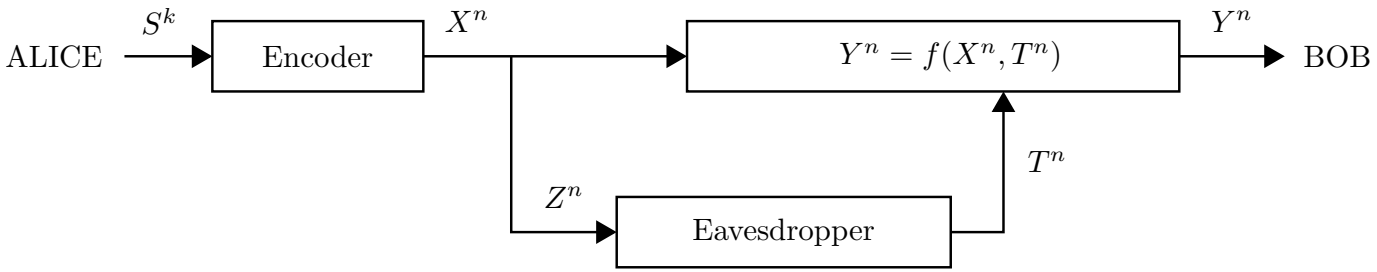
Type II Wiretap Channel with an Active Eavesdropper in Finite Blocklength Regime

Anna Frank, Harout Aydinian, and Holger Boche

Lehrstuhl für Theoretische Informationstechnik
Technische Universität München, Germany

IEEE Wireless Communications and Networking Conference
Doha, April 3, 2016

Motivation - The binary wiretap channel II with an active eavesdropper



Aggarwal et al (2009) considered the binary wiretap channel II in which the eavesdropper can modify the bits he observes (μ from n transmitted bits).

- In the first model, the eavesdropper erases the bits he observes.
- In the second model, the eavesdropper replaces the bits he observes.

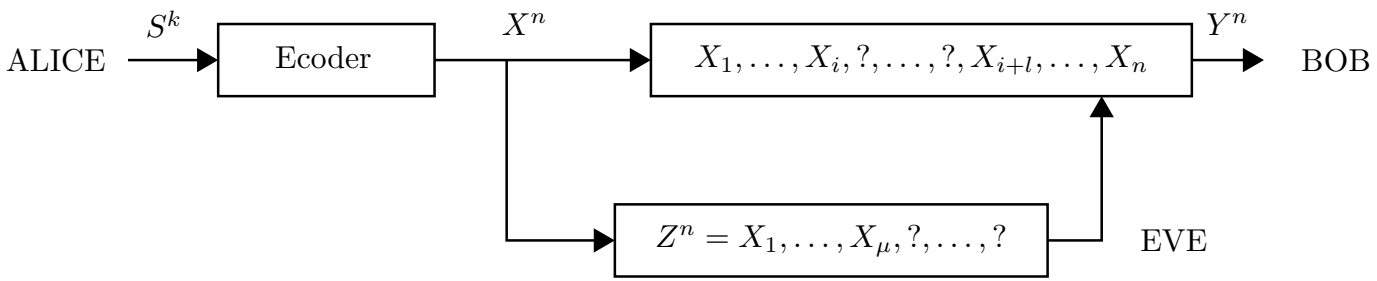
Achievable secrecy rates, where $\epsilon = \mu/n$

- for erasures: $R_s = (1 - \epsilon - h(\epsilon))^+$,
- for replacements: $R_s = (1 - \epsilon - h(2\epsilon))^+$.

A new model

The eavesdropper (Eve)

- can observe an interval of μ symbols from n transmitted symbols.
- can erase the symbols in any interval of length l



Remark

Eve is able to erase an arbitrary interval of positions of length l, unlike the model in Aggarwal et al (2009), where Eve can erase only the symbols she observes.

Our Objectives

Given parameters n, l, μ, and a finite field alphabet q.

Explicit construction of coding schemes that achieve

1. perfect reliability

$$H(S^k|Y^n) = 0,$$

2. perfect security

$$H(S^k|Z^n) = H(S^k),$$

3. maximum *secrecy rate* k/n.

Secure nested codes

- A nested linear code is a pair (C', C) of linear codes in $\mathbb{F}_q^n$ with $C \subset C'$.
- The mother (outer) code C' is partitioned into cosets of the coarse (inner) code C, thus the number of cosets $K = |C'|/|C|$.
- Each coset corresponds to a secret message $s^k \in \mathbb{F}_q^k$, $k = \log_q K$.

The encoding is stochastic and can be done in a linear fashion.

- The generator matrix G' of C' is given by

$$G' = \begin{bmatrix} G^* \\ G \end{bmatrix},$$

  where G^* and G are generator matrices for C^* and C respectively with $C^* \cap C = 0$.
- Let C' be an $[n, m]_q$ code.

Secure nested codes

- Encoding : $s^k \longmapsto x^n$

$$x^n = \begin{bmatrix} s^k & u^{m-k} \end{bmatrix} \begin{bmatrix} G^* \\ G \end{bmatrix},$$

where $u^{m-k} \in \mathbb{F}_q^{m-k}$ is chosen uniformly at random.

- The nested coding approach is a natural generalization of the Ozarow-Wyner's coset coding scheme.

In case of a noisy main channel:

- The mother code serves for the reliability and the coarse code is used for stochastic encoding to provide security.

- We call a nested code (C', C) secure if it satisfies the conditions $H(S^k|Y^n) = 0$ and $H(S^k|Z^n) = H(S^k)$.

Burst Erasure Correcting Codes

- Burst-erasure channels encompass many real-world communications systems including fading environments, packet based communications such as internet transmissions, and magnetic storage devices.

- A code capable of correcting all bursts (including wrap-arround bursts) of length l or less, is called *l-burst-erasure correcting code (cyclically l-burst-erasure correcting code)*.

Proposition

A linear $[n, k]_q$ code C is l-burst-erasure correcting iff every l consecutive columns of H_C are linearly independent. Correspondingly, C can correct l-burst-erasures, including wrap-around bursts, iff every l cyclically consecutive columns of H_C are linearly independent.

Burst Erasure Correcting Codes

Definition

(i) An $[n, k]_q$ code C, capable of correcting every burst of erasures of length $n - k$ is called an optimal burst-erasure correcting code.
(ii) If C can correct all burst erasures of length $n - k$, including cyclic (wrap-around) bursts, then C is called cyclically-optimal burst-erasure correcting, or c-optimal for short.

Proposition

If an $[n, k]_q$ code C is a c-optimal burst-erasure correcting code, then the dual code $C^{\perp}$ is a c-optimal burst-erasure correcting $[n, n - k]_q$ code.

Definition

An $m \times n$ $(m \leq n)$ matrix G over a given finite field is called good (cyclically good) if every m consecutive (cyclically consecutive) columns in it are linearly independent.

Upper bound for the secrecy rate

Theorem

In a WTC-II, with an active eavesdropper that can observe any interval of μ symbols, out of n transmitted symbols from $\mathbb{F}_q$, and erase any interval of l symbols, one can convey securely and with zero error decoding, at most $\hat{k}(n,l,\mu) = (n-l-\mu)^+$ symbols, that is the secrecy rate R_s is bounded by

$$R_s \leq (1 - l/n - \mu/n)^+.$$

Performance Criteria

Theorem

To achieve the positive secrecy rate $\hat{R}_s = (1 - l/n - \mu/n)^+$ *with a nested linear code* (C', C)*, the following three conditions are necessary and sufficient:*

(i) $n - l > \mu$

(ii) The mother code C' *is an* $[n, n-l]_q$ *optimal burst erasure (i.e.* l*-burst-erasure) correcting code.*

(iii) The coarse code $C \subset C'$ *is an* $[n, \mu]_q$ *code such that its dual code* $C^\perp$ *is an* $[n, n-\mu]_q$ *optimal burst erasure (i.e.* μ*-burst-erasure) correcting code.*

Main Result - Achievability

Denote $m = n - l$.

Theorem

(i) For arbitrary admissible parameters n, m, μ, that is for $1 \leq \mu < m \leq n$, and a finite field $\mathbb{F}_q$ with the non binary alphabet, there exist explicit constructions of secure nested codes (C', C), that achieve the maximum secrecy rate $\hat{R}_s$.

(ii) Such binary codes (C', C) exist for the following cases:
1) $1 \leq \mu < m \leq n/2$,
2) $n/2 \leq \mu < m < n$,
3) $1 \leq \mu < n/2 < m < n$,
where $n = 2lt$ if $\mu \leq l$, and $n = 2\mu t$ if $\mu > l$, with $t \in \mathbb{N}$.

Code Construction - Non binary finite field alphabet

Recursive construction:

Let G' be an $m \times n$ cyclically good matrix, which contains a $\mu \times n$ good submatrix G.

Claim: We can add a column $\mathbf{x}$ to G' s.t. $G'\mathbf{x}$ is a cyclically-good $m \times (n+1)$ matrix which contains a $\mu \times (n+1)$ good submatrix, i.e. $G'\mathbf{x}$ generates a secure nested code with maximum secrecy rate.

Starting with an cyclically good $m \times m$ matrix G' we fulfill the task for all parameters $1 \leq \mu < m < n$; $n = m+1, m+2, ...$

Conclusion - Open Problems

- Study other modification models of WTC-II with specified abilities of the eavesdropper.
- Better achievable secrecy rates for the model of Aggarwal et al.
- Developing practical codes for their model.

References

- V. Aggarwal, L. Lai, A. Calderbank, and H. Poor, "Wiretap channel type II with an active eavesdropper", IEEE Intern. Sympos. Inform. Theory, ISIT 2009(no. 3), pp. 1944–1948, 2009.
- L. H. Ozarow and A. D. Wyner, "Wire-tap channel II", B.S.T.J., vol. 63(no. 10), pp. 2135–2157, 1984.
- H. Hollmann and L. Tolhuizen, "Optimal codes for correcting a single (wrap-around) burst of erasures", IEEE Trans. on Info. Theory, vol. 54(no. 9), pp. 4361–4364, 2008.
- H. Boche and R. Schaefer, "Capacity results and super-activation for wiretap channels with active wiretappers", IEEE Trans. on Info. Theory, vol. 8(no. 2), pp. 1482–1496, 2013.
- L. Lai, H. El Gamal, and H. V. Poor, "Authentication over noisy channels", IEEE Trans. Info. Theory, vol. 55(no. 2), pp. 906–916, 2009.
- J. Nötzel, M. Wiese, and H. Boche, "The arbitrarily varying wiretap channel-Secret randomness, stability, and super-activation", Proc. Int. Symp. Inf. Theory (ISIT-2015), pp. 2151–2155, Hong-Kong, Jun. 2015.
- P. Wang and R. Safavi-Naini, "A model for adversarial wiretap channels", CoRR abs/1312.6457(2013).

Thank You!

Questions?

Remarks?