REVIEW PAPER

STUDY OF INDEX CODING PROBLEM AND ITS VARIANT

MAINLY PERFECLTY SECURE INDEX CODING, DYNAMIC INDEX CODING AND INDEX CODING WITH SIDE INFORMATION

SUBMITTED BY:

HARSHIT GUPTA

2017EET2303

SUBMITTED TO:

Dr. RANJAN BOSE

PROFESSOR (EE DEPARTMENT)

CODING THEORY (ELL710)

PAPERS REVIEWED:

1) M. M. Mojahedian, A. Gohari, and M. R. Aref. “Perfectly secure index coding,” in Proc. IEEE ISIT, 2015

2) M. Effros, S. E. Rouayheb, and M. Langberg. (2012). “An equivalence between network coding and index coding.” [Online]. Available: https://arxiv.org/abs/1211.6660

3) S. H. Dau, V. Skachek, Y. M. Chee, "Secure index coding with side information", arXiv:1011.5566.

Apart from these some other Reference are also used and mentioned in last page.

ABSTRACT:

The first paper explains the index coding problem in the presence of an eavesdropper. The researcher went on deriving four theorem in the elaboration of index coding.

The experiment is done first using perfectly secure index coding and the after relaxing this assumption and weak secrecy index coding and show the result difference between them. Primarily no changes were noted. Weak secrecy does not change the rate region when we have an epsilon-error decoding condition.

The paper attempts to establish a relation between secure index coding problems to one without secrecy. And derived a onetime pad strategy.

Second paper follow up the discussion on dynamic index coding. This paper is chosen to see the differences due to side information. This paper proposed different two max weight dynamic algorithms for dynamic index coding.

The third paper does the analysis with side information. Third paper largely discuss about ICSI (index coding with side information).the ICSI is performed on vector line index codes to better transmission rates.

INTRODUCTION:

Basic definitions:

1. **Index coding:**
   Index coding problem is one of the intensively used and most popular problem in wireless transmission coding.

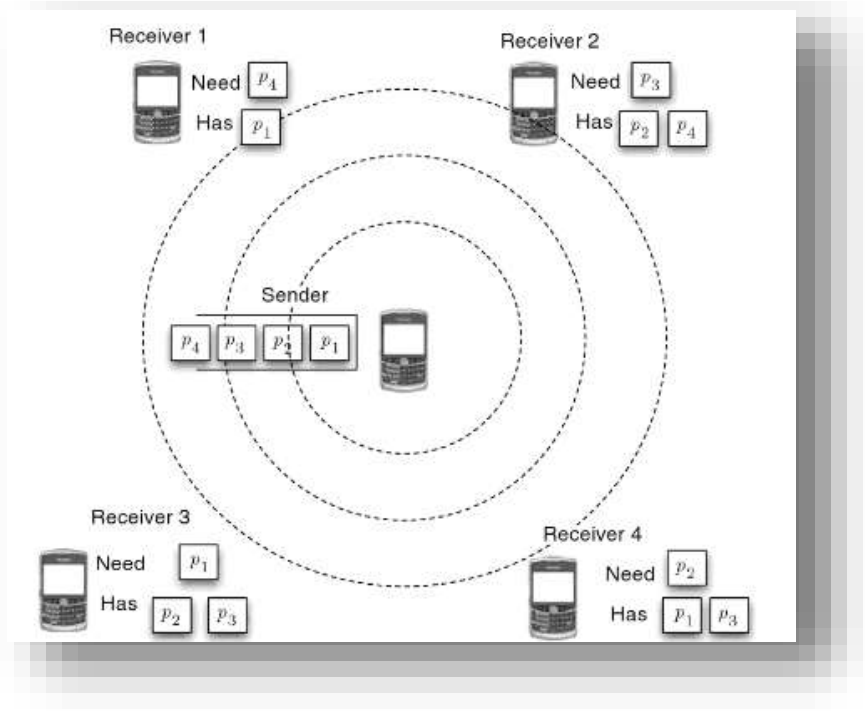

Figure 1 Index Coding

The basic index coding problem aims to transmit demanded data in minimum number of transmission.
There is one sender or server whose goal is send packets to receiver or server clients.
Here each receiver needs only certain set of data and aims to take advantage of rest of the data as side information.

From figure 1: Sender has packets p1, p2, p3 and p4. There are four receivers in a need of specific packet. Like receiver 1 has packet p1 and it needs packet p4.
The reference paper investigates this index coding problem in the presence of an eavesdropper.

2. **Perfect secrecy:**
   A cipher system is said to hold perfectly secrecy if there is no information retrieval of the plaintext from the observation of encrypted message

3. **Shannon's explanation of secrecy:**
   Eve has access to the cipher text C and her task is to obtain some information about either the transmitted message M (plaintext) or the key K used by Alice and Bob.

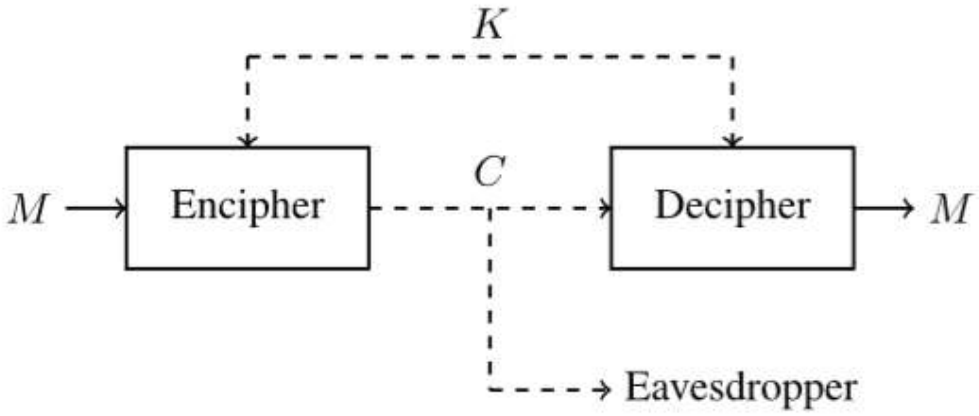

Figure 2 Shannon's Cipher System

Shannon showed that M can be transmitted in a way that C reveals nothing about M, if and only if H (K) ≥ H (M).

4. **Optimal index coding:**
   The goal is to find the minimum number of information bits that should be broadcast by the server so that each client can recover its desired messages with zero-error probability. This minimum required bits of information is called the optimal index code length.
   The general problem where each packet is sent to its authorized receiver and optimal algorithm in terms of minimum no of transmission is still unknown.
   Recent advancement in information theory shows that consider liner codes, the minimum that is optimal time is equal to the rank of the minimum rank matrix. Unfortunately the matrix completion problem is NP-hard in general.
   Overall, Optimal index coding is not less than intractable. That's why most popular coding schemes by following a systematic approach to these problems.

5. **Significance of Index coding**:
   Considering communication scenario with one server, two clients and a message set {M1, M2} of binary random variables. The first client has M2 as side information and wants M1, yet the second one has M1 and wants M2. The server can send the XOR of M1 and M2, instead of broadcasting each of them individually.
   Index coding is a special case of network coding problem the point to note here is that any **other network coding problem can be reduced to index coding problem.**

REVIEWS:

Review of Paper 1:

Perfectly Secure Index Coding

Consider a system shown in figure 2. There are a total of M messages which are converted into cipher text C using encryption key K. This is a simple toy example and can easily be generalised into higher system.

This system focus on transmitting the messages in the presence of an unwanted receiver.

The system is assumed to have perfect secrecy which guarantees that even having observed cipher text C no information can be obtained about plaintext.

Apart from these points, these system assumes Shannon's *zero-error* recovery of original message that implies desired client will be easily able to recover original message with H(M|K,C)=0.

Modelling of system that to be analysed is done without altering any generalization. The undesirable receiver co-exist with target receiver. To create or maintain *perfect secrecy* the transmitter and receiver share public and private keys. All legitimate clients have common key K and private key is assigned to specific client as K_i. The paper focuses on minimum number of transmission to send all messages.

Generalized one-time pad strategy: Public code C is generated using common key length, index code length and private key length.

The Shannon's cipher system is a special case which falls under generalized secure index coding problem. In Shannon system where there is only one receiver perfect secrecy condition states that rig/ark<=1 for all I belong to [t] which is an extension of the Shannon perfect secrecy condition to multiple receivers.

In other words, we showed that the conventional index coding rate region determines the cone of the secure rate region, which is equal to the cone of the generalized onetime pad strategy. Theorem 3 presents a similar statement to the Theorem 1 for the linear case. Moreover, we showed in Theorem 4 that relaxing the secrecy condition from perfect to weak secrecy does not change the rate region when we have an -error decoding condition. As a future work, one can study the effect of adversary's side information and/or capability of corrupting the public communication.

Discussion:

Definitions are present in the order and every definition is stated as it directly relates to main objective of the paper.

Proofs are given for every mathematical calculation involved into a used definition or to conclude something crucial like showing that code is *zero-error and epsilon-error perfectly secure achievable.*

Review of Paper 2:

Dynamic Index coding for Wireless broadcast networks

Similar to basic index coding theorem in dynamic index theorem we have a wireless broadcast station which act as a sender. Index coding optimizes the number of transmission. The advantage on which these coding are based is that multiple request from the clients are of the same message so instead of sending that message multiple times index coding gives advantages of sending that in less number of bits.

To understand the problem more precisely we take a bipartite graph. We know the plain text transmission is only optimal if the graph is acrylic. Dynamic coding uses a "dynamic max-weight algorithm" that run over variable length frames. The algorithm provides the facility of random packets arrivals and supports any bandwidth inside a capacity region.

One considerable point of this method that it does not acknowledge side information available at each receiver.

This problem is hence in those cases where there is chance of exploitation of system using side information.

Two algorithms were proposed in this paper. First algorithm works on rate vector. Both of them are two-max weight algorithms. Using simulation it was show that even the optimal solution is intractable but if operated inside code-contained capacity region .Then there are significant improvements in both throughput and existing delay latency.

The work is proposed on a bipartite graph so it is shown that in comparison to direct transmission it must exploit and use cycles in the demand graph.

An Equivalence between Network Coding and Index Coding

We show that the network committal to writing and index coding issues square measure equivalent. This equivalence holds within the general setting which incorporates linear and nonlinear codes.

Given any instance to the network coding drawback I, one will efficiently construct Associate in Nursing instance of the index coding drawback ˆ I such that: (a) There exists a linear answer to I if Associate in Nursing on condition that there exists an optimum linear answer to ˆ I, and (b) any optimum linear answer to ˆ I is efficiently changed into a linear answer to I.

When one needs to unravel a network coding instance I, a potential route is to show the network coding instance into an index committal to writing instance ˆ I.

Solve the index coding instance ˆ I, and switch the answer toˆ I into an answer to the initial network committal to writing instance I. Hence, any efficient theme to unravel index coding can yield an efficient theme for network coding. Expressed otherwise, our results imply that an understanding of the solvability of index coding instances can imply an understanding of the solvability of network committal to writing instances in addition.

Review of Paper 3

On Secure Index Coding with Side Information

This paper investigate the security aspects of some of the very occurring problem in wireless transmission.one of them is ICSI (Index Coding with Side Information). As the earlier paper had discussed that side information in dynamic index coding does not really matter but side information can be made useful or by increasing side information optimality can be achieved because number of transmission can be reduced.

The ICSI was first introduced by Birk and Kol. And the interesting part is it was came into existence because of popular demand in audio and video and daily newspaper delivery. INSI was first used by such type of application.

Similarly as technology advanced the area of application of index coding increased. Opportunistic wireless networks were started using ICSI. These were the networks in which any node on the network can listen to other wireless channel.

ICSI can be seen as a special case of popularly known NC coding problem. NC problem can be reduced to an instance of the ICSI problem.

Optimal solution of ICSI is a NP-hard problem. Because even for linear binary index code best solution is equivalent to finding min rank of a graph.

This paper restricts the study to linear index codes only but the results obtained are more or less same for other codes also. Linear index codes is chosen because of their vector property. Vector linear index code can achieve higher and better transmission rate than scalar one when used in ICSI problem.

ICSI problem can be written in the form of NC problem (non multicast). If modelled in NC problem then representation will be a directed graph in which each edge represents direction form a particular source to each sink which has the side information. The symbols transmitted on these edges cannot be made corrupted where in case of NC problem any edge can be corrupted. These two queer difference restrict the build-up of results over existing problem of NC schemes for IC schemes.

RESULTS;

Consider a system shown in figure 2. There are a total of M messages which are converted into cipher text C using encryption key K. This is a simple toy example and can easily be generalised into higher system. This system focus on transmitting the messages in the presence of an unwanted receiver.

Two algorithms were proposed in paper 2. First algorithm works on rate vector. Both of them are two-max weight algorithms. Using simulation it was show that even the optimal solution is intractable but if operated inside code-contained capacity region .Then there are significant improvements in both throughput and existing delay latency.

Third paper investigate the security aspects of some of the very occurring problem in wireless transmission.one of them is ICSI (Index Coding with Side Information). As the earlier paper had discussed that side information in dynamic index coding does not really matter but side information can be made useful or by increasing side information optimality can be achieved because number of transmission can be reduced.

METHDOLOGY USED FOR REVIEW:

The review of these paper is done to constructively analyse index coding while keeping its differences with other network coding. First a method is analysed using secrecy and then same method without secrecy. Analysing minimum number of transmission when with and without side information is carried out.

Some basic information and unknown terminology is searched on the internet and if something was included form that source then its link and name is mentioned in the reference page.

Most of the figures and `tables was given for understanding purpose so no additional or redundant is added in this document.

Mathematical proofs are not explained here but results are discussed for the same and some result from cited research papers were used directly.

CONCLUSION:

In these papers, we initiate a study of the security aspects of linear index coding schemes. We introduce a notion of block security and establish two bounds on the security level of a linear index code based on the matrix L.

Our second contribution is the analysis of the strong security of linear index codes. New bounds on the length of linear index codes, which are resistant to errors, eavesdropping, and information leaking, are established.

One important problem, which remains open, deals with a design of an optimal secure index coding scheme.

References:

[1] The Index Coding Problem: A Game-Theoretical Perspective Yu-Pin Hsu, I-Hong Hou, and Alex Sprintson

[2] Shannon's Theory of Secrecy http://www.eit.lth.se/fileadmin/eit/courses/edi051/lecture_notes/LN3.pdf

[3] Z. Bar-Yossef, Y. Birk, T. S. Jayram, and T. Kol, "Index coding with side information," in Proc. 47th Annu. IEEE Symp. Found. Comput. Sci. (FOCS), Oct. 2006, pp. 197–206.