is encoded by the PLPS unit and transmitted over the channel. Therefore, the first message remains hidden from the eavesdroppers. Afterwards, at each transmission (say i-th round, $i = 1, \ldots, N-1$) the network coding unit generates the combination $x_i \oplus x_{i+1}$. If the combination is not received correctly by the legitimate receiver, it will be retransmitted until it is received (where

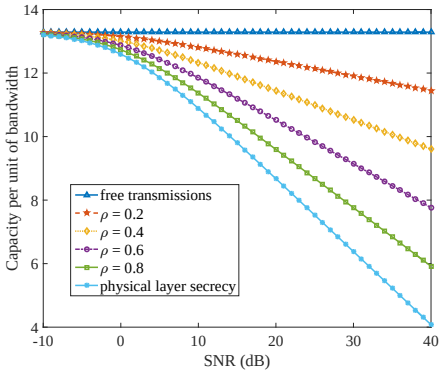

Fig. 2: Achievable rates for a given SNR at the legitimate receiver with respect to SNR at the eavesdropper for different values of ρ, compared to conventional physical layer perfect secrecy ($\rho = 1$), and free transmissions ($\rho = 0$).

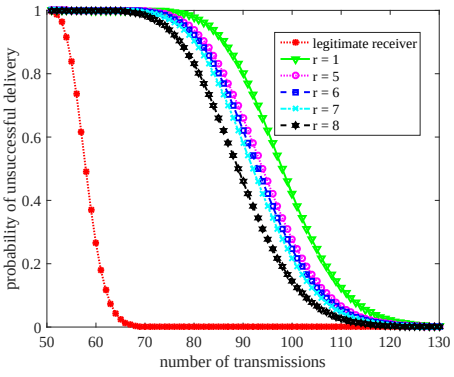

Fig. 3: Probability of unsuccessful reception at the legitimate receiver $P(N_L \leqslant N-1)$ and the eavesdropper $P(N_E \leqslant N-r)$.

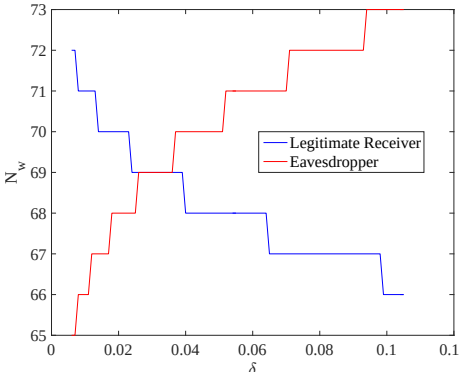

Fig. 4: Threshold values N_w^* and N_w^0 with respect to δ.

perfect feedback is available). The eavesdropper will not be able to decode and obtain any information about the individual messages. Therefore, the transmission is weakly secure.

IV. Numerical Experiments

The Shannon capacity of the proposed hybrid scheme for different values of $\rho = \frac{r}{N}$ has been compared with the conventional physical layer perfect secrecy systems ($\rho = 1$) and free transmissions ($\rho = 0$) in Fig. 2. We assumed a fixed Signal-to-Noise Ratio (SNR) of 40 dB for the legitimate receiver and represented the achievable data rates with respect to SNR at the eavesdropper, ranging from -10 dB to 40 dB. As it is expected, for larger values of the SNR, the gain of the proposed hybrid scheme over perfect secrecy is larger. Also for larger values of eavesdropper's SNR, the capacity grows almost linearly with respect to the SNR.

In another experiment, we have studied the adaptive approach. The probabilities of unsuccessful completion at the legitimate receiver and the eavesdropper after a certain number of combinations transmissions have been depicted for $N = 50$, $\alpha = 0.85$ and $\beta = 0.5$. More precisely the probabilities $P(N_E \leqslant N-1)$ for different values of r as well as $P(N_L \leqslant N-1)$ with respect to a range of values for N_w have been shown in Fig. 3. Roughly speaking, one can observe that even for $r = 7$, the probability of unsuccessful reception of N messages by the eavesdropper is close to 1 whereas the same probability is close to 0 for the legitimate eavesdropper. Therefore, with high probability, the system is r-secure for $r = 7$ without the extra coding by the PLPS.

For $\delta = \epsilon = 0.01$, the value of N_w^* has been compared with the average number of transmissions N_T required by the semi-adaptive method in table I. N_w^* can be considered as an upper bound for N_T in the semi-adaptive approach. Since $N_w^0 = 66$ for this setting, for $r = 7$ the adaptive method outperforms the semi-adaptive. Moreover, the sensitivity of the values of N_w^* and N_w^0 with respect to $\delta(= \epsilon)$ has been examined and depicted in Fig. 4.

V. Conclusion

We proposed a hybrid weakly secure method of transmission using linear network coding and physical layer secrecy. The key advantage of such a system is in throughput efficiency in comparison to strongly secure systems while a highly reliable (and tunable) level of secrecy is maintained. In future, it would be interesting to translate the parameters of the physical layer (e.g., transmission power, fading, path loss, stochastic geometry of the users and eavesdroppers) to probabilities of erasure and observe their impact on secrecy level.

Eve	r = 1	r =5	r = 6	r = 7	r = 8
N_T (semi-adaptive)	78	70	69	67	65
N_T (adaptive)	61	67	69	70	72

TABLE I: The total number of transmissions in the semi-adaptive and adaptive methods.

References

[1] A. D. Wyner, "The wire-tap channel," *Bell Labs Technical Journal*, vol. 54, no. 8, pp. 1355–1387, 1975.

[2] X. Zhou, L. Song, and Y. Zhang, *Physical layer security in wireless communications*. CRC Press, 2013.

[3] N. Cai and R. W. Yeung, "Secure network coding," in *IEEE International Symposium on Information Theory (ISIT)*, 2002.

[4] K. Bhattad and K. R. Narayanan, "Weakly secure network coding," in *Proc. First Workshop on Network Coding, Theory, and Applications (NetCod)*, Italy, April 2005.

[5] D. Silva and F. R. Kschischang, "Universal weakly secure network coding," in *IEEE Information Theory Workshop on Networking and Information Theory (ITW)*, 2009, pp. 281–285.

[6] S. E. Rouayheb, E. Soljanin, and A. Sprintson, "Secure network coding for wiretap networks of type ii," *IEEE Transactions on Information Theory*, vol. 58, no. 3, pp. 1361–1371, 2012.

[7] P. F. Oliveira, L. Lima, T. T. Vinhoza, J. Barros, and M. Médard, "Coding for trusted storage in untrusted networks," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 6, pp. 1890–1899, 2012.

[8] M. Yan and A. Sprintson, "Weakly secure network coding for wireless cooperative data exchange," in *Global Telecommunications Conference (GLOBECOM 2011), 2011 IEEE*. IEEE, 2011, pp. 1–5.

[9] K. Harada and H. Yamamoto, "Strongly secure linear network coding," *IEICE transactions on fundamentals of electronics, communications and computer sciences*, vol. 91, no. 10, pp. 2720–2728, 2008.

[10] M. Zorzi and R. R. Rao, "On the statistics of block errors in bursty channels," *IEEE transactions on communications*, vol. 45, no. 6, pp. 660–667, 1997.

[11] Y. Wei, Z. Yu, and Y. Guan, "Efficient weakly-secure network coding schemes against wiretapping attacks," in *Network Coding (NetCod), 2010 IEEE International Symposium on*. IEEE, 2010, pp. 1–6.

[12] M. Bloch, M. Hayashi, and A. Thangaraj, "Error-control coding for physical-layer secrecy," *Proceedings of the IEEE*, vol. 103, no. 10, pp. 1725–1746, 2015.

[13] T. Ho, M. Médard, R. Koetter, D. R. Karger, M. Effros, J. Shi, and B. Leong, "A random linear network coding approach to multicast," *IEEE Transactions on Information Theory*, vol. 52, no. 10, pp. 4413–4430, 2006.

[14] T. C. M and J. A. Thomas, *Elements of information theory*. John Wiley & Sons, 2012.

[15] S. Katti, H. Rahul, W. Hu, D. Katabi, M. Médard, and J. Crowcroft, "Xors in the air: Practical wireless network coding," in *ACM SIGCOMM computer communication review*, vol. 36, no. 4, 2006, pp. 243–254.