International Journal of Smart Sensor and Adhoc Network

Volume 3 | Issue 1 Article 18

October 2012

NB-JNCD Coding and Iterative Joint Decoding Scheme for a Reliable communication in Wireless sensor Networks with results

Kishore kumar R
Department of Computer Science & Engineering Siddaganga Institute of Technology, Tumkur,Karnataka,India., kishorekr@gmail.com

S Nayana
Department of Computer Science & Engineering Siddaganga Institute of Technology, Tumkur,Karnataka,India., snayana@gmail.com

NB-JNCD Coding and Iterative Joint Decoding Scheme for a Reliable communication in Wireless sensor Networks with results

Kishore kumar R, MTech Student
Department of Computer Science & Engineering
Siddaganga Institute of Technology,
Tumkur,Karnataka,India.

S Nayana, Assistant Professor
Department of Computer Science & Engineering
Siddaganga Institute of Technology
Tumkur,Karnataka,India.

Abstract:**Privacy threat is a very serious issue in multi-hop wireless networks (MWNs) since open wireless channels are vulnerable to malicious attacks. A distributed random linear network coding approach for transmission and compression of information in general multisource multicast networks. Network nodes independently and randomly select linear mappings from inputs onto output links over some field. Network coding has the potential to thwart traffic analysis attacks since the coding/mixing operation is encouraged at intermediate nodes. However, the simple deployment of network coding cannot achieve the goal once enough packets are collected by the adversaries. This paper proposes non-binary joint network-channel coding for reliable communication in wireless networks. NB-JNCC seamlessly combines non-binary channel coding and random linear network coding, and uses an iterative two-tier coding scheme that weproposed to jointly exploit redundancy inside packets and across packets for error recovery.**

KEYWORDS:**Network Coding, Non-Binary Channel Coding,Homomorphic Encryption Functions (HEFs), Network Coding Based Privacy-Preserving scheme, Security Analysis, Channel Coding, Channel Model.**

1. Introduction

A wireless sensor network (WSN) is a heterogeneous network composed of a large number of tiny low-cost devices, denoted as nodes (or motes), and one or few general-purpose computing devices referred to as base stations (or sinks). A general purpose of the WSN is to monitor some physical phenomena (e.g., temperature, barometric pressure, light) inside an area of deployment. Nodes are equipped with a communication unit (e.g., radio transceiver), processing unit, battery and sensor(s). Nodes are constrained in processing power and energy, whereas the base stations have laptop capabilities and not severely energy constrained.

The base stations usually act as gateways between the WSN and other networks (e.g., Internet). There is a wide variety of applications for WSNs [10], ranging from military applications (e.g., perimeter monitoring [11]) through environmental (e.g., animal habitat monitoring [12]) and health applications (e.g., patient health monitoring) to commercial applications (e.g., shopping habits monitoring, bridge structural health monitoring [13]).WSNs can be classified according to several aspects with impact on the security protocol design. One such aspect is the mobility of nodes and the base station. The nodes can be mobile or placed on static positions. The same holds true for the base station. Another consideration is the way the nodes are placed. The nodes can be deployed manually on specific locations following some predefined network topology or randomly deployed in an area, e.g., by dropping from a plane. The number of nodes is also a very important factor (number of nodes in a network can range from tens to tens of thousands). In our future work, we will focus on WSNs consisting of large number of nodes (hundreds or thousands) deployed without a priori topology design.

Multi-hop Wireless Networks are regarded as a highly promising solution for extending the radio coverage range of the existing wireless networks, and they can also be used to improve the system reliability through multi-path packet forwarding. MWNs are susceptible to various attacks, such as eavesdropping, data modification/injection, and node compromising. Since wireless networks do not have defined borders and air waves can penetrate into unintended areas allowing attackers to bypass perimeter firewalls, sniff sensitive information, access the internal network or attack wireless hosts without direct access to the network. These attacks may breach the security of MWNs, including confidentiality, integrity, and authenticity. In addition, some advanced attacks such as traffic analysis and flow tracing can also be launched by a malicious adversary to compromise user's privacy, including source anonymity and traffic secrecy.

Privacy is the right of an individual to be left alone [14]. It determines how much information about a person is exposed to others [15]. Privacy is most highly valued by 'public figures', but it is equally coveted by 'commoners' because they do not want to turn their

activities into a public spectacle. The central concept of privacy is anonymity, which refers to the state of an individual's information being publicly unknown. In reality, people do not intend to be entirely anonymous.

The capacity of multicast networks with network coding was given in [16]. We present an efficient distributed randomized approach that asymptotically achieves this capacity. We consider a general multicast framework-multisource multicast, possibly with correlated sources, on general networks. We use a randomized strategy: all nodes other than the receiver nodes perform random linear mappings from inputs onto outputs over some field. These mappings are selected independently at each node. For instance, if the network and network code are fixed, all that is needed is for the sources to send, once, at the start of operation, a canonical basis through the network. Our primary results show, first, that such random linear coding achieves multicast capacity with probability exponentially approaching with the length of code. Second, in the context of a distributed source coding problem, we demonstrate that random linear coding also performs compression when necessary in a network, generalizing known error exponents for linear Slepian-Wolf coding [17] in a natural way.

Compared to wire line communication, wireless communication suffers from high and time-varying packet loss due to the detrimental effect of fading of wireless channels. One method to provide reliable communication is using redundant information, which can be added either inside a packet (bit/symbol level or physical layer) or across multiple packets (packet level or network layer).The former is called error-correction and the latter is referred to as erasure-correction. For point to point communication in wireless environments, it is implemented at the physical layer to recover erroneous bits/symbols through redundant parity check bits/symbols appending to a packet. The error recovery capability depends on the specific coding strategy and the amount of redundant bits/symbols. Channel coding has been widely employed in practical wired and wireless systems. In [18], Lin et al. described many sophisticated channel coding schemes, such as Reed-Solomon code, convolution code, Turbo code and low-density parity-check (LDPC) code. Many schemes have sound performance and can approach the channel capacity of non-fading channels. However, when a channel experiences slow and deep fading, the performance of channel coding degrades dramatically. In such a case, the communication through the channel cannot continue and packet loss will occur. Network coding was first introduced to achieve the multicast capacity in wired lossless networks [19]. The studies in [20, 21, 22]extended network coding to wireless networks, again focusing on lossless channels. Later, Guo et al. proposed an efficient error recovery scheme using network coding for lossy erasure channels in underwater sensor networks [23, 24]. They showed that random linear network coding is simple and efficient in large multi-hop wireless Networks. Recently, Chen et al. applied network coding to user cooperation in one hop systems with single common destination, where multiple users can relay packets for each other [25]. Through analysis and simulation, these approaches have shown that network coding can reduce system outage probability significantly. In this paper, we propose a practical joint network-channel coding scheme, called Non-Binary Joint Network-Channel Decoding (NB-JNCD) for large wireless networks. NBJNCD seamlessly couples non-binary LDPC channel coding and non-binary random linear network coding. We will first present the proposed scheme using a simple topology with two sources and two relays. After some fundamental theoretical analysis and performance evaluation, we will describe how to extend the scheme to large wireless networks. Compared with other schemes, NB-JNCD will be shown to achieve significant performance gain.

2. Related Work

Several privacy-preserving schemes have been proposed, and they can be classified into three categories: proxy-based, mix-based, and onion-based. Proxy-based schemes include Crowds and Hordes. The common characteristic of these schemes is to employ one or more network nodes to issue service requests on behalf of the originator. In Crowds, for example, servers and even crowd members cannot distinguish the originator of a service request, since it is equally likely originating from any member of the crowd. Chaum's mix based schemes include MorphMix and Mixminion. These schemes commonly apply techniques such as shaping, which divides messages into a number of fixed-sized chunks and mixing, which caches incoming messages andthen forwards them in a randomized order. These two techniques can be used to prevent attacks such as size correlation and time correlation. Onion-based schemes include Onion Routing and Onion Ring. The common feature of these schemes is to chain onion routers together to forward messages hop by hop to the intended recipient. Therefore, every intermediate onion router knows only about the router directly in front of and behind itself respectively, which can protect user privacy if one or even several intermediate onion routers are compromised. Network coding has privacy-preserving features, such as shaping, buffering, and mixing. However, network coding suffers from two primary types of attacks, pollution attacks and entropy attacks. Pollution attacks can be launched by untrusted nodes or adversaries through injecting faked messages or modifying

authentic messages, which are fatal to the whole network due to the rapid propagation of pollution. In entropy attacks, adversaries forge non-innovative packets that are linear combinations of "stale" ones, thus reducing the overall network throughput. The vulnerabilities of inter/intraflow network coding frameworks are identified, and general guidelines are provided to achieve the security.

3. Existing System

Severalnetwork coding schemes have been proposed to protect privacy against traffic analysis/flow tracingin multi-hop wireless networks. By using Homomorphicencryption Function (HEF) on Global Encoding Vector (GEV), two major schemes that provide privacy in multi-hop wireless networks are: packet flow un-traceability and message content confidentiality, for efficiently preventing traffic flow analysis. The existing system implements the random coding feature and each sink can recover the source packets by inverting the GEVs with high probability.

Random coding feature enables the random combination of outgoing packets and finally selecting an arbitrary packet for transmission. Sink decoding enables sink to decrypt the packet using decryption and then inverses the Global Encoding Matrix (GEM) to recover original messages.

Network coding allows intermediate nodes to perform computation on input messages, making output messages be the mixture of the input ones. In practical network coding, source information should be divided into blocks with h packets in each block. All coded packets related to the k^{th} block belong to generation k and random coding is only performed among the packets in the same generation. Packets within a generation need to be synchronized by buffering for the purpose of network coding at intermediate nodes. GEVs are kept confidential at intermediate nodes by encrypting the GEVs in an end-to-end manner, which can prevent compromised intermediate nodes from analyzing GEVs or recovering the original messages.
An intuitive way to resolve this issue is to keep GEVs confidential to intermediate nodes by encrypting the GEVs in an end-to-end manner, which can prevent compromised intermediate nodes from analyzing GEVs or recovering the original messages. Such an intuitive approach, however, cannot prevent the adversaries from tracking the message cipher text since the "mixing" feature of network coding will be disabled by the end-to-end encryption.

4. Proposed System

In this paper, we present a practical scheme, non-binary joint network-channel coding (NB-JNCC), for reliable communication in wireless networks. NB-JNCC seamlessly combines non-binary channel coding and random linear network coding, and uses an iterative two-tier coding scheme that we proposed to jointly exploit redundancy inside packets and across packets for error recovery. Both theory and simulation have demonstrated the significant benefits of NB-JNCC. Compared to other schemes, NB-JNCC fully exploits the spatial diversity and approaches the upper bound of outage probability with acceptable performance loss.

We plan to pursue in the following directions:

1) Jointly design channel codes, network codes, modulation and routing for improved performance.
2) Pursue tighter performance bounds on diversity and outage probability in large-scale networks.
3) Carry out performance comparisons with related schemes in various network topologies.

5.Basic Schemes

5.1 Network Coding:

Unlike other packet-forwarding systems, network coding allows intermediate nodes to perform computation on incoming messages, making outgoing messages be the mixture of incoming ones. This elegant principle implies a plethora of surprising opportunities, such as random coding. Whenever there is a transmission opportunity for an outgoing link, an outgoing packet is formed by taking a random combination of packets in the current buffer. An overview of network coding and possible applications is shown below.

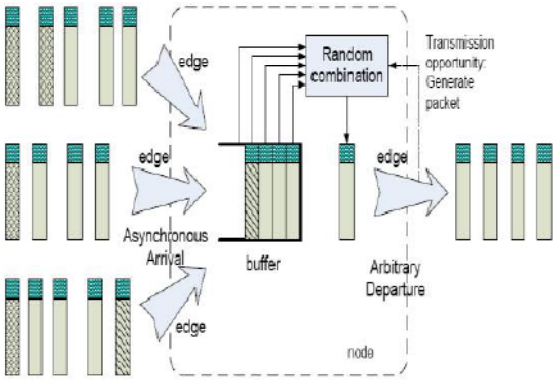


Fig 1.shows the HEF

As shown in Fig 1 Homomorphic Encryption Functions (HEFs) have the property of homomorphism, which means operations on plaintext can be performed by operating on corresponding cipher text. The HEF used for the computed function is $(f + d)$ and this can be

computed from $E(f)$and$E(d)$without knowing about the plaintextfand$d$.

A HEF needs to satisfy the following properties:

Additivity: Given the ciphertext$(f)$and(d), there exists a computationally efficient algorithm such that $(f + d) = Add(E(f), E(d))$.

Threat Models: We consider the following two attack models.

1. Outside attacker: An outside attacker can be considered as a global passive eavesdropper who has the ability to observe all network links. An outside attacker can examine the tags and message content, and thus link outgoing packets with incoming packets. Further, even if endtoend encryption is applied to messages at a higher layer, it is still possible for a global outside attacker to trace packets by analyzing and comparing the message cipher text.

2.Inside attacker: An inside attacker may compromise several intermediate nodes. Link-tolink encryption is vulnerable to inside attackers since they may already have obtained the decryption keys and thus the message plaintext can be easily recovered. Both inside and outside attackers may perform more advanced traffic analysis/flow tracing techniques, including size correlation, time correlation, and message content correlation. Adversaries can further explore these techniques to deduce the forwarding paths and thus to compromise user privacy. Without loss of generality, we assume that an anonymous secure routing protocol is deployed to assist network nodes to determine forwarding paths. The generation number of a packet can be hidden in the secure routing scheme through link-to-link encryption. In this way, attackers cannot find the generation number of a packet for their further analysis. Notice that secure routing paths are only required to be established at the beginning of each session; during the packet transmission, secure routing paths are not required to change or reestablished for each new generation.

5.2 Network Coding Based Privacy-Preserving Scheme

In this section, we propose a novel network coding based privacy-preserving scheme for MWNs, followed by theoretical analysis on the invertibility of GEMs.

1. The Proposed Privacy-Preserving Scheme: Though providing an intrinsic mixing mechanism, the original network coding cannot provide privacy guarantee due to explicit GEVs, since an adversary can recover the original messages as long as enough packets are collected. Link tolink encryption is vulnerable to inside attackers since they may already have compromised several intermediate nodes and obtained the secret keys. An intuitive way to resolve this issue is to keep GEVs confidential to intermediate nodes by encrypting the GEVs in an end-to-end manner, which can prevent compromised intermediate nodes from analyzing GEVs or recovering the original messages. Such an intuitive approach, however, cannot prevent the adversaries from tracking the message cipher text since the "mixing" feature of network coding may be disabled by the end-to-end encryption.

2.Intermediate recoding:After receiving a number of packets of the same generation, an intermediate node can perform random linear coding on these packets. To generate an outgoing packet, firstly, a random LEV $[\beta 1, \ldots . \beta n]$ is chosen independently; then, a linear combination of message content of the incoming packets is computed as the message content of the outgoing packet.

5.3 Security Analysis

The proposed scheme can provide privacy preservation by means of resisting traffic analysis/flow tracing attacks such as size correlation, time correlation, and message content correlation. Size correlation can be naturally prevented since each message is trimmed to be of the same length in network coding based schemes. Time correlation can be effectively resisted by the inherent buffering technique of network coding. Let the time length of buffering periods isT_b and the average arrival rate of coded packets be the time correlation attack can succeed only when exactly one packet arrives in the buffering periodT_b, since zero packets make the attack meaningless and more than one packet can induce the "mixing" operation, making time correlation useless. If coded packets arrive following the Poisson distribution, the probabilities of a successful time correlation attack.

1. Message content correlation:It can be resisted by the "mixing" feature of network coding. With the assistance of HEF, GEVs are kept confidential to eavesdroppers, making it difficult for adversaries to perform linear analysis on GEVs. In addition, HEF keeps the random coding feature, making the linear analysis on message content almost computationally impossible. Let the number of intercepted packets be$v$. The computational complexity for attackers to examine if a packet is a linear combination of c messages is in terms of multiplication, where l is the length of message content in terms of symbols.

2. Performance Evaluation and Optimization: In this section, we evaluate the performance of the proposed scheme in terms of invertible probability and computational overhead. A performance optimization framework is also developed to minimize the statistical computational overhead.

3. Communication Overhead: Let c messages be generated, and each message is of length l bits. For source encoding, each message is prefixed with $c$codewords from a ring of size a.Considering the cipher text expansion of the Paillier cryptosystem, we can calculate the communication overhead as2c.

4. Computational Overhead:In this proposed scheme Computational Overhead can be investigated respectively from three aspects: source encoding, intermediate recoding, and sink decoding. Since the computational overhead of the proposed scheme is closely related to the specific Homomorphic encryption algorithm, in the following analysis, we will take the Paillier cryptosystem as the encryption method when necessary. Note that the computational overhead is counted independent of the underlying network coding framework.

5. Source Encoding Overhead Consider c GEVs with $c$elements in each GEV, which form a$c \times c$ GEM. After source encoding, every element in the GEM is encrypted one by one. Thus, the computational overhead is $(c2)$ in terms of encryption operations. Every encryption operation requires 2 exponentiations, 1 multiplication, and 1 modulus operation in the Paillier cryptosystem. Therefore, the computational complexity is in terms of multiplication operations.

6. Intermediate recodingoverheadin intermediate nodes, linear transformation on the elements of GEVs can be performed only by manipulating the cipher text of these elements because intermediate nodes have no knowledge of decryption keys. According the computational complexity of producing one element in new GEVs is c exponentiations and $c-1$ multiplications on the cipher text.

7. Sink decodingoverhead:After receiving an encoded message, a sink can decrypt the elements in the GEV. According to the Paillier cryptosystem, decrypting an element requires 1 exponentiation, 1 multiplication, and 1 division operation.

5.4 Channel Model

We assume that all lossy channels suffer from slow fading. Fading keeps constant across one packet and varies from packet to packet independently (a.k.a block fading). We model the channel as Rayleigh fading with additive white Gaussian noise:

$$y = hx + w \quad (1)$$

Where$y \in C$, $x \in C$ and$w \in C$, here$y$is the received signal, the transmitted signalis x,the additive noise$w$and$h \in C$, $h$denotes the fading coefficient. Since $|h|$ follows the Rayleigh distribution, $|h|^2$ follows an exponential distribution with mean $1/\square$Thus the probability density function (pdf) of $|h|^2$ can be written as

$$p(z) = \square e^{-\square z} \left(z = |h|^2\right) \quad (2)$$

5.5 Nb-Jncd: Coding and Decoding

In the proposed NB-JNCD, we choose non-binary random linear network coding as the network coding scheme. Firstly, previous Studies in [23, 24, 27, 28, 29, and 30] have showed that random linear network coding is efficient and sufficient. Secondly, network coding performing non-binary operations on a high order Galois field can provide independent network codes with high probability. Thirdly, the randomness of such network coding scheme renders itself applicable to large networks as it allows distributed operation on each node without interrupting others. Lastly, when non-binary random linear network coding is combined with non-binary LDPC codes, the encoding and decoding procedures can be significantly simplified: bit-to-symbol conversion and its inverse is not needed and non-binary source coding and high order modulation can be unified without any conversion.

Step1:The source S_1 generates a packet u_1 with k symbols from Galois field$GF(2^q)$.

Step2: Encodes packets into x_1 using a non-binary LDPC encoder specified by a generator matrix$G_1$of size $k \times n$ as

$$x_1 = u_1 G_1 \quad (3)$$

Where x_1 and u_1 are row vectors of length n and k respectively.

Step3: Calculate channel code rate is $r_c = k/n$.

Similarly, from the above steps source S_2 can be obtained as $x_2 = u_2 G_2$, where G_2 is the code generator matrix. For simplicity, we assume that the size of G_2 is also $k \times n$. Thus the channel code rate is the same as that for source S_1.

Assume two packets x_1 and x_2 are broadcasted respectively to the relays and the sink uses orthogonal channels (at different time slots or via different frequencies). After receiving packets from the sources (recall that the channels between the sources and the relays are lossless), the relays first decode and obtain the original packets, then generate packets using network coding and non-binary LDPCchannel coding.

The two network codes at relays R_1 and R_2 are represented as

$$y_1 = \alpha_{11}u_1G_{11} + \alpha_{12}u_2G_{12},$$

$$y_2 = \alpha_{21}u_1G_{21} + \alpha_{22}u_2G_{22}, \quad (4)$$

Where the network coding coefficients $\alpha_{ij}\,(i,j=1,2)$ are drawn randomly from GF (2^q) and the generator matrices $G_{ij}\,(i,j=1,2)$ are assumed to be of size $k \times n$ Packets y_1 and y_2 will be sent to the sink from R_1 and R_2 respectively. At the sink node, four packets- x_1,x_2,y_1 and $y_2$will be received. The sink node forms a longer code as follows:

$$[x_1 \quad x_2 \quad y_1y_2] = [u_1 \quad u_2]\begin{bmatrix} G_1 & 0 & \alpha_{11}G_{11} & \alpha_{21}G_{21} \\ 0 & G_2 & \alpha_{12}G_{12} & \alpha_{22}G_{22} \end{bmatrix} \quad (5)$$

Here we assume that the network coding coefficients can be conveyed to the sink without error. The code in (5) can be viewed as an integrated channel code with packets $[u_1 \quad u_2]$ and generator matrix G' which is specified by

$$G' = \begin{bmatrix} G_1 & 0 & \alpha_{11}G_{11} & \alpha_{21}G_{21} \\ 0 & G_2 & \alpha_{12}G_{12} & \alpha_{22}G_{22} \end{bmatrix} \quad (6)$$

If we define the network code rate r_n as the percentage of direct received packets over all received packets at the sink, we will have $r_n = 2/4$ for the communication scenario. Thus, the integrated code is of rate$r = r_c \times r_n$. Given the generator matrixG', one can apply Gaussian elimination algorithm to obtain the corresponding parity check matrix H', which satisfies$H'G^T = 0$. One option for decoding is to adopt some variants of belief propagation operating on H' ;however, it is usually hard and sometimes infeasible to perform this kind of decoding as shown in figure 2.

5.6 Iterative Joint Decoding

In the proposed NB-JNCD, we choose non-binary irregular low density parity check (LDPC) codes presented in [16] as the channel Coding scheme. The rationales behind this are:

1) LDPC code can be graphically represented using factor graph.
2) The channel coding/decoding on non-binary Galois field can be seamlessly combined with the network coding/decoding.
3) The LDPC codes Presented in [26] can approach the channel capacity of non-fading channels. A non-binary LDPC is specified by a parity check matrix H of size $m \times n$ and a generator matrix G of size$k \times n$, which satisfy the relationship

$$HG^T = 0.$$

Both H and G have elements taken from GF (2^q).

We present a two-tier iterative joint network channel decoding scheme, which implements soft decoding and allows information exchange inside and across packets. We assume that all the generator matrices$G_i(i=1,2)$ and $G_{ij}\,(i,j=1,2)$ are the same, denoted as$G$. Now we can revise (5) as

$$\begin{pmatrix} x_1 \\ x_2 \\ y_1 \\ y_2 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ \alpha_{11}\alpha_{12} \\ \alpha_{21}\alpha_{22} \end{pmatrix}\begin{pmatrix} u_1 \\ u_2 \end{pmatrix} G = M \times U \times G \quad (7)$$

The left hand of (7) forms a matrix of size $4 \times n$, in which each row captures the relationship among symbols inside a packet defined by channel coding$G$, and each column captures the relationship among symbols on corresponding position of different packets defined by network coding M .Network decoding component, we use a selection updating rule. Suppose that any two rows of Mare linearly independent (this assumption holds for NB-JNCD with high probability over a high order Galois field), then any row can be represented as a linear combination of any two other rows. Thus, we can update the a priori information of symbols in a packet using extrinsic information of symbols in two other best packets (a packet is said to be better if it has smaller number of unsatisfied parity checks). Let us take the network updating of packet x_1 as an example: x_1 can be represented as a linear combination of $x_2$andy_1, $x_2$andy_2, or $y_1$and y_2. If packets x_2 andy_1 are better than packet y_2, then we will use x_2 and y_1 to update x_1. This selection updating rule can be easily generalized to any$M$. The whole decoding process can start with either channel decoding or network decoding. The decoding procedure continues round by round until all packets are correctly decoded or the maximum number of rounds is reached with a failure claimed. Except for the first round, a symbol node could combine the channel information and the updated a priori information from the network decoding component to perform channel decoding as shown figure 2. To make more illustrative let us follow the steps below.

Step1: Inputare Generate Matrices of $G_i(i=1,2)$and$G_{ij}\,(i,j=1,2)$.

Step2: Calculate the Relationship between the Channel coding G and Network coding M as shown below

$$\begin{pmatrix} x_1 \\ x_2 \\ y_1 \\ y_2 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ \alpha_{11}\alpha_{12} \\ \alpha_{21}\alpha_{22} \end{pmatrix}\begin{pmatrix} u_1 \\ u_2 \end{pmatrix} G = M \times U \times G \quad (7)$$

Step3: Use the Selection Updating rules i.e.,suppose that any two rows of mare linearly independent (this assumption holds for NB-JNCD with high probability over a high order Galois field), then any row can be represented as a linear combination of any two other rows.

Step4: Decoding Process to Channel decoding or Network Decoding.

Step5: Update the Priori Information from Network decoding and component to perform channel decoding.

Flow Chart:

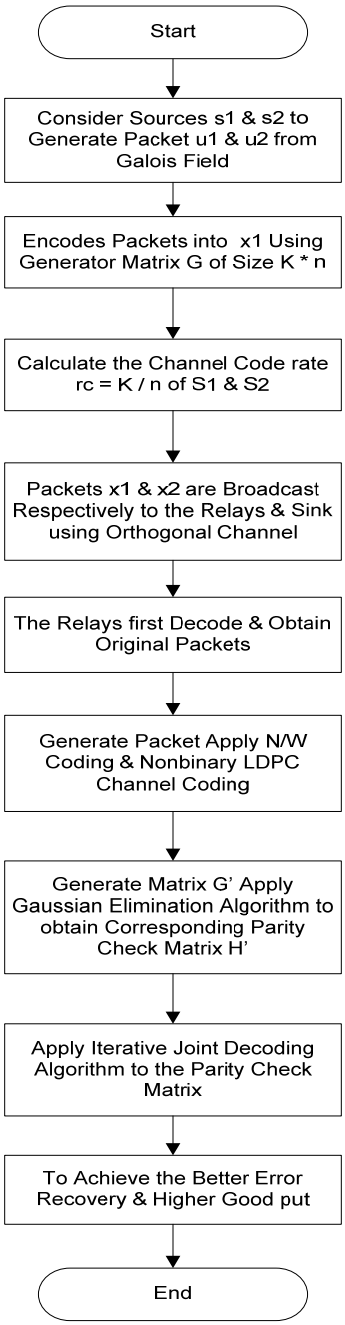


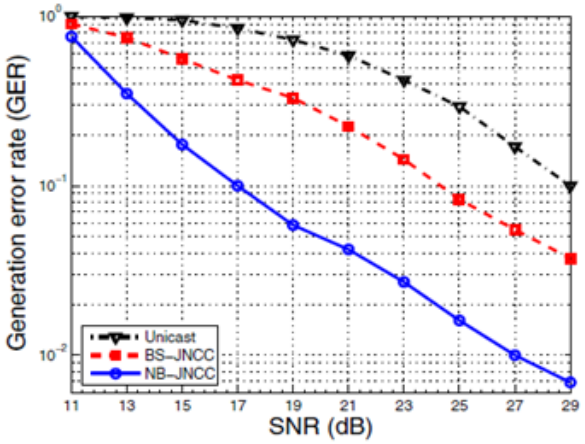
Fig2.shows of Code construction and Joint decoding scheme

6. Results

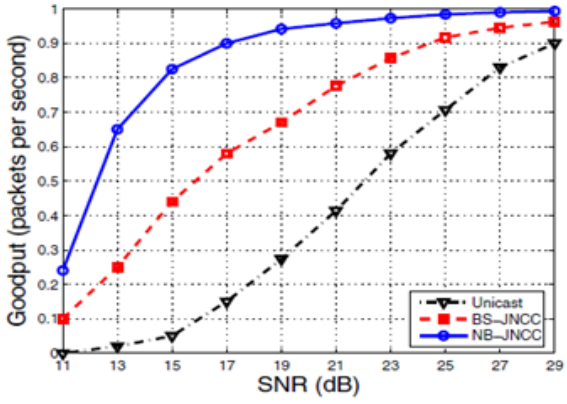
We consider the following three schemes: unicast, BS-JNCC, and NB-JNCC. Every generation contains two packets, each of k = 800 symbols over $GF(2^4)$, i.e., 4 bits in each symbol. For channel coding, the non-binary irregular LDPC code we use has average column weight of 2.8 and the channel code rate is $r_c = 0.8$. For network coding, the coefficients are randomly selected from $GF(2^4)$. Nodes in unicast only perform channel encoding and decoding. All the nodes use 16QAM modulation. The two sources generate packets with the rate of 10 packets per second (5 generations per second). We consider the following performance metrics as shown in figure 3:

• Generation error rate (GER): the number of successfully decoded generations at the sink over the total number of generations.

• Goodput (packets per second): the number of packets in successfully decoded generations at the sink per second. In this way, we ignore the packets in partially recovered generations.



(a) Generation error rate.



(b) Goodput.

Fig3. Shows the graph of generation error rate.

7.Conclusion

The proposed NB-JNCD seamlessly combines nonbinary channel coding and random linear network coding and can be directly coupled with high order modulation to provide high bandwidth efficiency, jointly design channel codes, network codes, modulation and routing for improved performance, pursue tighter performance bounds on diversity and outage probability in large scale networks and carry out performance comparisons with related schemes in various network topologies.

References:

[1] Yanfei Fan1, Jiming Chen, Xiaodong Lin, Xuemin (Sherman) Shen," Preventing Traffic Explosion and Achieving Source Unobservability in Multi-hop Wireless Networks using Network Coding".

[2] T.Venkata Ramudu, A.L.Srinivasulu,"Achieving Privacy Preservation Schemas against Traffic Analysis in Multi-Hop Wireless Networks".

[3] Tracey Ho, Member, IEEE, Muriel Médard, Senior Member, IEEE, Ralf Koetter, Senior Member, IEEE,David R. Karger, Associate Member, IEEE, Michelle Effros, Senior Member, IEEE, Jun Shi, and Ben Leong,"A Random Linear Network Coding Approach to Multicast".

[4] Ms.T.E.Janani Devi, 2Dr.S.Nagarajan,"Towards privacy preservation Against traffic analysis in Wireless networks".

[5] K. Sivakumar (HOD), S. Jenifar (PG Scholar), "Privacy Preservation against Traffic Analysis using Random Network Coding in Multi-Hop Wireless Networks".

[6] Zheng Guo, Jie Huang, Bing Wang, Member, IEEE, Shengli Zhou, Senior Member, IEEE,Jun-Hong Cui, Member, IEEE, and Peter Willett, Fellow, IEEE," A Practical Joint Network-Channel Coding Scheme for Reliable Communication in Wireless Networks-2012".

[7] Munawar Hafiz A Pattern Language for Developing Privacy Enhancing Technologies

[8] Jiri Kur,"Privacy preserving protocols for wireless sensor Networks".

[9] Zheng Guo, Jie Huang, Bing Wang, Member, IEEE, Shengli Zhou, Senior Member, IEEE,Jun-Hong Cui, Member, IEEE, and Peter Willett, Fellow, IEEE," A Practical Joint Network-Channel Coding Scheme for Reliable Communication in Wireless Networks-2012"

[10] I.F.Akyildiz,W.Su,Y.Sankarasubramaniam, and E. Cayirci. Wireless sensor networks: a survey. Computer Networks, 38:393-422, 2002.

[11] M.Grimmer, B. Ferriera, and K. Parker. Exscal: elements of an extreme scale wireless sensor network. In Embedded and Real-Time Computing Systems and Applications, 2005. Proceedings. 11th IEEE International Conference on, pages 102-108, Aug. 2005.

[12] Alan Mainwaring, David Culler, Joseph Polastre, Robert Szewczyk, and John Anderson. Wireless sensor networks for habitat monitoring. In WSNA '02: Proceedings of the 1st ACM international workshop on Wireless sensor networks and applications, pages 88{97, New York, NY,USA, 2002. ACM.

[13] Frank Stajano, Daniel Cvrcek, and Matt Lewis. Steel, cast iron and concrete: Security engineering for real world wireless sensor networks.In ACNS 2008,volume 5037 of LNCS, pages 460{478. Springer Verlag,2008.

[14] S. D. Warren and L. D. Brandeis. The right to privacy. Harvard Law Review, 4(5):193–220, December 1890.

[15] A. F. Westin. Privacy and Freedom. Atheneum, NY, 1967.

[16] R. Ahlswede, N. Cai, S.-Y. Li, and R. Yeung, "Network information flow," IEEE Trans. Inf. Theory, vol. 46, no. 4, pp. 1204–1216, Jul. 2000.

[17] I. Csiszar, "Linear codes for sources and source networks: Error exponents,universal coding," IEEE Trans. Inf. Theory, vol. IT-28, no. 4, pp.585–592, Jul. 1982.

[18] S. Lin and D. J. Costello. Error Control Coding. Prentice Hall, second edition, 2004.

[19] R. Ahlswede, N. Cai, S. R. Li, and R. W. Yeung. Network Information Flow. IEEE Transactions on Information Theory, 46(4), July 2000.

[20] S. Katti, D. Katabi, W. Hu, H. Rahul, and M. Medard. The Importance of Being Opportunistic: Practical Network Coding For Wireless Environments. In Proceedings of Allerton conference, September 2005.

[21] S. Katti, H. Rahul, W. Hu, D. Katabi, M. Medard, and J. Crowcroft. XORs in The Air: Practical Wireless Network Coding. In Proceedings of SIGCOMM, Pisa, Italy,September 2006.

[22] Y. Wu, P. A. Chou, and S.-Y. Kung. Information Exchange in Wireless Networks with Network Coding and Physical-layer Broadcast. In Proceedings of 39th Annual Conference on Information Sciences and Systemes (CISS), Baltimore, MD,USA, March 2005.

[23] Z. Guo, B. Wang, and J.-H. Cui. Efficient Error Recovery Using Network Coding in Underwater Sensor Networks. In Proceedings of IFIP Networking, pages 227–238, Atlanta,Georgia, USA, May 2007.

[24] Z. Guo, B. Wang, P. Xie, W. Zeng, and J.-H. Cui. Efficient Error Recovery with Network Coding in Underwater Sensor Networks. Ad Hoc Networks, 7(4):791–802, 2009.

[25] Y. Chen, S. Kishore, and J. Li. Wireless Diversity through Network Coding. In Proceedings of IEEE Wireless Communications and Networking Conference, Las Vegas,NV, USA, September 2006.

[26] J. Huang, S. Zhou, and P. Willett. Nonbinary LDPC Coding for Multicarrier Underwater Acoustic Communication. IEEE J. Selected Areas in Communications Special Issue on Underwater Wireless Communications and Networks,26(9):1684–1696, 2008.

[27] T. Ho, M. Medard, R. Koetter, D. Karger, M. Effros, J. Shi, and B. Leong. A Random Linear Network Coding Approach to Multicast. IEEE Transaction on Information Theory,52(10), October 2006.

[28] R. Koetter and M. Medard. An Algebraic Approach to Network Coding. IEEE/ACM Transactions on Networking,11(5):782–795, October 2003.

[29] S.-Y. R. Li, R. W. Yeung, and N. Cai. Linear Network Coding. IEEE Transactions on Information Theory,49(2):371–381, February 2003.

[30] X. Zhang, G. Neglia, J. Kurose, and D. Towsley. On the Benefits of Random Linear Coding for Unicast Applications in Disruption Tolerant Networks. In Proceedings of IEEE NETCOD, 2006.