Paper

Systematic-RLNC Based Secure and QoS Centric Routing Scheme for WSNs

Ajaykumar Notom, Sarvagya Mrinal, and Prandkar Parag

School of ECE, Reva University, Bangalore, India

https://doi.org/10.26636/jtit.2019.136219

Abstract—In this paper a highly robust and efficient systematic-random linear network coding (S-RLNC) routing scheme is proposed. Unlike classic security systems, the proposed S-RLNC transmission model incorporates an advanced pre-coding and interleaving concept followed by multi-generation mixing (MGM) based data transmission to assure secure and QoS efficient communication. The proposed S-RLNC MGM based routing scheme exhibits higher throughput (99.5-100%) than the existing NCC-ARQ-WSN protocol (80%). Unlike NCC-ARQ-WSN, the proposed model incorporates multiple enhancements, such as RLNC concept, systematic network coding, MGM concept, IBF provision and redundant packet optimization. Combined, all these optimizations have strengthened the proposed S-RLNC MGM to exhibit optimum performance for secure and QoS-centric communication over WSNs.

Keywords—multi generation mixing, systematic random linear network coding, secure communication, QoS, WSN.

1. Introduction

Recently, a novel approach, known as network coding (NC), has been proposed as a potential candidate for secure and reliable data transmission over wireless networks [1]. The NC algorithm has played a vital role in secure communication, even for MAC optimization in LTE systems. Its efficacy, combined with minimum computational overheads, had remained unexplored. NC algorithms are generally categorized into two types: systematic and non-systematic. A systematic NC algorithm exhibits partial encoding with a low rate of redundant data packet transmission. This characteristic makes it more efficient for low energy wireless communication environments. Classic practical network coding (PNC) is a linear systematic network coding algorithm that uses a fixed size of the bit sequence for secure node transmission of a single generation.

Contrary to the classic PNC, in this paper we introduce a novel Systematic-RLNC (S-RLNC) based secure, reliable and robust routing scheme for energy-efficient WSNs. Additionally, the proposed model intends to ensure higher throughput, minimum packet loss under dynamic network (link or loss) conditions to assist QoS delivery. The proposed Systematic-RLNC model exploits the key features of advanced pre-coding, compression, iterative buffer flush, multicast transmission over WSNs to ensure reliable data delivery. Unlike classic approaches, the proposed method intends to avoid processes such as data packet segmentation, encapsulation and projects input data packets (application layer) onto S-RLNC that splits it into different data chunks (samples) to be subjected to further processing with NC before transmission. In general, to perform QoS-centric (i.e. fast data transmission) communication, WSN MAC (IEEE 802.15.4) requires large size packets. Hence, the model takes all data samples and concatenates them to come up with a single packet unit which is further processed with the NC algorithm. Unlike classic PNC-based NC processing, the proposed S-RLNC solution does not encode complete data packets, but rather executes encoding over relatively smaller sizes, which significantly reduces computational overheads and reduces delay, as well as computational cost.

The article has been divided into five sections. Section 2 discusses previous research works focused on security- and energy efficiency-related algorithms. Section 3 contains details about the proposed enhanced S-RLNC assisted WSN transmission protocol. The S-RLNC MGM based WSN network with the butterfly network topology is also described in detail. Section 4 discusses the simulation results depicting packet loss, throughput, delay and energy efficiency for the proposed method. Its supremacy is underlined by comparing the proposed method with its existing counterparts. Section 5 concludes the paper.

2. Literature Review

Improvement in the efficacy of WSN functions has been improvised by employing routing methods that rely on the optimization of QoS factors, which, in turn, leads to increased power efficiency [2]. Enhanced performance of routing protocols is achieved through the optimization of QoS factors with the assistance of traffic sensitive queue management. The routing protocol was analyzed based on such QoS factors as throughput, jitter, packet delivery ratio, delay and energy consumption. Similar QoS-based routing

protocols have also been introduced to enhance overall performance of the network.

A framework capable of incorporating QoS with dissimilar security levels in WSNs and a model based on a PID controller was proposed in [4] to dynamically select the security level adapted to QoS and energy utilization levels. Steadiness factors affecting the security level and QoS are considered by employing the principle of a PID based on the past difference, the present scheme state (current) and expected scheme variation (future).

In [5], the authors concentrated on the effect of usual network attacks, on limiting energy and on the impact that poor deployment conditions of WSNs has on data transmission. They proposed a trust sensing-based secure routing mechanism (TSSRM) with lightweight features and a capability to restrict the usual attacks. The security route selection algorithm was also optimized by considering trust degree and QoS metrics.

The optimized node selection process (ONSP) method was introduced by [6] for robust multipath QoS routing for Wireless Multimedia Sensor Networks (WMSNs). This method was based on determining the optimized node that assists in resilient route discovery for enhancing QoS factors. It also extended the network's lifetime by introducing a load balancing algorithm that identifies optimized and braided pathways. These methods avoided obstructions, enhanced throughput, end-to-end delay, on-time packet delivery and extended network life span.

A secure QoS routing algorithm based on ant colony optimization (ACO) was addressed in [7], with efficient credit valuation techniques to attain better security performance. Creditworthiness of nodes was introduced as the control factor in this technique. This technique at first initializes the nodes that are not meeting QoS requirements. The set of candidate nodes is optimized. After that, the best route is found via the enhanced ACO algorithm. The technique chooses the node with a high creditworthiness level as the next hop, and is therefore able to evade a few attacks, ensuring that the optimal route offers superior dependability. Lastly, the security level of the algorithm was analyzed based on diverse network attacks.

In [8], the authors proposed a technique for employing a hybrid secure routing protocol which shows high-level scalability, security and cluster formation characteristics. The outcomes of this technique are contrasted with the LEACH protocol that helped enhance network life span. The dynamic trust management protocol in an information centric network and a delay tolerant network (DTN) was introduced in [9] for secure routing optimization. The proposed scheme was designed to recognize the malevolent node and the selfish node based on examining node energy and buffer levels, by employing the multi-hop forwarding algorithm. In the proposed scheme, the authors launched an information centric network (ICN) for validating the history of the node by computing its payoff. This approach offers a good security level and is leess time consuming. Similarly, a trust-based QoS protocol (TBQP) was developed in [10] by employing the metaheuristic genetic algorithm (GA) for optimizing and securing MANET. GA maintained QoS by choosing the fittest, i.e. the shortest route, thus delivering enhanced performance. Intelligent optimization methods or metaheuristic algorithms, such as GA, NN and those based on artificial intelligence (AI), the PSO method and simulated annealing (SA) address the QoS problems referred to above well. Ad-hoc networks suffer from the primary disadvantage concerning limiting the number of attacks against data, having the form of unauthorized data alteration and imitation caused by malicious nodes in the network.

A position based secure routing protocol (PBSRP) was presented in [11]. It is a hybrid of most forward within radius (MFR) and border node based most forward within radius (B-MFR) routing protocols. A security module was appended to this protocol by employing the station-to-station key agreement protocol in order to provide protection against different attacks. The process comprised three stages: initialization, optimum node choice and secure data delivery.

In [12], the authors proposed the energy aware routing algorithm based on clustering methods. Network leveling methods were incorporated to enhance the efficacy of clustering based on the HEED algorithm. They contrasted their proposed algorithm with basal metabolic rate (BMR) and concluded that the network life span was considerably improved and stopped the division of the network based on energy utilization equilibrium created in the network. The author of [13] employed event-based clustering algorithms to transmit data over a dissimilar geographical area, presuming that the sensor node equally shared the coordinates of the base station for identification of the nodes. Data collection and aggregation at the base station was a significant and critical task.

Paper [14] proposed a method for attaining secure MANET QoS routing in terms of QoS considerations. A novel method was presented for the ad-hoc on-demand multipath distance vector routing protocol (AOMDV) that tackled the problems of QoS, dependability and security by reducing data redundancy. Additionally, coding methods and diffusion of the original data over manifold paths have also been investigated.

Pathways from the source node to the base station in WSN algorithms have been deployed to ensure optimum energy savings [15]. Optimality is described in a constrained sense, wherein a route with a low energy requirement is used to exploit the lifetime of WSNs under dependability constraints, which means that every packet should arrive at the base station (BS) with a defined probability level. Energy efficiency was attained by choosing nodes for the multi-hop network based on the equally shared energy condition, over the entire network, after the packet arrived at the BS. To improve route dependability and robustness in multi-hop cognitive networks, context-awareness was considered in [16]. It allowed secondary consumers to choose the route in accordance with their QoS requirements. The

protocol eases the process of neighboring relay selection under dissimilar criteria, such as, for instance, direct accessible paths, route dependability and relay repute.
Novel routing as well as security-based metrics were described to gauge route robustness in spatial, frequency and temporal domains. The resources were acquired by mutually optimizing secure throughput and trading price. An end-to-end secure communication protocol based on the differentiated key pre-distribution methodology was designed in [17]. The core idea was to share dissimilar numerals of keys with dissimilar sensors to improve the buoyancy of definite connections. This characteristic was influenced during routing, where nodes were routed by higher buoyancy connections. By performing a scrupulous hypothetical study, an equation was obtained for establishing the quality of end-to-end secure communications. The equation is used to determine optimized protocol factors. A widespread performance estimation has demonstrated that the solutions are capable of offering highly secure communication between sensor and sink nodes, in arbitrarily deployed WSNs.
Paper [18] examined security threats and challenges faced by WSNs and obstructions concerning sensor security. Numerous attacks were categorized. The authors of [19] proposed a compressive security framework that provided security services for the sensor network. In addition, they appended an additional element, i.e. an intelligent security agent (ISA) to evaluate the level of security and cross layer communications. This framework is composed of such elements as an intrusion detection system, a trust framework, a key management scheme and a Link layer communication protocol.
The security issues affecting WSNs, their resource-restricted design, deployment features and security-related requirements that need to be met in order to design a secure WSN have been analyzed in [20]. The paper recognized attacks on different layers of WSNs and discussed a few countermeasures preventing those attacks. Key management, link layer and routing security were discussed as well, along with a few defensive measures applicable to WSNs.

3. The Proposed Scheme

Considering the significance of a QoS-centric and secure routing protocol for WSNs, an enhanced NC model known as systematic-random linear network coding (S-RLNC) algorithm-based transmission routing scheme is developed. Unlike in classic routing approaches, the proposed S-RLNC model intends to achieve higher throughput, minimum data drop probability, high reliability, minimum computational or signaling overheads and secure transmission, along with optimal resource (bandwidth) utilization. In terms of overall network performance and the security of transmission, the proposed S-RLNC based WSN routing protocol relies on pre-coding and interleaving-based transmission with multi-generation mixing (MGM). MGM is characterized by minimized utilization of redundant packets, which enables WSNs to offer high data transmission rates, minimum signaling overheads and good bandwidth utilization. The proposed system employs a single redundant packet (for the mixture of multiple generations) to enable complete data retrieval at the receiver that strengthens bandwidth efficiency. Furthermore, to support resource optimization, the iterative buffer flush (IBF) model is applied that significantly reduces bandwidth utilization for WSN data transmissions. Thus, the overall proposed transmission routing protocol ensures good data reliability, security and QoS assurance during transmissions over WSNs.

3.1. Pre-Coding and Interleaving

The use of RLNC augments data security across the network, which is further improved by the systematic model of transmission [21]. The S-RLNC algorithm applies RLNC to certain groups of the data packets, known as generations. Unlike classic RSA and AES types of cryptosystems, S-RLNC performs network coding over a stream of data, where new data chunks are formed based on a linear mathematical operation. In S-RLNC, the input data to be communicated over the sensor network are processed for network coding. In network coding, the input data are XOR-ed with a set of standard data, referred to as the coefficient matrix, obtained from the Galois field (GF). This ensures good security of data across the network, as only a defined receiver may retrieve the transmitted data. Unlike in classic PNC or NC-based approaches, S-RLNC augments the overall efficiency of multicast data transmission to ensure a secure and reliable real time data (RTD) transmission, particularly in those applications where data drop probability, security breaches, latency, etc. adversely affect QoS delivery. The proposed S-RLNC MGM algorithm ensures a minimum number of network-coded redundant packets (finite elliptic curve – FEC), which ensures a secure and delay-resilient RTD transmission over the WSN. The proposed redundant network coded packets offer an FEC that is better than that of the traditional repeat request (RREQ)-based mechanism relied upon to deal with packet losses [21].

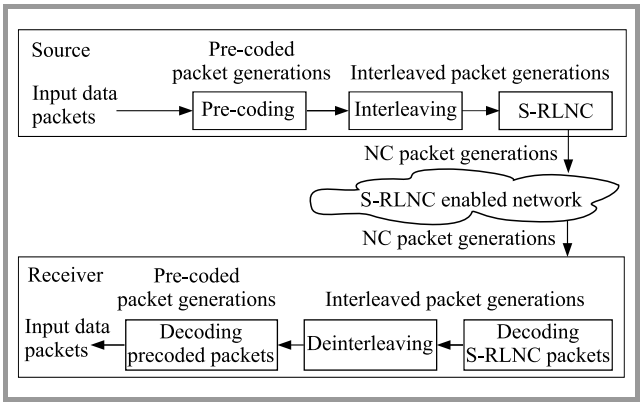

Fig. 1. Functional diagram of the proposed pre-coding and Interleaving based S-RLNC MGM model.

A brief summary of the proposed pre-coding and interleaving assisted S-RLNC algorithm is presented below.
To ensure good data security, the proposed S-RLNC algorithm uses a novel S-RLNC-assisted multicast transmission technique for QoS-centric and secure data transmission over WSNs. A snippet of the proposed S-RLNC model is depicted in Fig. 1. It shows three sequential steps of S-RLNC implementation:

- packet encoding at source node,
- packet decoding, appending and transmission at the intermediate node,
- packet decoding at sink node of a WSNs.

3.1.1. Packet Encoding at Source Node

In the proposed pre-coding scheme, the source (data) packets are combined linearly to generate a set of linear packets. Let $[X_M]_{n\times s}$ $(M = 1, 2, \ldots, m)$, where $m \geq n$ represents $n \times m$ data packets transmitted from a sensor node where an individual packet is a $1 \times s$ matrix comprising symbols from a GF of size 2^F, where F signifies the order of GF. Pre-coding generates an $m \times m$ matrix consisting of linear combinations $[Y_M]_{m\times s}$ $(M = 1, 2, \ldots, m)$, which is obtained by:

$$[Y_M]_{m\times s} = w_{m\times n}[X_M]_{n\times s} \ . \tag{1}$$

In Eq. (1), the variable w signifies the $m \times n$ part of the combination matrix (CM). In our model, to further augment the efficacy of the S-RLNC algorithm, and specifically to strengthen robustness against packet loss or security breaches, the pre-coded packet combinations have been processed for interleaving with each other. Finally, this generates $[\acute{Y}_\delta]_{m\times p}$ $(\delta = 1, 2, \ldots, m)$ such that:

$$[\acute{Y}_\delta]_{m\times s} = \gamma\big([Y_M]_{m\times s}\big) \ . \tag{2}$$

where γ is retrieved using:

$$\acute{Y}_\delta(M, w) = Y_M(\delta, w) \ . \tag{3}$$

In Eq. (3), $w(1 \leq w \leq s)$ states the location (symbol position) of a symbol in the packet.
In the proposed model, the S-RLNC algorithm is applied to the obtained matrix $\acute{Y}_\delta]_{m\times s}$ $(J = 1, 2, \ldots, m)$ which enables generating $[Z_\delta]_{1\times s}$ $(\delta = 1, 2, \ldots, m)$ with $1 \geq m$. The generations are obtained by $[Z_\delta]_{i\times s}$ $(\delta = 1, 2, \ldots, m)$, where each component of C_δ signifies a symbol pertaining to GF of 2^F. In this approach, the result is obtained based on linear packet combinations $[Z_\delta]_{1\times s}$ $(\delta = 1, 2, \ldots, m)$. It can be obtained by:

$$[Z_\delta]_{i\times s} = [C_\delta]_{i\times m} \times [\acute{Y}_\delta]_{m\times s} \ . \tag{4}$$

In Eq. (4), the $m \times 1$ generated packet combinations with $(Z_1, \ldots, Z_m)$ are obtained and indexed in the same interleaved group. In this process, each set of linear packet combinations $([C_\delta]_{1\times m}[Z_\delta]_{1\times s})$ is obtained as an outcome of a single generation. In classic NC or PNC approaches, the transmission takes place per generation, for which an individual redundant data set is required. These conventional approaches impose significantly higher bandwidth, energy consumption and signaling overheads. Therefore, to alleviate the issue of iterative redundant data transmission per generation, in this paper we have applied MGM transmission, which requires only one set of redundant packets for the data transmission of data and for successful retrieval of multiple generations.
In the S-RLNC algorithm, CM is known to all the nodes connected to the sensor network in a Multicast Group (MG), which helps retrieve or decode data at the receiver. Since CM encompasses non-zero elements, it is generated in such a manner that the overall rank of the $m \times m$ part of the CM matrix is m. This assures that each packet is combined linearly in each generation. It augments the probability of a packet combination, which is significant for all connected sensor nodes that may suffer from a loss condition due to changes in topology or network state.

3.1.2. Intermediate Nodes

Being a distributed and decentralized network, WSN comprises multiple nodes communicating in a multi-hop manner. In transmissions over WSNs, data may be subjected to multi-hop transmissions, creating vulnerability to being attacked at the neighboring node. Data may also be subjected to an attack, such as a reply attack at the neighbor node. However, QoS could be adversely affected due to unauthorized decoding of data at the intermediate node. Considering the above as a motivation, S-RPLNC introduces a novel secure processing feature that avoids unauthentic data retrieval at the intermediate node. In S-RLNC based data transmission, once the network-coded (sensor) data (referred to here as a coefficient matrix) is received from the sensor node, the intermediate node decodes the data first, and then remaining data is forwarded to the next hop. If the data is coming from the same source, it just appends or concatenates the new data and forwards it to the next hop. In other words, if the data arrives in the form of multiple packet combinations from the same packet generation, the intermediate node appends or adds packet elements of the combinations over the applied finite GF. The data packets pertaining to the same generation have the same rank and the interleaved group. Hence, S-RLNC appends, at the intermediate node, the rank and the interleaved group to the output packet combinations, before transmission. Thus, processing the data at the intermediate node is forwarded to the next hop.

3.1.3. Packet Decoding

Let the packet received at the sink node be $\big[[\hat{C}_\delta]_{\eta_\delta\times s}\big]$ with η_δ signifying the total number of linear packet combinations belonging to the δ-th S-RLNC generation. Now,

consider $[C_J]_{\eta_\delta \times m}$ $(J = 1, 2, \ldots, m)$ as CM and $[\hat{Z}_J]_{\eta_\delta \times m}$ $(J = 1, 2, \ldots, m)$ as the linear combination matrix received at the sink node. From the retrieved data combinations, the sink node selects m linearly independent combinations from each generation. The linear combinations selected are obtained by:

$$\left[[\hat{C}_\delta]_{m\times m}[\hat{Z}_\delta]_{m\times s}\right] = \kappa\Big(\left[[\hat{C}_\delta]_{\eta_\delta \times m}[\hat{Z}_\delta]_{\eta_\delta \times s}\right]\Big) \ . \quad (5)$$

In Eq. (5), parameter κ is used to select m linearly independent combinations from the δ-th generation, when $\eta_\delta \geq m$. This is done only when the sink has received m combinations from η_δ linear packet combinations. It is then followed by the selection of packet combinations and coefficients from δ-th generation to obtain the interleaved generation using:

$$\left[\hat{Y}_\delta\right]_{m\times m} = \left[\widehat{C_\delta}\right]_{m\times m}^{-1} \cdot \left[\widehat{Z_\delta}\right]_{m\times s} \ . \quad (6)$$

In the proposed transmission model, m interleaved generations belonging to an interleaved group are at first ordered in sequence of the rank value. This sequence is then processed for de-interleaving (Fig. 1) to generate pre-coded symbols (in that generation). It is represented by:

$$[\hat{Y}_M] = \bar{Y}\left[\hat{Y}_\delta\right]_{m\times s} \ . \quad (7)$$

The $\bar{Y}$ is obtained from:

$$[\hat{Y}_M] = (\delta, w) = \hat{\hat{Y}}_\delta(M, w) \ . \quad (8)$$

To augment computational efficacy, in the proposed S-RLNC model, the n packet combinations from each m group of de-interleaved combinations belonging to a pre-coded generation are considered along with their respective coefficient information. Consider that the selected coefficients and combinations be $[\omega_M]_{n\times n}[\hat{Y}_M]_{m\times s}$, then the original packets are decoded by:

$$[\hat{X}_M]_{n\times s} = [\omega_M]_{n\times n}{}^{-1}[\hat{Y}_M]_{n\times s} \ . \quad (9)$$

3.2. MGM Assisted S-RLNC

To ensure a QoS-centric and secure routing protocol for WSNs, S-RLNC employs MGM in which multiple generations are gathered and converted into groups. The data belonging to the group are processed for mixing into different groups [22]. To perform a multicast transmission, S-RLNC MGM considers z generation transmissions simultaneously. The overall functional schematic of the S-RLNC MGM model is depicted in Fig. 2. As already stated, in the proposed model, for each generation we have assigned a position index which is appended in CM before the transmission. Considering l as the initial generation and z as the final generation, the position index d exists between 1 and z $(1 \leq d \leq z)$.

In practice, the source sensor node, at first, performs linear combination of the initial d,n number of sensed packets

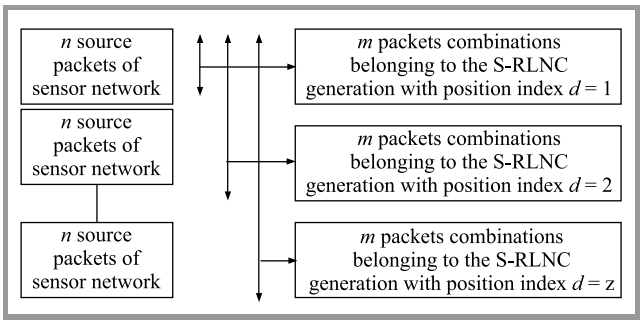

Fig. 2. S-RLNC MGM based secure data transmission over WSNs.

to form d,m linear combinations. To enable secure and efficient data delivery over WSNs to the sink under the likelihood of data losses, $z.(m-n)$ additional packets are transmitted as redundant packets. Let $[X_d]_{n\times s}$ be the N sensed data belonging to the d-th generation in CM, in which each source packet signifies a $1\times s$ matrix of symbols retrieved from the finite field $(2^F, F = 4, 9, 16\ldots)$, where F states the order of the GF. In the proposed routing model, at the source node, $A[C]_{m\times(d,n)}$ matrix with rank d,n is retrieved through a variable belonging to the same GF 2^F. The total number of output packets generated from d-th CM is estimated by:

$$[Y]_{m\times s} = [C]_{m\times(d.n)} \cdot [X]_{(d.n)\times s} \ . \quad (10)$$

In an MGM-based transmission, the estimated m combinations pertaining to $d\cdot z$ S-RLNC generations are transmitted from the source sensor node. Once data is received at sink node, it decodes the $d.n$ S-RLNC-MGM packets, where the rank of the CM obtained from the initial generations remains the same as $d.n$.

Let $d.n$ distinctive data packets be $\left[[\hat{C}_{(d.n)\times(d.n)}[\hat{Y}]_{(d.n)\times s}\right]$ with $[\hat{C}]_{(d.n)\times(d.n)}$ as the coefficients used for generating $[\hat{Y}]_{(d.n)\times s}$ packets. The data packets are decoded at the sink node using:

$$[\hat{X}_{d.n\times s} = [\hat{C}]^{-1}_{(d.n)\times(d.n)} \cdot [\hat{Y}]_{d.n\times s} \ . \quad (11)$$

WSNs often experience network condition changes and, hence, become vulnerable to packet loss. Under such circumstances, the S-RLNC-MGM model transmits only $m-n$ redundant packets from d generations, which helps decode a complete set of data at the sink node. Therefore, unlike classic $z.(m-n)$ packets, S-RLNC MGM requires merely $m-n$ redundant packets to decode all data successfully. This significantly reduces energy consumption, bandwidth utilization and signaling overheads. Once the data has been successfully retrieved at the receiver, S-RLNC MGM flushes the buffers to accommodate remaining data, which makes the proposed routing protocol bandwidth efficient. Additionally, it improves reliability of RTD transmission.

In practice, WSNs are often subjected to attacks, with eavesdroppers trying to manipulate data before it reached

its destination. Additionally, due to changes in the network state, the probability of data loss increases. Recent events prove that the eavesdroppers identify data or type of content in order to attack the transmission system, eventually leading to huge data losses and QoS violations. Under such circumstances, in order to ensure secure data transmission, the proposed S-RLNC MGM routing model relies on a network- and content-aware transmission scheduling scheme. In the proposed network- and content-aware transmission scheduling model, redundant packets are distributed in a manner that enables complete data decoding while maintaining minimum redundant packet demands. Considering the loss probability under attack conditions, in order to further enhance the proposed routing protocol, the S-RLNC MGM algorithm applies an enhanced redundant packet allocation strategy to ensure maximum or complete data decoding at the receiver.

In the proposed routing protocol, the source node retrieves event or sensed data from the application layer of an IEEE standard 802.15.4 protocol stack and prepares coded packets for further transmission. This is done in sets of $\sum_{d=1}^{z}$ network coded packets with z generations, where n_d represents total source packets pertaining to d-th generation. In this model, each source packet contains coefficients from finite field 2^F. As already discussed in previous sections, the sensed packets (also known as source packets) are combined linearly using the variables chosen from a similar GF, to generate $\sum_{d=1}^{z} m_d$ S-RLNC packets pertaining to the multiple generations $g_1, g_2, \ldots, g_z$, where m_d states the total number of coded packets from g_d generation. Here, m_d packets are obtained from the g_d-th generation by linearly combining initial $\sum_{v=1}^{d} n_v$ source packets. In this manner, the probability of decoding for the coded packets (m_d) generated for the g_d generation can be obtained. Let the likelihood of S-RLNC MGM coded packet reaching the sink be:

$$\alpha_{avg} = \frac{\sum_{v=1}^{\varphi} \alpha_v}{\varphi} \ . \tag{12}$$

Under any loss conditions, the data from g_d and previous generations $g_1, \ldots, g_{d-1}$ may be decoded only when $\sum_{v=1}^{d} n_v$ linearly dependent packet combinations reaches to the sink from all $g_1, \ldots, g_d$ generations. This overall mechanism assists the sink node in decoding data from each generations $g_1, \ldots, g_d$ if g_d (where $0 \le d \le d$), is decoded successfully and $\sum_{v=d+1}^{d} n_v$ linearly independent coded packets are received from $g_{d+1}, \ldots, g_d$ generations.

Let the likelihood of decoding packets from g_d be ς_d. Then, it is assumed that a sufficiently large finite field size (GF) is considered for CM generation. Under such circumstances, with $d = 1$, ς_1, becomes equal to the likelihood of receiving minimal n_1 coded packets out of the transmitted m_1 coded packets from generation g_1:

$$P_{dec}(n, m, \alpha_{avg}) = \sum_{v=n}^{m} \binom{m}{v} \alpha_{avg}^{v} (1 - \alpha_{avg})^{m-v} \ , \tag{13}$$

$$\varsigma_1 = P(n_1, m_1, \alpha_{avg}) \ . \tag{14}$$

Similarly, ς_2 is equal to the probability of retrieving the minimum of n_2 packets from g_2 generation, provided g_1 is decoded completely. Furthermore, g_1 and g_2 are decoded under the condition that the sum of $N-1+n_2$ packet combinations is retrieved from their corresponding generations. Finally, *varsigma*$_2$ is obtained as:

$$\varsigma_2 = \varsigma_1 . P(n_1, m_1, \alpha_{avg}) + (1 - \varsigma_1) . P\left(\sum_{v=1}^{2} n_v , \sum_{v=1}^{2} m_v , \ \alpha_{avg} \right) . \tag{15}$$

Now, ς_d is transformed into a more generalized form:

$$\varsigma_d = \begin{cases} P(n_1, m_1, \alpha_{avg}) & ; \ d = 1 \\ \left\{ \varsigma_{d-1} . P(n_d, m_d, \alpha_{avg}) + \sum_{v=1}^{d-1} \left[\varsigma_{d-v-1} \cdot \prod_{w=d-v}^{d-1} \left((1 - \varsigma_k) . P\left(\sum_{w=d-1}^{d} n_w , \sum_{w-d-1}^{d} m_w, \alpha_{avg} \right) \right) \right] \right\} & ; \ d \ge 1 , \end{cases} \tag{16}$$

where $\varsigma_0 = 1$.

g_d could be decoded only when $\sum_{v=d}^{d} n_v$ linearly independent packets are obtained from $g_d, \ldots, g_{\tilde{d}}$ generations, where $d \le \tilde{d} \le z$, the decoding probability for g_d be ρ_d, then with $d = z$ and:

$$\rho_z = \varsigma_z \ . \tag{17}$$

Meanwhile, for $d = z - 1$, the decoding probability is:

$$\rho_{z-1} = \varsigma_{z-1} + (1 - \varsigma_{z-1}) . \varsigma_z \ . \tag{18}$$

When $d = 1$, then expression is represented by:

$$\rho_1 = \varsigma_1 + (1 - \varsigma_1) . \varsigma_2 + \ldots + (1 - \varsigma_1) \ldots (1 - \varsigma_{z-1}) \varsigma_z \ . \tag{19}$$

By applying Eqs. (17)–(19), a generalized form for the packet decoding probability is derived and represented by:

$$\rho_d = \begin{cases} \varsigma_d & ; \ d = z \\ \varsigma_d + \sum_{v=d+1}^{z} \left[\varsigma_v \cdot \prod_{w=d}^{v-1} (1 - \varsigma_w) \right] & ; \ d < z \end{cases} . \tag{20}$$

The average decoding probability $\bar{\rho}$ can be obtained by:

$$\bar{\rho} = \frac{\sum_{d=1}^{z} \rho_d}{z} \ . \tag{21}$$

In the proposed model, $m_1, m_2, \ldots, m_z$ uses the probability of decoding with $\mathrm{Max}(\bar{\rho})$ such that:

$$\sum_{d=1}^{z} (m_d) = R, \tag{22}$$

where R refers to the addition of all packet combinations.

4. Results and Discussion

Based on the previous section, a 5-nodes model is designed using the S-RLNC MGM technique, which is discussed in this section. Considering transmission security, the proposed S-RLNC MGM model assures that only the recipient of the transmitted packet decodes the data using specified credentials and a specific position index (in combination matrix of the received combination set). Considering varying network loss patterns under dynamic WSNs, the Gilbert-Elliot model (GEM) has been applied in this paper, and overall performance has been assessed with varying loss probabilities.

In simulations, the loss pattern varied from 0.005 to 0.5. Under a loss probability (or condition), in order to increase data rate at the receiver end, an increase in the number of redundant packets is generally suggested. However, it functions at the cost of increased signaling overheads, energy consumption and bandwidth utilization. All these factors adversely affect QoS of WSNs. In order to alleviate such issues, this paper proposes a redundant packet allocation strategy. To assess its efficacy, we simulated a developed model with varying redundant packets and found that the proposed routing protocol shows an almost 100% packet decoding rate with only 2 redundant packets per S-RLNC MGM combination matrix transmission or combination set at the sink node. The results obtained are presented in Fig. 3.

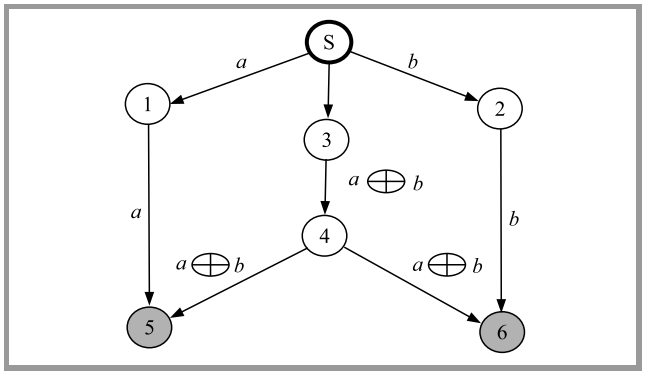

Fig. 3. S-RLNC MGM based WSN network with a butterfly network topology.

The security of S-RLNC depends primarily on the depth or length of GF. However, higher GF often imposes huge computational and processing time costs. Hence, we have examined the performance of the S-RLNC MGM model with GF = 8 and GF = 16. The results obtained indicates that the proposed transmission model could ensure satisfactory performance with GF = 8. To simulate the proposed routing model, we have applied a butterfly architecture-based RLNC with six nodes distributed across the network. The applied network model comprises a single source node, intermediate nodes and a sink node. The S-RLNC MGM model is assessed for both unicast and multicast transmissions over WSNs.

An illustration of the deployed network pattern is given in Fig. 3. The source node is marked by "S", while intermediate nodes are represented by numbers 1 to 4, and the sink nodes are represented by numbers 5–6. Thus, the simulated model signifies both unicast transmission (source S to nodes *a* and *b*; node S to 3, nodes 3–4, nodes 1–5, nodes mbox2–6) and multicast transmission (node 4 to nodes 5–6). Here, nodes 5–6 are considered to be sink nodes and, hence, throughput and packet loss are estimated at these nodes to assess performance. The proposed routing model is developed and simulated with the use of Matlab software.

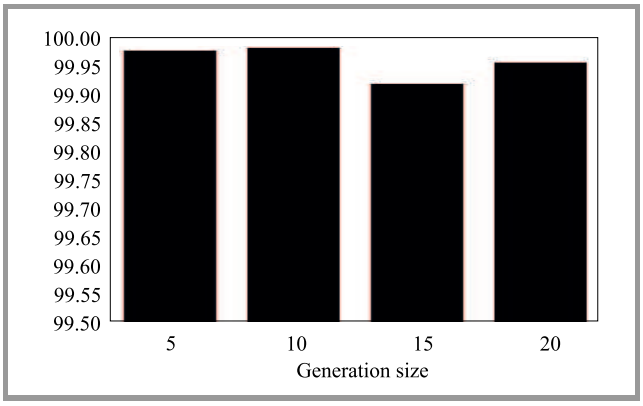

Fig. 4. Throughput of the S-RLNC MGM model with GF = 8.

Figure 4 shows the throughput performance of the proposed S-RLNC MGM model. The maximum throughput of the packet delivery rate is 99.95%, which is more than in the classic NC-based WSN routing protocol [23]. The efficacy of the proposed routing model under varying load conditions (packet generation size which signifies the number of packets transmitted per generation) is assessed. In Figs. 4–9, x axis shows the number of packets generated per generation. Since an increase in the number of packets per generation might affect the efficiency at the receiver, we have varied the generation size to examine performance. Additionally, a higher generation size ensures a high data transmission rate. With this motivation in mind, performance of the proposed S-RLNC MGM model is examined with different packet sizes. Figure 4 shows throughput with

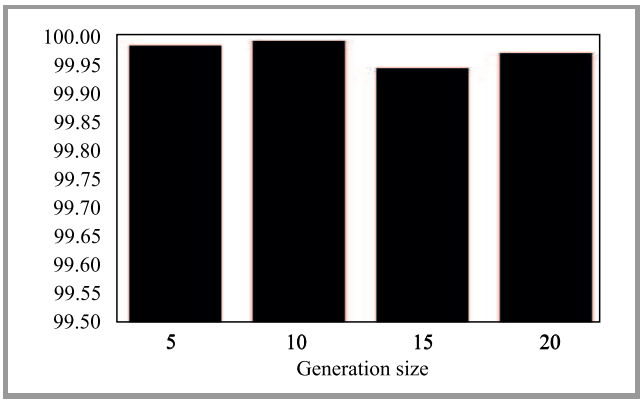

Fig. 5. Throughput of the S-RLNC MGM model with GF = 16.

GF = 8 to generate initial CM, while the throughput with GF = 16 is shown in Fig. 5. Based on the results, one may conclude that the proposed routing model shows a similar finite field size. Therefore, for real-time applications, the protocol could rely on GF = 8, as this would significantly reduce computational overheads and latency.

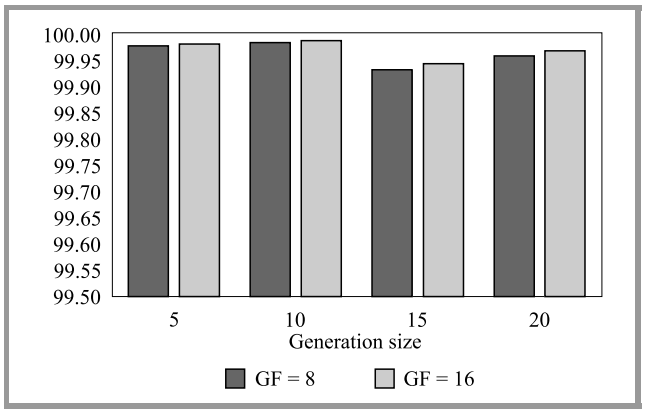

Fig. 6. Throughput performance with GF = 8 and 16.

Figures 7 and 8 show packet loss ratio or drop rate at the receiver or sink under different packet generation size and GF conditions. The proposed routing model exhibits the minimum packet loss at the generation size of 10 with GF = 8. This means a packet loss of nearly 1.5% packet loss, while the maximum loss occurs at 15 packets per generation (6.5%). Noticeably, the loss rate is obtained as an average of the losses observed at nodes 5–6. To the contrary, S-RLNC MGM with GF = 16 exhibits the minimum packet loss at generation size of 10. Based on overall results, it may be estimated that the proposed routing model offers better performance with 10 packets per generation, as this enables the achievement of an optimum or maximum data decoding rate at the sink.

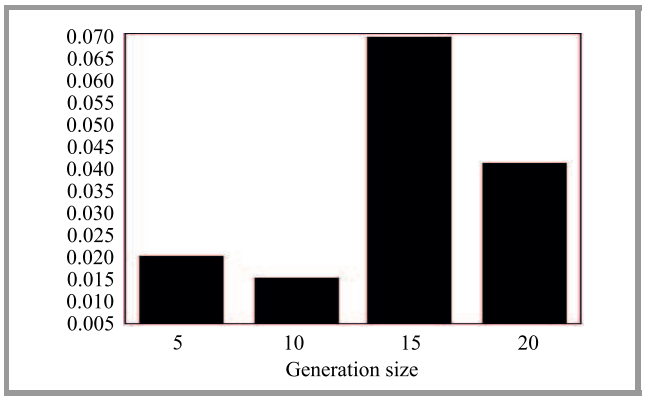

Fig. 7. Packet loss ratio of the S-RLNC MGM model with GF = 8.

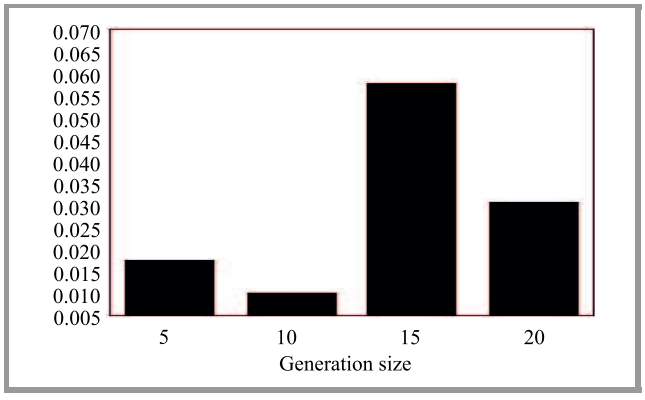

Fig. 8. Packet loss ratio of the S-RLNC MGM model with GF = 16.

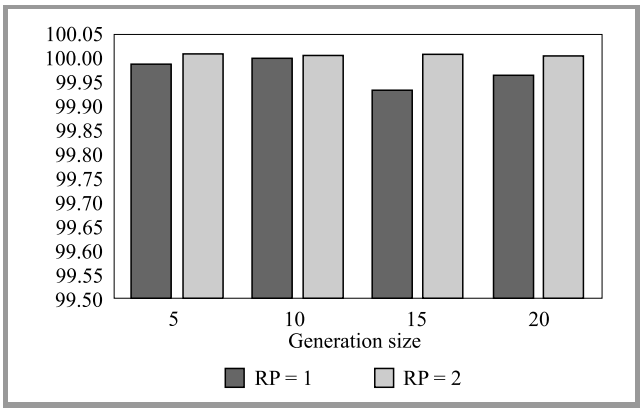

Fig. 9. Throughput of the S-RLNC MGM model with redundant packets 1 and 2 over varying generation size (GF = 8).

Next, we examined the performance of the proposed routing protocol with 1 and 2 redundant packets per combination set transmission (with all *m* generations). The results (Fig. 9) show that the proposed S-RLNC MGM based routing protocol may ensure an almost 100% successful data delivery rate, even at 2 redundant packets per generation.

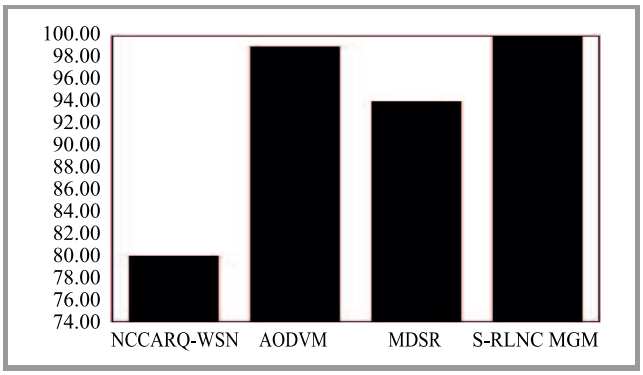

Fig. 10. Comparative performance of the proposed S-RLNC MGM model and existing protocols.

In order to compare performance (Fig. 10) with that of the exiting approaches, we have compared the performance of S-RLNC MGM with the network coding-based cooperative automatic repeat request MAC protocol for WSN (NCC-ARQ-WSN) routing scheme [23]. NCC-ARQ-WSN focuses on enabling IEEE 802.15.4 stations to establish request cooperation between neighboring nodes after receiving any erroneous data. Here, the motive was to inform neighboring nodes about receiving erroneous data. Addi-

tionally, NCC-ARQ-WSN applied NC over the data before relaying it to the neighboring node. NCC-ARQ-WSN applied the classic NC scheme that suffers from significantly higher computational overheads and signaling costs. In addition, the S-RLNC MGM routing model has exhibited better performance than AODVM and MSDR [24].

5. Conclusions

In major, real-time communication schemes relying on WSNs, signaling overheads, retransmission and energy consumption are the key issues that need to be taken into consideration. The proposed routing model intended to deal with all these challenges by incorporating systematic network coding, random linear coding, MGM and IBF. One noticeable novelty of the proposed systematic RLNC is that it avoids encoding all source data, which eventually reduces computational cost and end-to-end delay. Furthermore, unlike classic ACK-based feedback systems, it ensures that the transmitted data reaches the sink node and, hence, guarantees more reliable transmission without imposing additional signaling costs. The use of the MGM scheme reduces the number of additional redundant packets fostering successful data retrieval at the receiver. This not only reduces computational cost and energy consumption, but also mitigates bandwidth utilization. All these novelties allow the proposed system to achieve better QoS and guarantee higher transmission security levels.

References

[1] V. Patil, S. Gupta, and C. Keshavamurthy, "An enhanced network coding based mac optimization model for QoS oriented multicast transmission over LTE networks", *Int. J. of Com. Science and Inform. Secur.* (*IJCSIS*), paper ID 301116206, pp. 843–851, 2016 [Online]. Available: https://www.academia.edu/31261832/An_Enhanced_Network_Coding_Based_MAC_Optimization_Model_for_QoS_Oriented_Multicast_Transmission_Over_LTE_Networks

[2] K. Dhote and G. M. Asutkar, "Optimization of routing techniques in wireless sensor network using queue management", in *Proc. Devices for Integrated Circuit DevIC 2017*, Kalyani, India, 2017, pp. 500–504 (doi: 10.1109/DEVIC.2017.8074000).

[3] G. Kalnoor and J. Agarkhed, "QoS based multipath routing for intrusion detection of sinkhole attack in wireless sensor networks", in *Proc. Int. Conf. on Circ., Power and Comput. Technol. ICCPCT 2016*, Nagercoil, India, 2016 (doi: 10.1109/ICCPCT.2016.7530341).

[4] A. Rachedi and A. Hasnaoui, "Security with Quality-of-Services optimization in Wireless Sensor Networks", in Proc. 9th Int. Wirel. Commun. and Mob. Compu. Conf. IWCMC 2013, Sardinia, Italy, 2013, pp. 1319–1324 (doi: 10.1109/IWCMC.2013.6583747).

[5] D. Qin *et al.*, "Research on trust sensing based secure routing mechanism for wireless sensor network", *IEEE Access*, vol. 5, pp. 9599–9609, 2017 (doi: 10.1109/ACCESS.2017.2706973).

[6] A. Alanazi and K. Elleithy, "Optimized Node Selection Process for quality of service provisioning over wireless multimedia sensor networks", in *Proc. 2nd Int. Conf. on Mob. and Secure Serv. MobiSecServ 2016*, Gainesville, FL, USA, 2016 (doi: 10.1109/MOBISECSERV.2016.7440227).

[7] Q. Shi and Z. Li, "A secure QoS Routing Algorithm Based on ACO for Wireless Sensor Network", in *Proc. IEEE 10th Int. Conf. on High Perform. Comput. and Commun. & IEEE Int. Conf. on Embedd. and Ubiquit. Comput.*, Zhangjiajie, China, 2013, pp. 1241–1245 (doi: 10.1109/HPCC.and.EUC.2013.176).

[8] C. Deepa and B. Latha, "HHCS: Hybrid hierarchical cluster based secure routing protocol for Wireless Sensor Networks", in *Proc. Int. Conf. on Inform. Commun. and Embedd. Sys. ICICES 2014*, Chennai, India, 2014 (doi: 10.1109/ICICES.2014.7033805).

[9] M. Malathi and S. Jayashri, "Design and performance of dynamic trust management for secure routing protocol", in *Proc. IEEE Int. Conf. on Adv. in Comp. Appl. ICACA 2016*, Coimbatore, India, 2016, pp. 121–124 (doi: 10.1109/ICACA.2016.7887935).

[10] S. Zafar and M. K. Soni, "Trust based QOS protocol(TBQP) using meta-heuristic genetic algorithm for optimizing and securing MANET", in *Proc. Int. Conf. on Reliabil. Optimiz. and Information Technol. ICROIT 2014*, Faridabad, India, 2014, pp. 173–177 (doi: 10.1109/ICROIT.2014.6798315).

[11] S. K. Bhoi and P. M. Khilar, "A secure routing protocol for Vehicular Ad Hoc Network to provide ITS services", in *Proc. Int. Conf. on Commun. and Sig. Process*., Melmaruvathur, India, 2013, pp. 1170–1174 (doi: 10.1109/iccsp.2013.6577240).

[12] Z. Abolfazli and M. Mahdavi, "A homogeneous wireless sensor network routing algorithm: An energy aware cluster based approach", in *Proc. 22nd Iranian Conf. on Elec. Engin. ICEE 2014*, Tehran, Iran, 2014, pp. 1717–1722 (doi: 10.1109/IranianCEE.2014.6999815).

[13] A. Tripathi, N. Yadav, and R. Dadhich, "Secure-SPIN with cluster for data centric wireless sensor networks", in *Proc. 50th Int. Conf. on Adv. Compu. & Commun. Technol*., Haryana, India, 2015, pp. 347–351 (doi: 10.1109/ACCT.2015.26).

[14] S. Sedaghat, F. Adibniya, and V. Derhami, "A mechanism-based QoS and security requirements consideration for MANETs QoS routing", in *Proc. 6th Int. Symp. on Telecommun. IST 2012*, Tehran, Iran, 2012, pp. 1123–1128 (doi: 10.1109/ISTEL.2012.6483155).

[15] J. Levendovszky and H. N. Thai, "Quality-of-Service routing protocol for Wireless Sensor Networks", *J. of Inform. Technol. Softw. Engin.*, vol. 4, no. 2, 2015 (doi: 10.4172/2165-7866.1000133).

[16] B. Lorenzo, I. Kovacevic, F. J. Gonzalez-Castano, and J. C. Burguillo, "Exploiting context-awareness for secure spectrum trading in multi-hop cognitive cellular networks", in *Proc. IEEE Globecom Worksh. GC Wkshps 2015*, San Diego, CA, USA, 2015 (doi: 10.1109/GLOCOMW.2015.7413995).

[17] W. Gu, N. Dutta, S. Chellappan, and X. Bai, "Providing end-to-end secure communications in wireless sensor networks", *IEEE Trans. on Netw. and Serv. Manag.*, vol. 8, no. 3, pp. 2015–218, 2011 (doi: 10.1109/TNSM.2011.072611.100080).

[18] M. Roopak, T. Bhardwaj, S. Soni, and G. Batra, "Review of threats in Wireless Sensor Networks", *Int. J. of Comp. Sci. and Inform. Technol.* (*IJCSIT*), vol. 5, no. 1, pp. 25–31, 2014 [Online]. Available: http://ijcsit.com/docs/Volume 5/vol5issue01/ijcsit2014050106.pdf

[19] K. Sharma, M. K. Ghose, and Kuldeep, "Complete security framework for Wireless Sensor Networks", *Int. J. of Comp. Sci. and Inform. Secur*. (*IJCSIS*), vol. 3, no. 1, 2009 [Online]. Available: https://arxiv.org/ftp/arxiv/papers/0908/0908.0122.pdf

[20] J. Rehana, "Security of Wireless Sensor Network", TKK T-110.5190 Seminar on Internetworking, 2009 [Online]. Available: http://www.cse.tkk.fi/en/publications/B/5/papers/Rehana_final.pdf

[21] S. Jaggi *et al.*, "Resilient network coding in the presence of Byzantine adversaries", in *Proc. 26th IEEE Int. Conf. on Comp. Commun. INFOCOM 2007*, Barcelona, Spain, 2007, pp. 616–624 (doi: 10.1109/INFOCOM.2007.78).

[22] M. Halloush and H. Radha, "Network coding with multi-generation mixing: a generalized framework for practical network coding", *IEEE Trans. on Wirel. Commun.*, vol. 10, no. 2, pp. 466–473, 2011 (doi: 10.1109/TWC.2011.120810.090280).

[23] A. Antonopoulos and C. Verikoukis, "Network coding-based cooperative ARQ medium access control protocol for Wireless Sensor Networks", *Int. J. of Distrib. Sensor Netw.*, vol. 8, no. 1, 2012 (doi: 10.1155/2012/601321).

[24] B. Sun, Y. Song, C. Gui, and T. Zhang, "Performance of Network Coding Based Multipath Routing in Wireless Sensor Networks", *Int. J. of Comp. Sci. (IJCSI)*, vol. 9, issue 6, no 2, pp. 182–187, 2012 [Online]. Available: https://pdfs.semanticscholar.org/ba24/0f1e5aed473b8641b987da440cf214ed532f.pdf

Ajaykumar Notom is currently a lecturer at BGS Polytechnic, Chikkaballapur, Bangalore, India. He is pursuing his Ph.D. at REVA University, Bangalore, focusing on security-related aspects of Wireless Sensor Networks. He has published several Scopus-indexed journals and conference papers, as well as IEEE conference papers.

https://orcid.org/0000-0002-5220-8650
E-mail: ajaykumarnotom@gmail.com
School of ECE
Reva University
Bangalore, India

Parag Parandkar is an Associate Professor at the School of Electronics and Communication Engineering, REVA University, Bangalore, India. He is a life member of the Institute of Electronics and Telecommunication Engineers and a member of IEEE. He has been on organizing committees of various national and international symposiums, expert lectures, seminars and short term courses, and has delivered numerous courses and pursued other related academic activities.

https://orcid.org/0000-0003-4430-2580
E-mail: mrinalsarvagya@gmail.com
School of ECE
Reva University
Bangalore, India

Mrinal Sarvagya holds a Ph.D. in Wireless Communication and an M.Tech. degree in Digital Communication from IIT Kanpur, as well as a B.E. degree in electronics and communication engineering from Government Engineering College, Ujjain. She is a member of such professional bodies as WIE, IEEE, IETE, and IEEE ComSOC. She has 23 years of teaching experience, with expertise in various subjects, like wireless communication, advanced digital communication, computer communication and networking, channel estimation and modeling, ad-hoc wireless networks, protocol engineering. Her areas of research focus on wireless communication, channel equalization in OFDM-IDMA/SCM receivers, and cognitive radio networks.

https://orcid.org/0000-0002-3552-3210
E-mail: parag.vlsi@gmail.com
School of ECE
Reva University
Bangalore, India