International Journal of Innovation and Scientific Research
ISSN 2351-8014 Vol. 24 No. 1 Jun. 2016, pp. 61-69
© 2015 Innovative Space of Scientific Research Journals
http://www.ijisr.issr-journals.org/

A Survey of Secure Network Coding Against Eavesdropper

Ali Khan, Zahid Mahmood, and Farooq Aftab

School of Computer and Communication Engineering,
University of Science and Technology,
Beijing, China

ABSTRACT: Network coding, which gives the better performance and throughput to the system, is used for performing some encoding operations by intermediate nodes in multicast network. When we talk about transmission, security becomes one of the main focus points. As nodes mix the incoming symbols and output it this leads it vulnerable to adversary attack. In this paper we discuss the Secure Network Coding scheme which helps against eavesdropper adversary threat. We analyze the performance of these schemes. We also discuss different security levels and proposed schemes associated to these.

KEYWORDS: Network Coding, Security, Eavesdropper, Secure Network Coding, Security levels.

1 INTRODUCTION

In the traditional routing where the routers typically store and forward the information cannot be overlaid. Network coding, which was first introduced by Ahlswede et al. [1], shows how the information can be transmitted more efficiently with better throughput if the intermediate nodes perform encoding on the received packets instead of just store and forward as in traditional routing. The basic importance of network coding can be easily understood by Fig. 1. In this butterfly network topology a single source (s) wishes to transmit information to destinations *t* and *u*. Each edge is represented as error free channel which is capable of delivering a single bit. A network coding solution helped to achieve throughput 2-packets per channel use. The source sends two packets x and y, but instead of routing one and blocking the other, node *b* transmits their *XOR*. Node t receives x and $x \oplus y$ *since* $x \oplus (x \oplus y) = y$, so node *t* can recover both *x* and *y*. By using encoding operation at an internal node and decoding at sink nodes the multicast throughput has improved beyond what can be achieved in routing.

Network coding has advantages like enhancing better throughput [2], network robustness [3] and reduce network congestion [4]. NC has been applied to many areas as Adhoc Network [5], DTNs [6], P2P network [7], Wireless Sensor Network [8], Content distribution Network [9] and many more.

As network coding allows intermediate nodes to linearly combine multiple packets into encoded ones which lead to vulnerability of network being attacked by adversary. To tackle this security issue Cai and Yeung [10] proposed secure network coding for the first time which laid foundation to the new paradigm of research. They gave a security solution against an eavesdropper adversary that has the ability of observing bounded number of edges over a wiretap network and yields a network code by linear transformation on each and every edge. Bhattad et al. [11] proposed weakly secured network coding without affecting the throughput. Feldman et al. [12] pointed out the relation between secure network coding and secret sharing. They also discussed the tradeoff between code alphabet size and size of message set. Rouayheb et al. [13] shows secure network coding depending on maximum distance separable based on wiretap channel of type II given by Ozarow and Wyner [14] and derived new bounds on required field size. After these many other schemes were proposed for secure network coding.

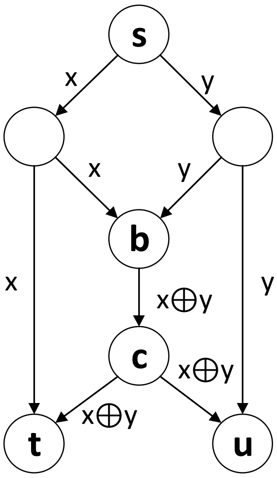

Fig. 1. Network Coding (Butterfly Network)

Over the past years there have been many secure network coding techniques proposed against Eavesdropping attack. In this paper we analyze different secure network coding techniques which are suitable against eavesdropping attack and secure the confidentiality and integrity of the communication network. We discuss different security levels and categorize proposed schemes on the basis of these levels of security.

In this paper we analyze the schemes which are suitable against eavesdropper adversary attack for securing networks. Section 2 discusses the overview of architecture of network coding in terms of security, section 3 is about the schemes which tackle the eavesdropping attack, section 4 has the performance analysis of the schemes, section 5 discuss security levels and schemes associated with these levels. Follow by the conclusion.

2 NETWORK CODING MODEL

2.1 ENCODING MODEL

The model of communication network is an acyclic directed graph presented by $G(V, E)$ where V is set of nodes and E is the set of edges. The messages between nodes are transmitted in packets and each packet is assumed to be an element of finite field $F_q = GF(q)$ and can be written in binary vector of length $n = \log_2(q)$ bits. A source node $s \in V$ and a set of destinations $D \subseteq V$. Let $h(i)$ the maximum number of packets transmitted from s to all the destination nodes D in i rounds. Then the capacity h^* of network is given by

$$h^* = \lim_{i\to\infty} \sup \frac{h(i)}{i}$$

2.2 EAVESDROPPING SECURITY MODEL

We have conventional Alice, Bob and Eve topology. Alice is sending a message to Bob over a network and Eve has the ability to eavesdrop the communication between Alice and Bob. We say that Eve is strong both coherent and non-coherent way and knows encoding decoding schemes. Coherent means that the encoding decoding are the same and both the communicating parties know the pattern already as they have some agreement on it. This type of communication is not secure as eavesdropper can know the pattern and thus network is always under threat. Non-coherent is that the encoding decoding patterns are different receiver doesn't know anything about the encoding pattern and is more secured than coherent.

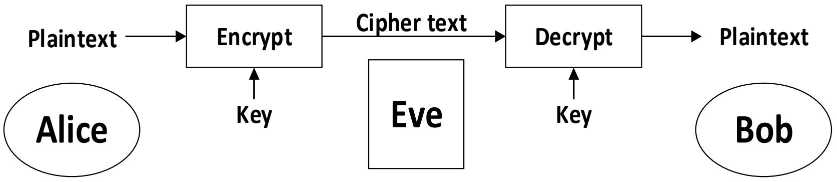

Fig. 2. Security Model

Let us assume Eve can control certain node Z_1 which is subset of links Z_o. The adversary adds some corrupted packets into the message so the effect on network will be $Y = TX + T'Z$ where X is the encoding source, Z is error specified, Y is incoming message at terminal and T and T' is the linear transformation over Finite field $\mathbf{F}$. In case of coherent setting in the presence of eavesdropper the expression for secure coding is

$$R = H(X) = H(X|Y_i) + I(X;Y_i) = H(X|Y_i) + I(X;Z,Z^-)$$
$$= I(X;Z,Z^-) = I(X;Z) + I(X;Z^-|Z)$$
$$= I(X;Z^-|Z) \leq H(Z^-) \leq C - z_1$$

Where eavesdropper has access to link z_1.If the network is perfectly secure then $H(X|Y_i) = 0$ which means the terminal is able to deduce source information and $I(X;Z) = 0$ which means the communication is secure. C is the maximum multicast and R is the optimal rate of communication.

We consider the original coding scheme as fixed, the code design specifies the matrix T which defines transmitted message as $M = T(X,R)$. The error correction uses finite field $\mathbf{F}$ of size $q >= \binom{|E|}{z_1}$ where $\binom{|E|}{z_1}$ means that the possible subset of channel links that adversary can eavesdrop. In the case of non-coherent the source node passes its message through linear filter. The other nodes in the network perform random linear combination over sufficiently large finite field as of the distributed random linear network coding scheme. They generate a distributed non coherent random linear code that secures the network from wire tapper which is at the most on link z_1.

These basic models and their calculation can give us better understanding of the security schemes for eavesdropping attack in the next section.

3 Security Schemes

In communication where some secret information is shared, the confidentiality becomes the top priority and should be acquired by all means. Many researchers over the years proposed security schemes against eavesdropping attack.

Yawen et al [15] proposed two secure network coding schemes. These schemes permute a function to randomize the message vector which is transmitted by a source. Details of schemes are as follow:

3.1 Basic Scheme

The source selects a random symbol w and inserts it at the end of message vector. Source sends messages vector $X = (x_1, x_2, \dots, x_{n-1}, w)^T$ where x_1 to x_{n-1} are information symbol and inserted random symbol is w. Source uses a random permutation function h (which is a public function) with w to randomize the information symbols. Using h function source computes a vector $X' = (x'_1, x'_2, \dots, x'_n)^T$ where

$$\begin{cases} x'_1 = x_1 + h(w) \\ x'_2 = x_2 + h^2(w) \\ \dots\dots\dots\dots \\ x'_{n-1} = x_{n-1} + h^{n-1}(w) \\ x'_n = w \end{cases} \qquad (1)$$

$\mathrm{h}^2(\mathrm{w}) = \mathrm{h}(\mathrm{h}(\mathrm{w}))$ means that h function is applied twice to w and so on. After the calculation of vector X', it multiplies a full rank matrix C of $\mathrm{n} \times \mathrm{n}$ to X' and get $\mathrm{X}'' = \mathrm{CX}'$. C should have the property that the last row of its reverse matrix C^{-1} is not in the linear span of all eavesdropping matrix that have $(\mathrm{n}-1) \times \mathrm{n}$ dimension.

Each destination node first decodes each element in vector X'' by solving a set of linear equations. The receiver obtains vector X' by $X' = C^{-1}X''$ where C^{-1} is reverse full rank matrix C. As receiver knows the value of w, which is last element in vector X', it can calculate x_1 to x_{n-1} by

$$x_i = x'_i - h^i(w), i \in \{1, \dots, n-1\} \qquad (2)$$

3.2 Advanced scheme

Instead of inserting random symbols into message vector, source applies h function to the information symbols directly. If multicast capacity is 2 then message vector sent by source is $X' = (x'_1, x'_2)^T$ where

$$\begin{cases} x'_1 = x_1 + h(x_2) \\ x'_2 = h(x'_1) + x_2 \end{cases} \qquad (3)$$

In general case multicast capacity is $n(n \geq 2)$ then message vector $X' = (x'_1, \dots, x'_n)^T$ is

$$\begin{cases} x'_1 = x_1 + h(x_2) \\ x'_2 = h(x'_1) + x_2 \\ \dots\dots\dots\dots \\ x'_{n-1} = x_{n-1} + h(x_n) \\ x'_n = h(x'_1) + \dots + h(x'_{n-1}) + x_n \end{cases} \qquad (4)$$

It first solves for elements in X' then it calculates $x_n, x_{n-1}, \dots, x_1$ iteratively by

$$\begin{cases} x_1 = x'_n - h(x'_1) + \dots + h(x'_{n-1}) \\ x_{n-1} = x'_{n-1} - h(x_n) \\ x_{n-2} = x'_{n-2} - h(x_{n-1}) \\ \dots\dots\dots\dots.. \\ x_1 = x'_1 - h(x_2) \end{cases} \qquad (5)$$

Peng Zhang et al. [16] proposed P-Coding technique against eavesdropping attacks by permutation performed on coded message and its coding vector. After the PEF (Permutation Encryption Function) operations, symbols of the messages and corresponding GEVs (Global Encoding Vectors) are mixed and reordered together as in Fig 3. Details are as follows:

For utilizing the permutation encryption two issues should be considered.

1) The plaintext m should be protected otherwise it is easy to deduce key k by relating it with ciphertext c and can be formalized as $I(K, M|C) = 0$ where $I(\cdot,\cdot \mid \cdot)$ is the conditional mutual information.
2) The encryption key should be randomly chosen.

3.3 P-Coding Scheme

The P-Coding scheme is consist of three stages: source encoding, intermediate recording and sink decoding. It is assumed that Key Distribution Center (KDC) is responsible for symmetric key establishment then the source and sinks can get the PEF key k offline.

Source Encoding: Consider that a source s has h messages $x_1, \dots, x_h$ to be sent out with their corresponding unit vectors. The source performs linear combination on these messages with randomly chosen LEVs. For instance with LEV $\beta(e_i)$ the coded message is $y(e_i) = [\beta(e_i), \beta(e_i)X]$ where $X = [x_1, \dots, x_h]^T$. Then the source performs permutation encryption on each message $y(e_i)$ to get its cipher text $c[y(e_i)] = E_k[y(e_i)]$.

Intermediate Recording: The intermediate nodes do not have any knowledge of key being used because the symbols of messages as well as their corresponding GEVs are re-arranged by PEF. As permutation encryptions are exchangeable with symbol level linear combinations, intermediate recording can transparently performed on the encrypted messages:

$$c[y(e_i)] = c\left[\sum\nolimits_{e' \in \Gamma^-(v)} \beta_{e'}(e) \cdot y(e')\right] = \sum\nolimits_{e' \in \Gamma^-(v)} \beta_{e'}(e) \cdot c[y(e')] \qquad (6)$$

Sink Decoding: Each sink node, on receiving a message $c[y(e_i)]$ from its incoming link $e' \in \Gamma^-(v)$, it decrypts the message by performing permutation decryption:

$$D_k\{c[y(e_i)]\} = E_{k^{-1}}\{E_k\,[y(e_i)]\} = y(e_i) \qquad (7)$$

Once h linearly independent messages $\mathrm{y(e_1), \dots, y(e_h)}$ are collected then the sink derives the following matrix:

$$\mathrm{Y} = \begin{bmatrix} \mathrm{y(e_1)} \\ \vdots \\ \mathrm{y(e_h)} \end{bmatrix} = \begin{bmatrix} \mathrm{g(e_1), g(e_1)X} \\ \vdots \\ \mathrm{g(e_h), g(e_h)X} \end{bmatrix} = [\mathrm{G, GX}] \qquad (8)$$

Then the source messages can be recovered by applying Gaussian elimination on Y:

$$\mathrm{Y} = [\mathrm{G, GX}] \xrightarrow{\text{Gaussian elimination}} [\mathrm{I, X}] \qquad (9)$$

3.4 ENHANCED P-CODING SCHEME

In practical network coding scenarios the source may need to transmit a large volume of data D. For this Source should divide D into generations:

$$\mathrm{D} = [\underbrace{\mathrm{x_1, \dots, x_h}}_{\mathrm{G_1}}, \underbrace{\mathrm{x_{h+1}, \dots, x_{2h}}}_{\mathrm{G_2}}, \underbrace{\mathrm{x_{(n-1)h+1}, \dots, x_{nh}}}_{\mathrm{G_3}}, \dots]$$

In P-Coding an accidental key disclosure in one generation will compromise the secrecy of the following transmission if the same key is used throughout the transmission. For this issue randomly perturbing key is used in each generation. Let $\mathrm{k_i}$ denote the key used in $\mathrm{i^{th}}$ generation then $\mathrm{k_i}$ is calculated by $\mathrm{k_i = \omega_i{}^{\circ}k_{i-1}}$ where ω_i is a perturbing key with length n. If ω_i is changed in each generation and only shared by the source and sinks then this will effectively prevent single generation failure.

Liu et al. [17] proposed a novel secure network coding based on two coding model intra-generation secure coding and inter-generation secure code. Intra Generation Secure Coding (Intra-GSC) is used in secure network coding to limit the encryption operations for each generation, and subject the scrambled and the remaining original source vectors to a linear transformation. This method for secure network is then generalized by using Inter-Generation Secure Coding (Inter-GSC).

3.5 BASIC SCHEME USING INTRA-GSC

The plaintext of one generation is represented as $\mathrm{m \times n}$ matrix $\mathrm{V = (v_1^T, v_2^T, \dots, v_m^T)^T}$ where $\mathrm{v_i = (v_{i1}, v_{i2}, \dots, v_{in}) \in F_q^n (i = 1,2, \dots, m)}$ are termed as source vectors. At first $\mathrm{r (r < m)}$ source vector of the generation is randomized by the source. For this purpose a stream cipher E is used to encrypt r source vector. For each $\mathrm{i = 1,2, \dots, r}$ we have $\mathrm{v_i = (v_{i1}, v_{i2}, \dots, v_{in}) \xRightarrow{\text{Encryption}} u_i = (u_{i1}, u_{i2}, \dots, u_{in})}$. In other words

$$\begin{cases} \mathrm{u_{i1} = E(id, v_{i1}) \doteq v_{i1} + h_{i1}} \\ \mathrm{u_{i2} = E(id, v_{i2}) \doteq v_{i2} + h_{i2}} \\ \quad \vdots \\ \mathrm{u_{in} = E(id, v_{in}) \doteq v_{in} + h_{in}} \end{cases}, \qquad (10)$$

Where each $\mathrm{h_{ik}}$ is a random symbol in $\mathrm{F_q}$ to scramble $\mathrm{v_{ik}}$ for $\mathrm{k = 1,2, \dots, n}$ and the single generation mixing network coding (SGMNC) transmission for one generation is denoted by id. Naturally $\mathrm{h_i = (h_{i1}, h_{i2}, \dots, h_{i,n-1}, h_{in}}$ can be seen as a random vector to scramble $\mathrm{v_i}$.

The source generates an invertible random matrix A as $\mathrm{A = (A_1 \quad A_2)}$in which $\mathrm{A_1 = (a_{ij}) (i = 1,2, \dots, m; j = 1,2, \dots, r)}$ is $\mathrm{m \times r}$ matrix in $\mathrm{F_q^*}$ (set of all non-zero elements of $\mathrm{F_q}$) and

$$\mathrm{A_2} = \begin{pmatrix} \mathrm{a_{1,r+1}} & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \mathrm{a_{r,r+1}} & 0 & 0 & \cdots & 0 \\ \mathrm{a_{r+1,r+1}} & 0 & 0 & \dots & 0 \\ 0 & \mathrm{a_{r+2,r+2}} & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & \mathrm{a_{mm}} \end{pmatrix}_{\mathrm{m \times (m-r)}}$$

Note that $\mathrm{a_{ij}, a_{ij} (i = 1,2, \dots, r; j = r+1, r+2, \dots, m)}$ in $\mathrm{A_2}$ are also selected at random in $\mathrm{F_q^*}$.The source calculates the $\mathrm{m \times n}$ matrix C i.e.

$$\mathrm{C = A \cdot W = (c_1^T, c_2^T, \dots, c_m^T)^T} \qquad (11)$$

Where $W = (u_1^T, \dots, u_r^T, v_{r+1}^T, \dots, v_m^T)^T$

For the sake of security, A must be protected and transmitted with the message packets. Therefore, the encoded packets are constructed as follows:

When $i = 1,2, \dots, r$

$$c_i^* = (E(id, a_{i1}), \dots, E\big(id, a_{i,r+1}\big), c_i$$

When $i = r + 1, r + 2, m,$

$c_i^* = (E(id, a_{i1}), \dots, E\big(id, a_{i,r}\big), E(id, a_{ii}), c_i$ where $E(id,\cdot) \in F_q$. The source generates the global coding vector for each packet c_i^* for $i = 1,2, \dots, m$ and sends out all the coded packets into the network using standard RLNC protocol.

When receiving m linear independent legitimate packets $w_i(i = 1,2, \dots, m)$ belonging to the generation id, a receiver can easily decode $c_i^*(i = 1,2, \dots, m)$with Gaussian Elimination with high probability. Then it decrypts and subsequently reconstructs A. The receiver can solve $u_1, \dots, u_r, v_{r+1}, \dots, v_m$ by calculating c_i^*. Finally $v_1, v_2 \dots, v_r$ are recovered by decrypting $u_1, \dots, u_r$ using the secret key. A larger value of r means a large communication overhead. Actually $r = 1$ is secure enough with a coding field of proper size for general applications.

3.6 GENERALIZED SCHEME USING INTER-GSC

The basic scheme can be easily generalized and compatible with multiple generations mixing network coding (MGMNC). For simplifying, one set J is secured in one time shot.

The mixing set include w generations $g_i(i = 1,2, \dots, w)$ each with a size of l_i and $L = \sum_{i=1}^{w} l_i$. Similar to MGMNC, each mixing set can be viewed as an encoding unit and all generations in the unit perform the operations of Inter-GSC which finally makes the whole L packets $v_1, v_2, \dots, v_L$ in J are encoded together.

First only r packets of the first generation in the mixture set J are needed to be encrypted using the secret keys. The first r packets of the generation 1 in J are encrypted as below:

$v_i = (v_{i1}, v_{i2}, \dots, v_{in}) \xRightarrow{\text{Encryption}} u_i = (u_{i1}, u_{i2}, \dots, u_{in})$ for $i - 1,2, \dots, r(r < l_1)$

The source generated $L \times L$ invertible matrix $\overline{A}$ as follows and then computes

$C = \overline{A} \cdot W = (c_1^T, c_2^T, \dots, c_L^T)^T$ where $W = (u_1^T, \dots, u_r^T, v_{r+1}^T, \dots, v_L^T)^T$.

$$\overline{A} = \begin{pmatrix} a_{11} & \cdots & a_{1r} & a_{1,r+1} & 0 & \cdots & 0 \\ \vdots & \cdots & \vdots & \vdots & 0 & \cdots & 0 \\ a_{r+1,1} & \cdots & a_{r+1,r} & a_{r+1,r+1} & 0 & \cdots & 0 \\ a_{r+2,1} & \cdots & a_{r+2,r} & 0 & a_{r+2,r+2} & \cdots & 0 \\ a_{r+3,1} & \cdots & a_{r+3,r} & 0 & 0 & \cdots & 0 \\ \vdots & \cdots & \vdots & \vdots & \vdots & \ddots & 0 \\ a_{L1} & \cdots & a_{Lr} & 0 & 0 & \cdots & a_{LL} \end{pmatrix}$$

Similar to the Intra-GSC, the ith row of $\overline{A}$ is encrypted and then concatenated with $c_i(i = 1,2, \dots, L)$, which constitute the forwarding packets $c_1^*, c_2^*, \dots, c_L^*$. The source encodes and forwards the L packets $c_1^*, c_2^*, \dots, c_L^*$ belonging to w generations using MGMNC.

A receiver can decode the received largest subset of the generation in J with incremental decoding or collective decoding until all generations of J are recovered. After decrypting the encrypted element of the matrix $\overline{A}$ using the right secret keys, the receiver can reconstruct the vectors $u_1, u_2, \dots, u_r\ v_{r+1}, \dots, v_L$ by $W = \overline{A}^{-1} \cdot C$ and finally recovers the plaintext vectors $v_1, v_2, \dots, v_r$.

4 PERFORMANCE EVALUATION

Following Table 1 gives the comparative analysis of schemes discussed in above section.

Table 1. Comparative Analysis of Schemes

Schemes	Field size	Security type	Computational complexity	Encryption volume per generation
Yawen et al. Advance Scheme	Large	Weak	$O(m^2n)$	0
Enhanced P-Coding Scheme	Small	Weak	$O(m^2n)$	$m(m+n)$
Intra GSC	Small	Weak	$O(rmn)$	$m(r+1)+rn$
Inter-GSC	Small	Weak	$O(\frac{rLn}{w})$	$\frac{L(r+1)+rn}{w}$

Larger value of source vector r can obtain the stronger security level, while more encryption operations to the plaintext data have to be performed. There is a tradeoff between the security level and computational complexity. The value of r also determines high bandwidth overhead for the packet transmission. From the table 1 we can observe that except for Yawen et al. proposed schemes which are based on large field size as compared to others but all the scheme has common security type i.e. weakly secured.

If we look at the computational complexity for encoding single generation of these schemes we can say in Intra-GSC to inter-GSC it has decreased. So Inter-GSC is less complex as compared to other schemes.

As we know the required number of cryptographic operations is directly related to volume of data to be encrypted. We observed that the Inter-GSC has lower encryption volume per generation as we can see w generations are encoded together so if the value of w is large then the encryption overhead per generation is smaller.

5 RELATED WORK

The research on securing network coding focuses on how to secure network coding system in the presence of various attackers. The security is divided into three different levels in network coding system:

5.1 SHANNON/PERFECTLY SECURED

The system in which the adversary cannot get any information about the source message from the intercepted packets is said to be Shannon Secured or perfectly secured. The equation can be formulated as:

$$\mathrm{H}(\mathrm{X}|\mathrm{W_i}) = \mathrm{H}(\mathrm{X}), \qquad \forall \mathrm{W_i} \in \mathrm{A}$$

5.2 WEAKLY SECURED

The system in which the adversary cannot obtain any meaningful information about the message from the intercepted packets is said to be Weakly Secured. This can be given as:

$$H(x_i|W_i) = H(x_i), \qquad \forall x_i \in X;\ \forall W_i \in A$$

5.3 COMPUTATIONAL SECURED

The system in which adversary is assumed to be resource bounded is said to be computational secured. It is satisfied if the amount of effort to obtain any meaningful information about $\forall \mathrm{x_i} \in \mathrm{X}$ using the all the possible methods exceeds computational resources of the adversary.

We can categorize different scheme proposed by researchers into security levels discussed above. Table 2 gives the overview of schemes on the basis of different levels of security.

Table 2. Different Security Level Schemes

Schemes	Security Level	Explanation
Cai et al. [10]	Shannon	First identified the eavesdropper who can monitor limited links and presented an approach to transform any linear network code to be secure in the presence of this kind of adversary.
Feldman et al. [12]	Shannon	Found a tradeoff between multicast capacity and the field size. Making network coding secure is equivalent to find codes with some distance properties.
Rouayheb et al. [13]	Shannon	Proposed scheme by implementing cosset coding at the source without affecting the underlying network code architecture.
Silva et al. [18]	Shannon	Proposed scheme named Maximum Rank Distance (MRD)
Bhattad et al. [11]	Weakly	Proposed a scheme in which adversary cannot get any meaningful information and multicast capacity can be achieved by performing linear transformation at the source.
Yawen et al. [15]	Weakly	Proposed schemes that permute a function to randomize the message vector which is transmitted by a source.
Peng Zhang et al. [16]	Weakly	Proposed P-Coding technique against eavesdropping attacks by permutation performed on coded message and its coding vector
Liu at el. [17]	Weakly	Proposed a novel secure network coding based on two coding model intra-generation secure coding and inter-generation secure code.
Vileta et al. [19]	Computational	Proposed a scheme in which a set coding vectors encrypted and another unencrypted are attached to maintain standard coding processes at intermediate nodes.
Fan et al. [20]	Computational	Proposed Homomorphic encryption technique.
Jain et al. [21]	Computational	Gave a necessary and sufficient condition for the unicast in cyclic networks to be secure by exploiting the topological features of communicating system.
Lima et al. [22]	Computational	Considered the threat posed by intermediate nodes and developed an algebraic security.

6 Conclusion

In this paper we have analyzed different security schemes against eavesdropping attack. We have observed how different parameters like computational complexity and encryption volume per generation are related to each other and affect the overall performance of the schemes. We conclude that Inter GSC is better security scheme against eavesdropping attack. We also investigate different security levels and the schemes proposed for them.

References

[1] Ahlswede R., Cai Ning, Li S. R. *et al*, “Network information flow”, IEEE Transactions on Information Theory, vol. 46, no. 4, pp. 1204-1216, 2000.

[2] Li S. R., Yeung R. W., Cai Ning, “Linear network coding”, IEEE Transactions on Information Theory, vol. 49, no. 2, pp. 371-381, 2003.

[3] Koetter R., Kschischang F. R., “Coding for errors and erasures in random network coding”, IEEE Transactions on Information Theory, vol. 54, pp. 3579-3591, 2008.

[4] Chen Lijun, Ho T., Chiang M., *et al*, “Congestion Control for Multicast Flows with Network Coding”, IEEE Transactions on Information Theory, vol. 58, pp. 5908-5921, 2012.

[5] D. Annapurna, N. Tejas, K. B. Raja and K. R. Venugopal, “An energy efficient multicast algorithm for an Adhoc network using network coding and MAC scheduling”, International Conference on Signal Processing and Communication (ICSC), pp. 62–67, 2013.

[6] E. Altman, L. Sassatelli, & F. De Pellegrini, “Dynamic Control of Coding for Progressive Packet Arrivals in DTNs”, IEEE Transactions on Wireless Communication, vol. 12, no. 2, pp. 725–735, 2013.

[7] A. M. Sheikh, A. Fiandrotti, & E. Magli, “Distributed scheduling for scalable P2P video streaming with network coding”, IEEE INFOCOM Proceedings, pp. 11–12, 2013.

[8] R. R. Rout & S. K. Ghosh, “Enhancement of Lifetime using Duty Cycleand Network Coding in Wireless Sensor Networks”, IEEE Transactions on Wireless Communication, vol. 12, no. 2, pp. 656–667, 2013.

[9] Q. Yan, M. Li & Z. Yang, “Throughput Analysis of Cooperative Mobile Content Distribution in Vehicular Network using Symbol Level Network Coding”, IEEE Journal of Selected Areas of Communication, vol. 30, no. 2, pp. 484–492, 2012.

[10] Cai Ning & Yeung R. W., “Secure network coding”, Proceedings of International Symposium in Information Theory, Lausanne, Switzerland: IEEE Press, pp. 323, 2002.

[11] Bhattad K., Narayanan K. R., “Weakly secure network coding”, Proceedings of 1st Workshop on Network Coding, Theory, and Applications, Riva del Garda, Italy, IEEE Press, 2005.

[12] Feldman J., Malkin T., Servedio R. A., *et al*, “On the capacity of secure network coding”, Proceedings of 42nd Annual Allerton Conference on Communication, Control, and Computing, Monticello, pp. 388-401, 2004.

[13] Rouayheb S. Y. E., Soljanin E. & Sprintson A., “Secure network coding for wiretap networks of type II”, IEEE Transactions on Information Theory, pp. 1361-1371, 2012.

[14] Ozarow L. H. & Wyner A. D., “Wire-tap channel II”, AT&T Bell Labs. Tech. J., pp. 2135-2157, 1984.

[15] Yawen Wei, Zhen Yu & Yong Guan, “Efficiently weakly secure network coding schemes against wiretapping attacks”, IEEE International Symposium on Network Coding (NetCod), pp. 1-6, 2010.

[16] Peng Zhang, Yixin Jiang, Chuang Lin, Yanfei Fan & Xuemin Shen, “P-Coding: Secure network coding against eavesdropping attacks”, IEEE Proceedings of INFOCOM, pp. 1-9, 2010.

[17] Liu Guangjun, Liu Binyue, Liu Ximeng, Li Fang & Guo Wangmei, “Low-complexity secure network coding against wiretapping using inta/inter-generation coding”, IEEE Transaction of China Communications, pp. 116-125, 2015.

[18] D. Silva & F. R., “Security for wiretap networks via rank-metric codes”, Proceedings of IEEE ISIT, pp. 176-180, 2008.

[19] J. P. Vilela, L. Lima & J. Barros, “Lightweight security for network coding”, Proceedings of IEEE ICC, pp. 1750-1754, 2008.

[20] Y. Fan, Y. Jiang, H. Zhu, & X. Shen, “An efficient privacy-preserving scheme against traffic analysis in network coding”, Proceedings of IEEE INFOCOM, pp. 2213-2221, 2009.

[21] K. Jain, “Security based on network topology against the wiretapping attack”, IEEE Wireless Communications, pp. 68-71, 2004.

[22] L. Lima, M. Médard, & J. Barros, “Random linear network coding: A free cypher?”, Proceedings of IEEE ISIT, pp. 546–550, 2007.