Computers and Electrical Engineering 87 (2020) 106774

Contents lists available at ScienceDirect

Computers and Electrical Engineering

journal homepage: www.elsevier.com/locate/compeleceng

Efficient and secure multi-homed systems based on binary random linear network coding☆

Reem Melki[a,*], Hassan N. Noura[b], Ali Chehab[a]

[a] American University of Beirut, Department of Electrical and Computer Engineering, Lebanon
[b] Arab Open University, Faculty of Computer Studies, Lebanon

ARTICLE INFO

Article history:
Received 18 April 2019
Revised 4 July 2020
Accepted 13 July 2020

Keywords:
Binary RLNC
Data confidentiality
Source authentication
Invertibility
Dynamic cryptographic algorithms
Multi-homed systems

ABSTRACT

Recently, multi-homing has received a lot of interest, since it enables devices which are currently equipped with multiple network interfaces to transmit data over multiple paths, simultaneously. However, with parallel transmission over heterogeneous links, issues and challenges related to security arise. In this paper, we propose a novel channel-based security solution to enhance the security of multi-homed systems. Unlike existing techniques in the literature, the proposed scheme utilizes simple cryptographic operations and Random Linear Network Coding (RNLC), to ensure better robustness against attacks, and improve the performance and reliability of transmitted messages, concurrently. In particular, channel-based parameters are combined with a master secret key, only known to communicating entities, to derive dynamic cipher primitives, which include substitution tables, permutation tables and binary RNLC matrices. The theoretical and experimental results showed that the proposed scheme is secure and efficient compared with many work in this field.

1. Introduction

In the last decade, the rapid increase in the number of hand-held devices and the tremendous growth in data traffic, have triggered major shifts towards new technologies and applications that support high data-rate and low-latency communication. Nevertheless, the heterogeneous nature of communication systems exerted huge pressure on the current network infrastructure in terms of computational power, energy and network resources, which led to additional challenges [1]. Consequently, Network Coding (NC) has emerged as a promising candidate to improve the behavior of wireless networks, increase the overall system throughput, and to solve the problem of network traffic. This technology possesses significant advantages over simple routing since it allows participating nodes in a network to encode incoming data packets instead of simply forwarding them, which achieves maximum information flow in multicast networks and reduces end-to-end delay [2].

Random Linear Network Coding (RLNC), which is an advanced NC scheme, is a simple yet powerful technique that is able to approach system capacity with negligible feedback overhead. More specifically, intermediate nodes perform linear encoding by randomly combining multiple incoming packets using local encoding coefficients, and then, relaying the resulting

☆ This paper is for regular issues of CAEE. Reviews processed and recommended for publication to the Editor-in-Chief by Area Editor Dr. G. Martinez Perez.

* Corresponding author.
E-mail addresses: rmm71@aub.edu.lb (R. Melki), hnoura@aou.edu.lb (H.N. Noura), chehab@aub.edu.lb (A. Chehab).

https://doi.org/10.1016/j.compeleceng.2020.106774

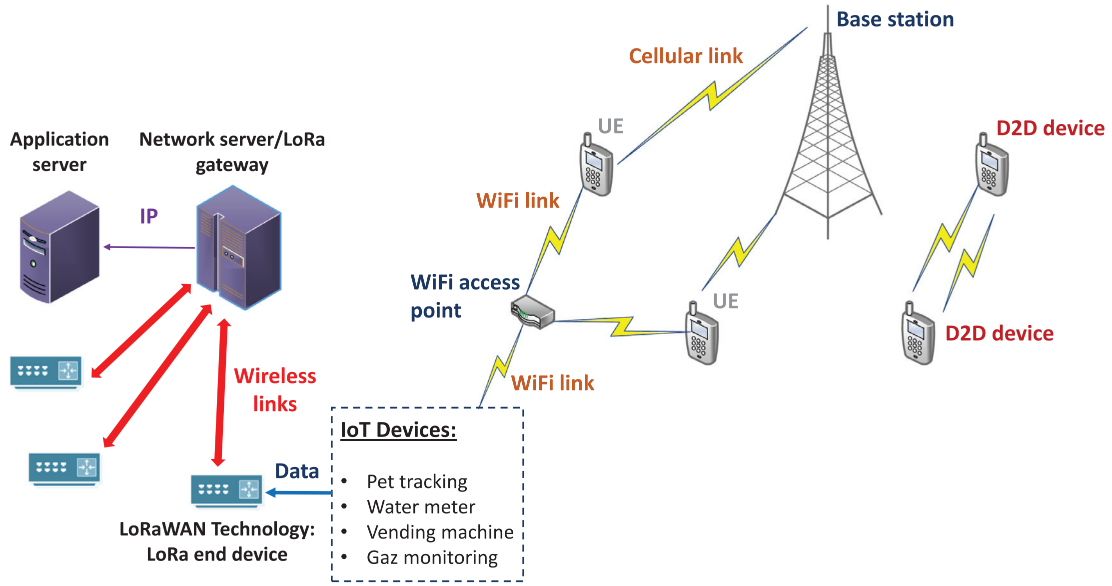


Fig. 1. Examples of multi-homed devices: an IoT device having two possible connections (WiFi and LoRaWAN), a D2D device having two possible connections and a user equipment having a WiFi and cellular connection.

packets to the next intermediate nodes or destination nodes. At the receiver, coded packets can be successfully decoded using Gaussian elimination [2]. Regardless of the many benefits offered by RLNC, when the network includes erroneous channels that are susceptible to noise, fading, and link failure, the overall network performance degrades, dramatically. Moreover, RLNC is also prone to various types of security threats such as eavesdropping attacks and Byzantine modifications [3]. While, the former compromises data confidentiality, the latter disrupts the authentication of the network. Hence, the challenge of providing reliable and secure data transmission arises. In fact, the practical benefits of RLNC are limited to the security level of this technology, especially when used for relaying sensitive information in the financial and military domains [4].

On the other hand, multi-homing has emerged as a new paradigm that allows hosts with multiple IP (Internet Protocol) addresses, to connect to more than one network and relay data over several channels, simultaneously. These devices can have two or more external links to the same Internet service provider or different Internet service providers (several network interfaces in multi-homed devices). Also, there are mainly two types of multi-homing: IPv4 multi-homing and IPv6 multi-homing. This technology promises increased throughput, efficient performance, enhanced reliability and connectivity, and better robustness against failures. An example of a multi-homed device is a mobile phone, which can connect to WiFi (Wireless Fidelity), LTE (Long Term Evolution) and 5G. Recently, the “Dual Connectivity” standard has been introduced in the 3GPP Release 12 for small cell enhancement through simultaneous data transmission. This feature allows the user equipment to have two separate connections in heterogeneous networks (one providing 4G access and the other providing 5G access), thus, increasing the per-user throughput [5]. The concept of multi-homing has also been adopted in other technologies such as Internet-of-Things (IoT) which supports multiple protocols such as Bluetooth, WiFi, cellular, ZigBee and LoRaWAN (Fig. 1).

To improve the performance of data communication in multi-homed systems even further, RLNC can be utilized, where one can exploit the advantages of both technologies to overcome the limitations hindering the efficient deployment of high data-rate and delay-sensitive applications [5].

In this paper, an efficient RLNC-based security solution is proposed for multi-homed systems (end-to-end). More specifically, the coefficients of the binary RLNC matrices are secured and modified in such a way that these matrices are only known to the communicating entities and have a determinant equal to one. This condition should be valid at all times in order to ensure the successful decoding of encoded data. Hence, a new approach for generating dynamic and invertible binary matrices is defined and verified, theoretically and experimentally. The coefficients of the encryption/encoding binary RLNC matrices are derived from a secret dynamic key, which is obtained by combining a secret master key with a random channel-extracted nonce. The proposed scheme leverages the random and dynamic features of physical channels to increase the security level. The secret key is also used to generate the cryptographic primitives needed for the proposed ciphering/deciphering process such as substitution tables, block permutation tables and random selection vectors. In addition to data confidentiality and reliability, the proposed scheme ensures source authentication and message integrity. By doing so, the proposed solution jointly improves the security and performance of multi-homed systems. To the best of the authors' knowledge, this is the first work that utilizes the binary field to reduce the computational complexity of RLNC and secure multi-homed networks. Finally, security and performance tests are presented to prove the robustness and efficiency of the proposed scheme.

Table 1
Table of notations

Notation	Definition
n	Total number of sub-channels
N_0	Channel nonce
SK	Secret session key
K_{IA}	Source authentication and message integrity key
MK	Master key
N	Size of input data (bytes)
G	Encryption/encoding matrix
π	Permutation table
π^{-1}	Inverse permutation table
SRM	Random selection table for the channel coding matrices
SRM^{-1}	Inverse of SRM
π_{SRM}	Permutation table for SRM
SL	Random selection table for each link/RAT
SL^{-1}	Inverse of SL
π_{SL}	Permutation table for SL
S	Substitution table
S^{-1}	Inverse substitution table
π_S	Permutation table for S
π_{BL}	Block permutation table
π_{UBL}	Permutation table for π_{BL}
C	Encrypted/encoded matrix
I	Identity matrix
$det(.)$	Determinant operation
$\wedge$	Logical AND operation
$\odot$	Binary matrix multiplication
$\|\|$	Concatenation operation
$\oplus$	Exclusive-OR (XOR)

The rest of this paper is organized as follows. Section 2 presents the table of notations, the multi-homed general system model and some basic concepts of RLNC. Section 3 reviews current scenarios of RLNC and discusses the possibility of enhancing the security of multi-homed systems with RLNC. Section 4 presents the proposed authentication-confidentiality scheme and the proposed technique used to construct the invertible and dynamic binary matrices. Section 5 assesses and analyzes the security properties of the proposed scheme, especially in terms of randomness, uniformity, sensitivity, recurrence and independence. Section 6 studies the performance of the proposed scheme in terms of computational complexity, delay, error propagation and flexibility. Finally, Section 7 concludes this work and discusses its future prospects.

2. Background

In this section, the table of notations, the system model, the basic methodology of RLNC and the considered threat model, are presented and discussed thoroughly.

2.1. Preliminaries and notation

Table 1 represents all of the notations used in this paper.

2.2. System model of multi-homed networks

Since most state-of-the-art networking devices (e.g., smart-phones) are, currently, equipped with multiple radio interfaces of different access technologies, multi-homing has emerged as a new mechanism that exploits this feature and enables hosts with multiple network interfaces (IP addresses) to establish multiple simultaneous connections. Consequently, this has enhanced system performance in terms of efficient resource utilization, increased throughput and better robustness against failures [6]. Multi-homing has been adopted in many technologies (Fig. 1), few of which are Internet-of-Things (IoT), Device-to-Device, Machine-to-Machine, and Wi-Fi/LTE communication systems.

Throughout this paper, we consider a general multi-homed system with n RATs (sub-channels). A message of size N bytes is to be transmitted over the n available sub-channels/RATs, where each link has a different data rate. Using the proposed cryptographic scheme, data will be encrypted, encoded, authenticated, and then transmitted over multiple RATs (Fig. 2). It should be noted that communication is assumed to be end-to-end. Upon the reception of ciphered data, the legitimate receiver performs the inverse cryptographic solution (decoding and then decryption), after validating the integrity and authentication of data.

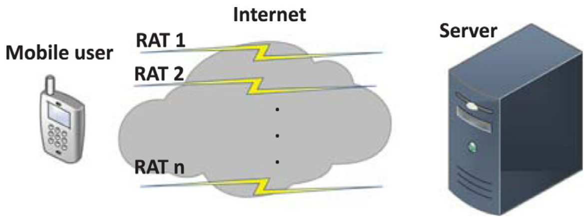


Fig. 2. A general multi-homed system model.

2.3. RLNC: basic concept

Random Linear Network Coding (RLNC) is an emerging coding discipline that allows independent network nodes to generate linear mappings of input to output data symbols over a finite field [7]. The RLNC process is briefly described as follows:

1. The original stream of data is divided into symbols of fixed sizes.
2. Then, each symbol is multiplied with scalar coding coefficient that is randomly chosen from a Galois field (GF(2^q), q is the field size), as illustrated in Eq. (1):

$$y_l = \sum_{p=0}^{P-1} c_l.x_l, \tag{1}$$

where P is the number of packets stored at the node's network coding buffer ($0 \leq p \leq P$), c_l corresponds to the random linear network coding coefficient, and x_l and y_l are the original and coded packets transmitted on link l, respectively [8]. In principle, the utilized random linear network coding coefficients can be either integer values or binary. Unlike the former case, the latter is not heavily employed. Moreover, binary RLNC ($n \times n$) is a special case of integer RLNC.

This simple operation can be viewed as creating linear combinations of data symbols, using coding vectors that contain random coding coefficients. As a result, network reliability and efficiency are enhanced, simultaneously [7].

2.4. Threat model

For the design and evaluation of robust security solutions for current and future communication systems, a suitable threat model is required. In this paper, two types of adversaries are considered: the *honest-but-curious* adversary, and the *malicious* adversary.

- *Honest-but-curious* adversary (passive): This is a legitimate user who follows the protocol properly and does not deviate from it. However, such users try to acquire as much information as possible from the legitimately received messages (passive eavesdropping). Thus, *passive attacks* are considered within the threat model to prove that the privacy and data confidentiality requirements are achieved [9]. It should be noted that the security mechanism is proposed for multi-homed systems. Hence, the eavesdropper gathers information from several links/sub-channels, simultaneously, which might be a challenging task. Assuming that the eavesdropper is able to access information on multiple links at the same time, finding the correct dynamic secret key (cryptographic primitives) for each message is difficult and not straightforward.
- *Malicious* adversary (active): This is an illegitimate user who attempts to deviate from the defined security protocol by injecting, modifying or deleting valid data. These users also try to impel other users to act maliciously and deviate from the defined protocol, by substituting their local inputs. In fact, the intentional modification of encrypted data by a malicious attacker compromises its integrity. As such, we consider the *malicious* user threat model to prove the proposed scheme's robustness in terms of confidentiality, integrity, source authentication, and data availability [10]. Since the proposed solution is based on the dynamic key approach, related-key attacks, statistical attacks and all well-known cryptanalysis (linear and differential attacks) are thwarted. Moreover, in multi-homed systems, the illegitimate user (active adversary) should be able to monitor several sub-channels, concurrently. However, this is not feasible in most cases.

3. Related work

In this section, we briefly present and discuss the schemes in the literature that target the security of both, multi-homed networks and RLNC. Here, it should be noted that all of the schemes presented in the literature employ integer-based RNLC matrices on transmitted symbols. In contrast, this paper relies on secure and efficient binary RLNC matrices to enhance the security of multi-homed networks with minimum cost.

Table 2
A Summary of the existing security schemes for multi-homed schemes in the literature.

Security schemes	Advantage	Limitation	Resource and communication overhead	Complexity
Securing cache contents	The proposed scheme, jointly, achieves the privacy of users, and integrity and availability of contents	The scheme only protects cached contents and not transmitted messages (data confidentiality is not achieved	It requires additional resources or communication overhead related to the Chinese remainder theorem	Not computationally complex: Chinese remainder theorem reduces the complexity of polynomial multiplication
Enhancing IPv6 addressing format	The proposed scheme does require additional resources	Authors target the addressing format of IPv6 packets and not the confidentiality of transmitted data	It does not require additional resources or communication overhead	Not computationally complex: only the addressing format is enhanced
Modifying the existing protocol stack to enhance 3GPP femtocell architecture	The enhancement of the femtocell technology in terms of service registration, identity verification and node multi-homing	Authors focus on the mobility and security issues of femtocells rather than the security of multi-homed systems	It does not require additional resources or communication overhead	Computational complex: modifying the protocol stack
Securing SCTP in multi-homed systems	The comparison of the different schemes to secure the SCTP protocol in multi-homed systems	The security of SCTP does not secure data at lower layers of the protocol stack	It requires additional resources or communication overhead related to traditional security algorithms	Complex: utilizing conventional security algorithms that require multiple rounds
Data scrambling	The scheme secures data using a simple operation	The scrambling vectors are exchanged using symmetric key encryption, which requires the transmission of additional messages	Three additional messages are transmitted and additional resources are required to perform multiple encryption/decryption operations	Not computationally complex
security-aware energy-efficient resource allocation algorithm	Scheme jointly enhances performance and security	Data transmitted is not secured	It requires additional resources	Computationally complex: optimization problem

3.1. Security of multi-homed systems

In [11], the authors present an approach for optimizing and securing data transmitted over multiple RATs. The proposed scheme scrambles data on different RATs using different scrambling vectors, which are exchanged between users using symmetric key encryption. The main disadvantage of this technique is that it requires the exchange of additional messages (a three-way handshake) and multiple encryption/decryption operations which introduce considerable delay.

The technique presented in Demir and Suri [12] aims at providing a secure and reliable communication in case of a Distributed Denial-of-Service (DDOS) attack or link/node failure, in a smart grid environment. In particular, the authors present a multi-homing-based fast recovery mechanism to re-transmit dropped packets.

Differently, the work in Shuminoski et al. [13] presents an advanced security module that takes into consideration the desired Quality-of-Service (QoS) requirements with vertical multi-homing and multi-streaming framework for 5G mobile terminals with radio network aggregation capability. Whereas, the authors in Xu et al. [14] propose a security-aware energy-efficient resource allocation algorithm, which does not directly secure data transmitted over multiple RATs.

In [15], a secure caching scheme for multi-homed users is presented, based on game theory, where a trust mechanism is designed to guarantee the availability of cached contents. An encryption protocol based on the Chinese remainder theorem is also introduced to preserve the privacy of mobile users and the integrity of the contents.

On the other hand, a new approach that enhances the IPv6 addressing format in a backward-compatible manner, is presented in Atkinson et al. [16]. The approach does not require additional resources; hence, existing IPv6 routers can still be utilized. Similarly, the existing protocol stack of the 3GPP femtocell architecture is modified in Namal et al. [17], to enhance the femtocell technology in terms of service registration, identity verification and node multi-homing. In particular, the authors focus on the mobility and security issues related to the femtocell technology. Finally, a comparison of the various techniques used to secure the Stream Control Transmission Protocol (SCTP) in multi-homed networks is presented and thoroughly analyzed in Venkadesh et al. [18]. Table 2 summarizes and compares the related schemes presented in the literature.

So far, very few schemes that target the confidentiality of data transmitted over multiple channels have been presented in the literature. Moreover, most of the existing security solutions require high overhead (computational and resources), which is not suitable for resource-limited multi-homed devices. Conventional security solutions include block ciphers such as the optimized Advanced Encryption Standard (AES) [19]. AES can also be used as a message authentication algorithm to ensure

Table 3
A Summary of the three main RLNC-based confidentiality schemes in the literature.

Security schemes	Advantage	Limitation	Resource and communication overhead	Complexity
Homomorphic encryption	Any change or modification in the ciphertext is reflected in the plaintext	Asymmetric HE is costly and inefficient. symmetric HE is more preferable	Asymmetric HE exhibits high costs and overhead in terms of latency, storage, and required resources	Computationally complex
Selective homomorphic encryption	The GEVs are encrypted instead on the entire payload	GEVs are only secured and not the payloads (not fully secure or robust)	It introduces less overhead since on the GEVs are encrypted	Not computationally complex
Traditional encryption	Robust traditional schemes are used to encrypt the packets' payloads, which results in a high security level	Traditional encryption schemes require multiple iteration rounds which is not suitable for current and future devices (resource-limited)	Traditional encryption schemes require a high resources and communication	Computationally complex

data integrity and source authentication. However, this class of cryptographic algorithms requires multiple iterations of the round function, which introduces a significant amount of overhead in terms of latency and resources. Another type of security solutions is chaotic cryptography. It employs pseudo-random non-linear functions to achieve the desired cryptographic properties. However, chaotic cryptography is very complex since it is based on floating-point numbers and conversion operations. Recently, Physical Layer Security (PLS) has emerged as a novel paradigm to achieve robust security, efficiently [20]. It has been the focus of many researchers, lately, where several security solutions have been proposed for single end-to-end communication systems, but none for multi-homed systems. Therefore, new security solutions that enhance the security and performance of multi-homed systems should be designed and proposed.

3.2. Securing RLNC matrices

Several techniques that ensure the authentication and confidentiality of data encoded using RLNC (integer/symbol level) have been presented in the literature [21]. A set of these solutions relies on a new kind of encryption, Homomorphic Encryption (HE), to thwart passive attacks [21]. HE could be based on symmetric or asymmetric encryption, and arithmetic operations, performed on the ciphertext, are reflected on the plaintext. However, the use of a public HE scheme is costly in terms of delay and additional resources since complex computations are required at each participating node [22]. The second class of RLNC-based security schemes is simple and straightforward. Specifically, all of the packet's payloads are encrypted using traditional encryption techniques (multiple rounds and multiple operations). As a result, this introduces a large overhead in terms of latency, computational complexity and utilized resources. Finally, the third class of schemes is selective HE. Instead of encrypting the entire payload, selective HE secures only the Global Encoding Vectors (GEV) of each packet. The three discussed RLNC schemes are summarized in Table 3.

In [23], the authors present a scheme that encrypts a set of encoding matrices at the source, and appends another unencrypted set, to maintain the standard encoding processes at intermediates nodes. Clearly, this scheme requires the encryption of fewer data segments, however, it requires two decoding rounds, which is considered inefficient. In [24], a static key matrix is utilized to secure the coefficients of the encoding matrices. The same key matrix is distributed to destination nodes through a secure channel, and it is used throughout the communication session. This leads to the problem of single generation failure, where accidental key disclosure compromises the secrecy of the following communication sessions. Finally, in Zhang et al. [22], a dynamic permutation cipher scheme is presented and applied on each packet using the same dynamic key.

All of the presented RLNC security techniques prove that there exists a strong trade-off between security and performance. Hence, in what follows, we propose a simple and efficient encryption/encoding scheme for muti-homed systems, based on binary RLNC, which balances both security and performance.

4. Proposed solution

The proposed scheme is mainly divided into two parts: key generation and data encryption/encoding.

4.1. Key generation

The proposed key derivation scheme is based on the work presented in Melki et al. [20]. More specifically, the physical properties of wireless channels are exploited to generate a random Secret Key, (*SK*), which is used to derive the cipher primitives of the proposed encryption/encoding scheme. Moreover, we assume that end-to-end users have n radio interfaces/RATs (n sub-channels), and they share a common key, the Master Key, *MK*.

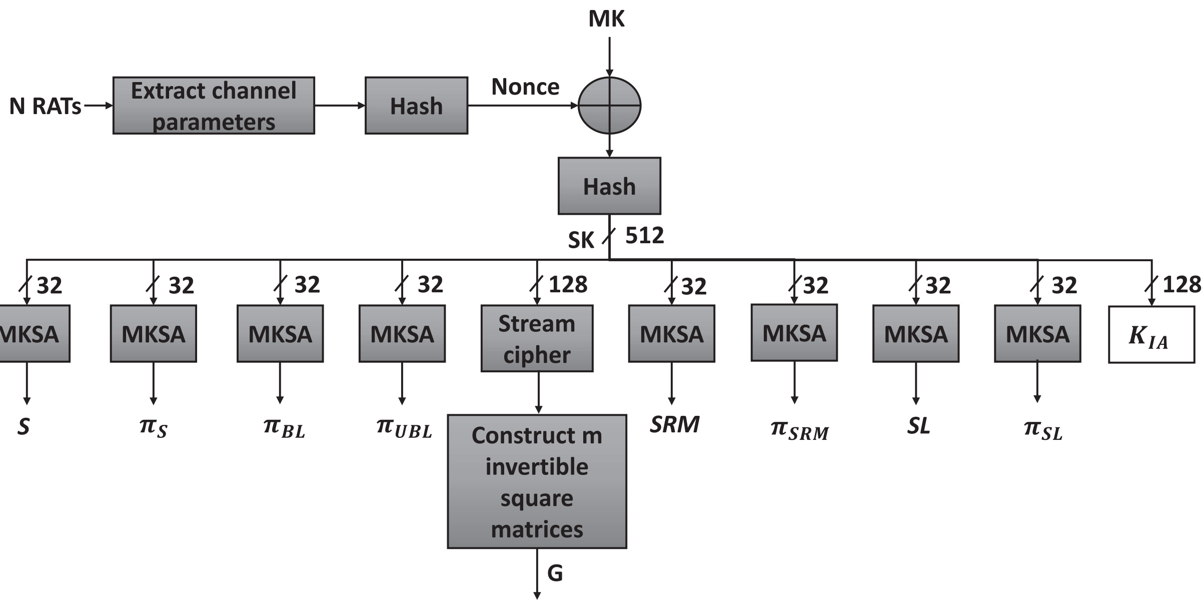


Fig. 3. The proposed key distribution scheme.

First, the communicating devices estimate each of the n active sub-channels. Then, n random nonces are extracted, concatenated and hashed to obtain N_0. Afterwards, N_0 is XORed with the pre-shared common key MK, and hashed to generate the dynamic secret key, SK (512 bits) (Fig. 3). Here, the $SHA-512$ is used for the hashing operation.

Next, SK is divided into ten sub-keys of different sizes. The first two sub-keys (both are 32 bits long) are used to generate the set of substitution boxes, $S : S_1, S_2, \ldots, S_n$, each with 256 elements, having values between 1 and 256, in addition to the update permutation tables for the substitution boxes, $\pi_S : \pi_{S_1}, \pi_{S_2}, \ldots, \pi_{S_n}$, having the same size. These are used to perform byte-substitution on input bytes before encryption/encoding. The first substitution box, S_1, is generated, and all of subsequent substitution boxes are just shifted versions of it.

The second pair of keys, having a length of 32 bits, is used to derive n block permutation tables, $\pi_{BL} : \pi_{BL1}, \pi_{BL2}, \ldots, \pi_{BLn}$, along with their update permutation tables, $\pi_{UBL} : \pi_{UBL1}, \pi_{UBL2}, \ldots, \pi_{UBLn}$. This is done using the RC4 Modified Key-Scheduling Algorithm (M-KSA) [25]. These tables, each of size $(1 \times m)$, are used to perform block permutation for every n columns of encrypted/encoded data. The fifth sub-key, which is 128 bits long, is used to obtain $m = N/(n^2)$ binary invertible encryption/encoding matrices, $G : G_1, G_2, \ldots, G_m$ of size $(n \times n)$ and having values of 0's and 1's, where each unique matrix is randomly multiplied by an $(n \times n)$ binary sub-matrix of the input data (m blocks/sub-matrices). Another pair of 32-bit sub-keys is used to generate a random matrix selector SRM of size $(1 \times m)$, and an update permutation table for SRM of the same size (π_{SRM}). SRM has random values between 1 and m and it is used to randomly select the encryption/encoding matrix which will be multiplied by each data sub-matrix. Similarly, two 32-bit sub-keys are used to derive the random link selector SL and the update permutation table π_{SL}, both having a size of $(n \times 1)$ and values between 1 and n, which will be used to randomly select the rows that will be transmitted on each link/RAT. Finally, the last 128-bit sub-key is used to produce the message integrity/authentication key K_{IA}.

It should be noted that π_S, π_{UBL}, π_{SRM} and π_{SL} are used to update the cipher primitives, S, π_{BL}, SRM and SL for each input message, respectively.

4.2. Data encryption using binary RLNC

In this subsection, both the proposed encryption and decryption processes are described in detail.

4.2.1. RLNC channel coding and data encryption

An input stream of N bytes is divided into n rows and N/n columns, forming a data matrix of size $(n \times (N/n))$, where n is the number of available sub-channels. If N is not divisible by n, padding is applied. Next, each of the N/n bytes on each row is randomly substituted using one of the corresponding substitution boxes, $S_1, S_2, \ldots, S_n$. The substituted bytes are then encrypted and encoded as follows:

- The matrix of substituted bytes is further divided into $m = (N/n)/n$ sub-matrices, each having n rows and n columns (bytes).
- Using the random matrix selector SRM, which contains random numbers between 1 and m, each of the m data sub-matrices $(n \times n)$ is mixed with one of the invertible, unique, binary encryption/encoding matrices $(n \times n)$ from the

set G. Here, binary matrix mixing/multiplication refers to row-column multiplication and byte-addition using the XOR operation. That is:

$$C_{4\times1} = G_{4\times4} \odot X_{4\times1}, \tag{2}$$

$$\begin{bmatrix} C_1 \\ C_2 \\ C_3 \\ C_4 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix} \odot \begin{bmatrix} X_1 \\ X_2 \\ X_3 \\ X_4 \end{bmatrix} = \begin{bmatrix} X_1 \oplus X_2 \oplus X_4 \\ X_2 \oplus X_4 \\ X_1 \\ X_3 \oplus X_4 \end{bmatrix}$$

where $\odot$ represents the binary matrix multiplication, $\oplus$ is the XOR operation, G is an example of a (4×4) binary encryption/encoding matrix, X is a (4×1) plaintext matrix which includes 4 bytes, X_1, X_2, X_3 and X_4, and C is the resulting ciphered/encoded matrix which has 4 rows and 1 byte column (8 binary columns). More specifically, the addition and subtraction arithmetic operations are replaced by the logical operation Exclusive-OR ($\oplus$), the multiplication operation is replaced by the logical AND operation ($\wedge$). This step is described in the pseudo code of Algorithm 1.

Algorithm 1 Binary multiplication matrix algorithm.

```
procedure Z = BINARY_MULTIPLICATION(X, Y)
    [m, n] = size(X)
    [n, q] = size(Y)
    for i ← 1 to m do
        for j ← 1 to q do
            tmp ← 0
            for k ← 1 to n do
                tmp ← tmp ⊕ (X(i, k) ∧ Y(k, j))
            end for
            Z(i, j) ← tmp
        end for
    end for
    return Z
end procedure
```

- The resulting m encrypted/encoded matrices, C_i $(1 \leq i \leq m)$, will also have n rows and n columns (byte values).

At the output of the encryption/encoding operation, each of the n rows undergoes block permutation. Specifically, the m blocks on each row are randomly re-ordered and permuted using a different permutation table, $\pi_{BL1}, \pi_{BL2}, \ldots, \pi_{BLn}$. Each block consists of a single row with n bytes. Then, the Message Authentication Code (MAC) of each block is calculated using K_{IA}, and appended to the message itself. This step is crucial for ensuring source authentication and message integrity (Fig. 4). Finally, each row of the m obtained encrypted/encoded sub-matrices is randomly transmitted on one of n available sub-channels (RATs) using the link selector (SL), which is an $(n \times 1)$ matrix having random values between 1 and n (Fig. 5).

For every new input message, new cryptographic primitives are generated by randomly permuting the old cryptographic primitives using π_S, π_{UBL}, π_{SRM} and π_{SL}.

4.2.2. Generation of encryption/encoding RLNC binary matrices

The process of encoding in binary Galois field based on the matrix, G, has many advantages, some of which are the reduction of the required computational complexity, increasing the throughput and decreasing the energy consumption. However, the generation of these matrices is not straightforward since they should possess specific properties in order to fit within the proposed scheme, and to ensure its efficient deployment in today's communication systems. Hence, in the following, we describe a new scheme for generating binary invertible matrices, in addition to several matrix forms.

As mentioned previously, the encryption/encoding matrix G_i $(1 \leq i \leq m)$ should have n rows and n columns, where any G_i should be invertible. For this purpose, we first construct a generic $(n \times n)$ matrix, Gt_i, using a binary square sub-matrix, Mu_i, and an identity matrix, Im_i, and then, derive G_i. Note that Mu_i is a non-zero matrix having a size of $(\frac{n}{2} \times \frac{n}{2})$ and Im_i is an identity matrix of the same size. In order to ensure the invertibility of Gt_i, the determinant should always be equal to 1. The determinant, in the binary field, is equal to the determinant in the integer field modulo 2. The $(n \times n)$ binary invertible matrix is given by:

$$Gt_i = Gt_i^{-1} = \begin{bmatrix} Mu_i & Mu_i \oplus Im_i \\ Mu_i \oplus Im_i & Mu_i \end{bmatrix} \tag{3}$$

Theorem 1. *Gt_i is invertible and has a determinant equal to one for any sub-matrix Mu_i.*

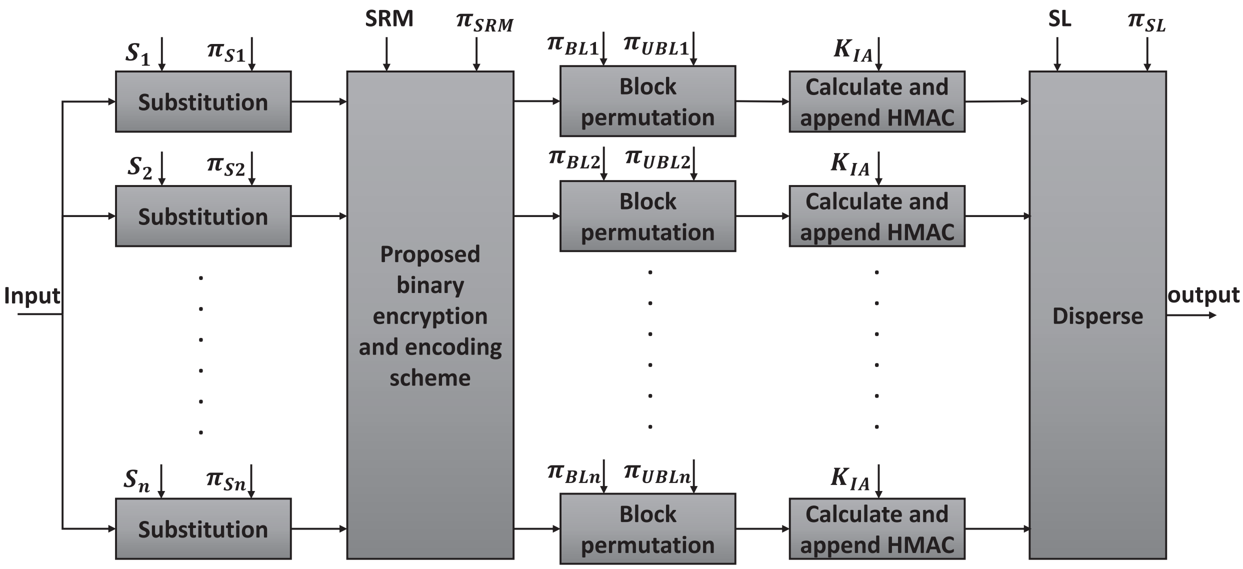


Fig. 4. Proposed cryptographic scheme based on substitution, permutation and binary RLNC encoding.

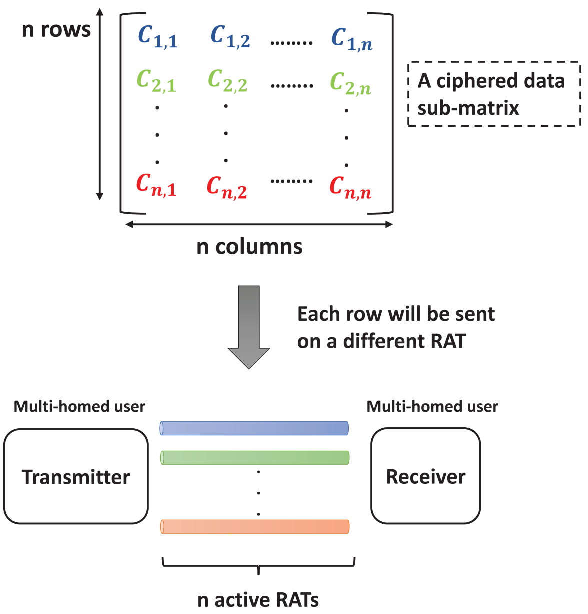


Fig. 5. Proposed transmission mechanism over multiple RATs.

Proof. A general form of a 2 × 2 matrix is shown below:

$$M = \begin{bmatrix} a & b \\ c & d \end{bmatrix}, det(M) = ad - bc. \tag{4}$$

In order to ensure the invertibility of M, $det(M)$ should always be equal to 1. We assume that d is equal to the value of a, hence, the determinant of M, $det(M) = 1 = a^2 - bc$, and $bc = a^2 - 1 = (a-1)(a+1)$. Consequently,

$$M = \begin{bmatrix} a & a+1 \\ a-1 & a \end{bmatrix}, det(M) = a^2 - a^2 + 1 = 1. \tag{5}$$

Replacing a with a matrix A, and 1 with an identity matrix Im, would also result in an invertible block matrix, Q. In general, the determinant of an invertible block matrix, Q, consisting of four sub-matrices A, B, C and D, is equal to

$$Q = \begin{bmatrix} A & B \\ C & D \end{bmatrix} = \begin{bmatrix} A & A+I_m \\ A-I_m & A \end{bmatrix}, \tag{6}$$

$$\begin{aligned}det(Q) &= det(A) \times det(D - CA^{-1}B)\\ &= det(A) \times det(D - CBA^{-1})\\ &= det(A) \times det(A - A^2A^{-1} + I_m^2 \times A^{-1})\\ &= det(A) \times det(A - A + A^{-1})\\ &= det(A) \times det(A^{-1})\\ &= det(A \times A^{-1})\\ &= det(I_m)\\ &= 1,\end{aligned}$$

where $C \times B$ is equal to $A^2 - Im^2$, $A^2 \cdot A^{-1}$ is equal to A and $A^{-1} \cdot Im^2$ is equal to A^{-1}.

Now, replacing the integer matrix A with a binary matrix Mu_i, having $n/2$ rows and $n/2$ columns, yields:

$$Gt_i = \begin{bmatrix} Mu_i & Mu_i \oplus Im_i \\ Mu_i \oplus Im_i & Mu_i \end{bmatrix}, \tag{7}$$

where Im_i is an identity matrix having the same dimensions as Mu_i. Here, it should be noted that the addition and subtraction arithmetic operations are replaced with the logical XOR ($\oplus$) operation, and the multiplication operation is replaced by the logical AND operation ($\wedge$).

Since, Gt_i is a binary block matrix, the determinant of this matrix is written as:

$$\begin{aligned}det(Gt_i) &= det(A) \wedge det(D \oplus C \wedge A^{-1} \wedge B)\\ &= det(A) \wedge det(D \oplus C \wedge B \wedge A^{-1})\\ &= det(Mu_i) \wedge det(Mu_i \oplus Mu_i^2 \wedge Mu_i^{-1} \oplus\\ &\quad Im_i^2 \wedge Mu_i^{-1})\\ &= det(Mu_i) \wedge det(Mu_i \oplus Mu_i \oplus Mu_i^{-1})\\ &= det(Mu_i) \wedge det(Mu_i^{-1})\\ &= det(Mu_i \wedge Mu_i^{-1})\\ &= det(Im_i)\\ &= 1,\end{aligned} \tag{8}$$

where $C \wedge B = (Mu_i^2 \oplus I_m^2)$, $Mu_i^2 \wedge Mu_i^{-1} = Mu_i \wedge Mu_i \wedge Mu_i^{-1} = Mu_i$ and $Mu_i^{-1} \wedge Im_i^2 = Mu_i^{-1}$. Therefore, Gt_i is invertible for any sub-matrix Mu_i, and $Gt_i = Gt_i^{-1}$. □

Hence, Gt_i always has a determinant equal to one, and Gt_i^{-1} is equal to Gt_i, which reduces the delay of decoding.

In order to obtain G, which is a set of $(n \times n)$ diffusion matrices, we generate first m such Mu_i matrices. The coefficients of each Mu_i matrix, which is used to derive one unique encryption/encoding matrix (G_i for all $i \in [1, m]$), are generated using SK. Using the proposed matrix generation technique and the generic matrix form, one can ensure that all of the obtained encryption/encoding matrices are secure and invertible. Consequently, this enhances the performance and security of end-to-end wireless communication systems.

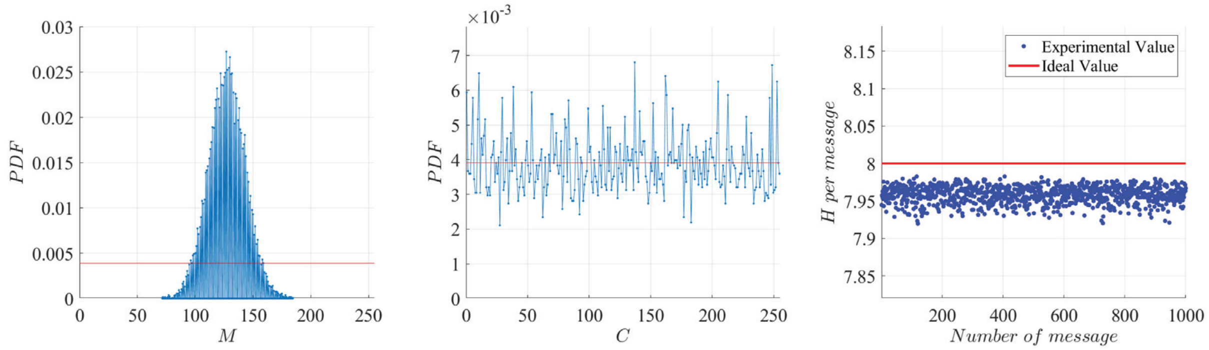
4.2.3. Decryption and data recovery

At the receiver, the same steps are followed but in a reversed order. In addition, the inverse cipher primitives (S^{-1}, SRM^{-1}, π_{BL}^{-1}, and SL^{-1}) are used. First, the ciphered data received on each of the n rows are de-shuffled using the inverse link selector SL^{-1} (for all m sub-matrices). Next, inverse block permutation is performed to obtain the ciphered matrices C_i ($1 \leq i \leq m$), using the set π_{BL}^{-1}.

Next, C_i $(n \times n)$ and G_i^{-1} (which is equal to G_i) $(n \times n)$ are multiplied using Equation 2. The resulting bytes are substituted using S^{-1} to obtain the transmitted plaintext bytes.

The advantage of the proposed decryption process is that it decreases the computational complexity and overcomes the issue of connection failure due to fading, Doppler effects or availability attacks. In particular, original data are encrypted/encoded at the byte/bit level using simple and lightweight cryptographic operations, which jointly, enhance the security and performance of multi-homed systems.

For every input message, new cipher primitives are generated using the update permutation tables, π_{UBL}, π_S, π_{SRM} and π_{SL}. This guards against many attacks such as chosen/known plaintext/ciphertext attacks.



(a) PDF of the original message (b) PDF of the obtained ciphertext (c) Entropy of the ciphertext message

Fig. 6. The probability density function of the (a) original input and the (b) ciphered/encoded output for 1000 iterations and using 256 QAM modulation. (c) The entropy of the ciphertext.

4.3. Discussion

The proposed scheme aims at jointly enhancing the security and performance of multi-homed systems using RLNC. More specifically, random physical properties, which are extracted from multiple end-to-end wireless channels, are combined with a master key to generate a secret session key [20]. The resulting key is then used to derive the needed cipher primitives, which include a substitution table, a block permutation table, the RLNC matrices and two random selection tables. By doing so, the cryptographic primitives used in the ciphering and encoding process become only known to the communicating entities, and hence, data confidentiality is successfully achieved. The proposed scheme also achieves source authentication and message integrity, by calculating and appending the MAC of each ciphered message to the message itself using the secret session key. Unlike the work presented in the literature, this paper presents a scheme that secures and encodes binary input data, which is a hard challenge. In general, RLNC a simple network coding scheme that allows intermediate nodes to generate random and independent linear mappings of input to output data symbols over a finite field (coefficients chosen from a Galois field) [7]. Consequently, this technology improves the network performance substantially. On the other hand, ensuring the inveritibility of binary RLNC matrices is a crucial condition for the proposed deciphering process, therefore, original RLNC matrices are modified in such a way that these matrices are invertibile and have a determinant equal to one. Moreover, a general form for RLNC binary matrices is proposed and verified theoretically. Another aspect of the proposed scheme is that it overcomes link errors and availability attacks. More specifically, wireless channels are subjected to many errors that result from doppler effects, noise, fading and jamming. Consequently, some links (sub-channels) in multi-homed systems might suffer from bad quality, erroneous reception of data or failure. Using the proposed solution, communicating entities can utilize a subset of the available RATs/links to carry redundant data, which enhances the reliability of wireless communication (transmitted data are correctly recovered). As a result, key establishment, data confidentiality, message authentication/integrity and network coding are achieved using the proposed security solution.

5. Security and cryptanalysis

In this section, we describe and asses the robustness of the proposed scheme against well-known attacks, which include statistical attacks, linear/differential attacks, chosen/known plaintext/ciphertext attacks, brute force attacks and key-related attacks.

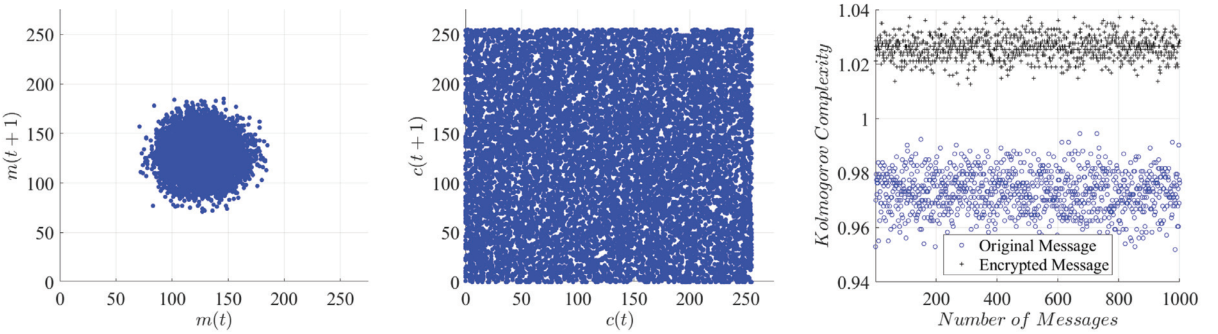
The proposed scheme is considered public and the cryptanalyst is assumed to have complete knowledge regarding all the required steps, but none regarding the secret key that is used for data encryption.

5.1. Statistical attacks

In order to resist statistical attacks, ciphered data should have a high randomness degree. For this purpose, several randomness tests, which include entropy analysis, Probability Density Function (PDF), correlation, and recurrence, are presented to prove the proposed scheme's robustness against statistical attacks.

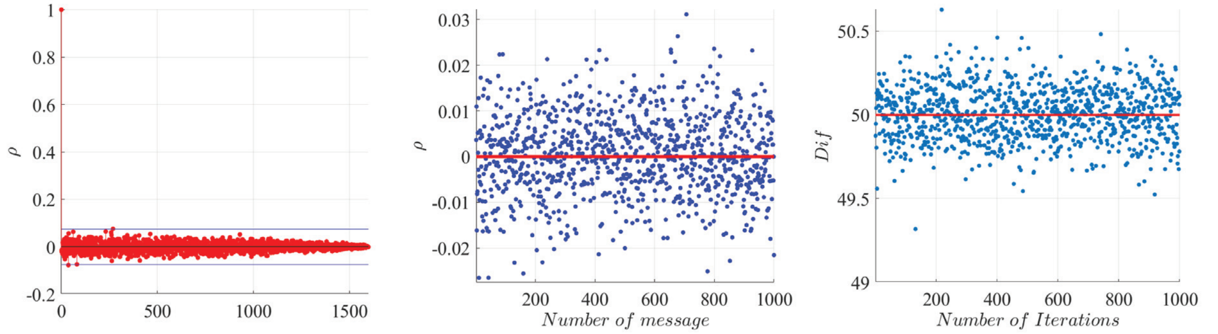
5.1.1. Uniformity using probability density function (PDF)

One way to quantify the uniformity property is by plotting the PDF of encrypted symbols and verifying visually the type of the distribution. This simple method is sufficient to prove that the proposed scheme has a good mixing level (randomness). Fig. 6a and b represent the PDF of the original and encrypted data, respectively. The plot clearly verifies that the original data is normally distributed, while encrypted symbols are uniformly distributed (random output). In order to



(a) Recurrence of the original message (b) Recurrence of ciphertext (c) Kolmogorov complexity of binary ciphertext

Fig. 7. The recurrence plots of the (a) original message and its (b) encrypted version.



(a) Auto-Correlation (b) Correlation (c) Difference

Fig. 8. The sample (a) auto-correlation function for a random dynamic key, (b) inter-correlation and (c) independence results for 1000 random dynamic keys.

validate this result, the entropy test is performed. Specifically, a uniform probability (distribution) represents maximum uncertainty, which yields to maximum entropy (the entropy of the obtained encrypted symbols should be equal to 1 and 8 at the bit and byte levels, respectively).

5.1.2. Entropy

Generally, the entropy values of encrypted symbols at the byte level should be equal to 8, which corresponds to maximum uncertainty (randomness). Fig. 6c shows that the encrypted symbols (byte level) have an entropy value close to the desired value of 8, at both, the message and block levels. The Kolmogorov entropy (complexity) of the original and encrypted messages has also been plotted. The Kolmogorov complexity of the original data is less than one, whereas that of the encrypted data is above one (Fig. 7c). This confirms that the proposed scheme produces encrypted symbols that are, indeed, uniform and random.

5.1.3. Recurrence

The recurrence function measures the correlation between a specific symbol and its delayed version. In general, encrypted symbols should have a highly scattered recurrence plot, which proves that the tested scheme has the proper randomness level. Since the input data (original) has a normal distribution, all of the recurrence points are grouped within one area (center) as shown in Fig. 7a. On the other hand, Fig. 7b shows that the recurrence plot of the encrypted data spans the entire cipher symbol space (randomized and scattered).

5.1.4. Correlation

Another important security property is correlation. For a specific scheme to be considered secure, the original and encrypted data should be un-correlated (correlation close to zero). The presented results in Fig. 8b indicate that the cross-correlation coefficient ranges between $\{-0.02, 0.03\}$ and has a mean of 0, which is the desired outcome. Also, the auto-correlation of the obtained ciphertext confirms the high randomness degree of the proposed scheme since all values are centered around zero (Fig. 8a).

Table 4
Independence between original fragments (row index) and encrypted ones (column index) n= 8.

Row index of encrypted/Column index of original fragments	O1	O2	O3	O4	O5	O6	O7	O8
E1	49.9531	50.0625	50.4297	49.3906	51.0234	50.0234	50.4922	49.5078
E2	49.6719	50.2500	49.3672	49.8750	50.2422	49.3203	49.9766	49.4922
E3	50.1016	49.9766	49.9219	50.3047	50.3281	49.5781	50.0938	49.4219
E4	49.9609	50.7266	49.8438	50.0859	50.3438	49.7500	50.4687	51.0000
E5	49.1641	49.6328	50.2344	50.0391	49.3750	48.7969	51.1094	50.2969
E6	49.7578	50.3516	50.6094	50.9922	49.9063	50.5313	50.1094	50.5938
E7	50.0859	49.6641	49.4531	50.1328	50.1406	49.9063	50.4063	48.9375
E8	50.3047	50.1172	51.4531	49.6484	50.1875	49.7656	49.6719	50.2500

Table 5
Independence among encrypted fragments.

Row index of encrypted/Column index of encrypted	E1	E2	E3	E4	E5	E6	E7	E8
E1	–	49.4063	50.2734	49.9219	50.3359	50.1953	50.6797	49.3359
E2	49.4063	–	49.8984	49.9688	50.1953	50.3203	50.4609	50.7891
E3	50.2734	49.8984	–	49.4609	49.8281	50.3125	50.9844	49.9844
E4	49.9219	49.9688	49.4609	–	50.4453	50.4609	49.9609	50.2578
E5	50.3359	50.1953	49.8281	50.4453	–	50.1875	48.6094	49.9375
E6	50.1953	50.3203	50.3125	50.4609	50.1875	–	50.1563	49.2969
E7	50.6797	50.4609	50.9844	49.9609	48.6094	50.1563	–	49.6094
E8	49.3359	50.7891	49.9844	50.2578	49.9375	49.2969	49.6094	–

5.2. Linear/differential attacks

Here, the adversary exploits the relationship between encrypted symbols to recover the original data. In the proposed scheme, encrypted symbols are highly uncorrelated since the cipher primitives are regularly updated. Consequently, chosen/known plaintext/ciphertext attacks, single data failure and accidental key disclosure are avoided. The difference test is presented to prove the independence of encrypted data.

5.2.1. Independence

To satisfy the independence criterion, the difference value should always be close to 50%. This is based on the fact that any bit difference in the original data should change at least half of the bits at the output. In Fig. 8c, the results show that the plotted difference values, between the original and the encrypted messages, have a mean equal to the desired value, 50%. Moreover, the independence property has been assessed at the fragment level (row level of an $n \times n$ block matrix) for a fixed value of $n = 8$. The results, in Table 4, complement those in Fig. 8c, where the independence values range between 49% and 51%. This is also true for Table 5, where all of the difference values, between the encrypted fragments, are very close to 50%.

5.3. Weak keys and key-related attacks

The proposed key generation technique derives a secret session key by combining channel-based information with a master key that is only known to the communicating entities. Using this key, the cryptographic primitives, needed for the ciphering process, are obtained and updated. In order to assess the scheme's security against key-related attacks, the sensitivity of *SK* is evaluated.

5.3.1. Key sensitivity

In this test, the sensitivity of the secret key is studied, in order to assess the proposed scheme's robustness against weak keys and key-related attacks. More specifically, a one-bit change in the secret key should result into 50% difference in the set of encrypted symbols. Consequently, two secret keys, SK and SK', which differ by only one bit, are used to encrypt input symbols. Fig. 9 plots the key sensitivity values corresponding to 1,000 randomly generated secret keys. The results clearly show that the key sensitivity value is always close to 50%. Table 6 evaluates the key sensitivity values between two sets of encrypted fragments, both having a dimension of (8×8). Again, the key sensitivity property is also confirmed in this study.

5.3.2. Message sensitivity

The proposed solution has a dynamic structure and depends on variable factors that change frequently (channel nonce). Therefore, the obtained ciphertext satisfies the necessary avalanche effect and the desired security level, since for every input message, new cipher primitives are generated using the proposed update process. This, in turn, reduces the error propagation since only one round is required (unlike conventional multi-round structures).

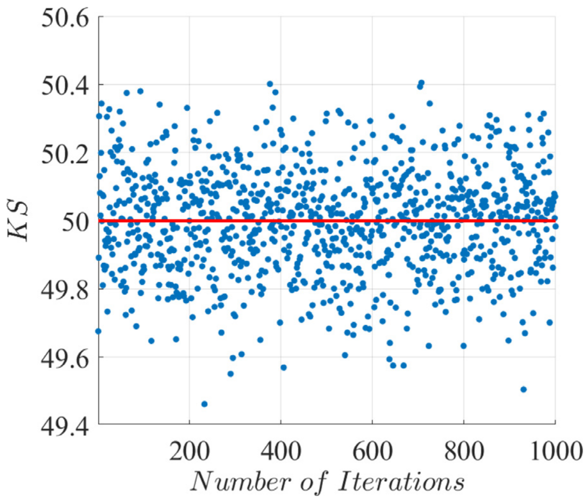


Fig. 9. Key sensitivity.

Table 6
Key sensitivity between two sets of encrypted fragments (One bit difference between both secret key (*SK* and *SK*′) and for $n = 8$.

Row index of encrypted/Column index of encrypted fragments	E1	E2	E3	E4	E5	E6	E7	E8
E1’	49.7500	49.9531	49.8203	49.4609	50.0234	50.5938	50.3359	49.6250
E2’	50.2813	49.8438	50.0703	50.2891	51.2266	50.0000	50.5703	50.0000
E3’	50.9141	50.4922	49.7813	50.8125	50.7031	49.6797	49.8281	49.6953
E4’	49.9531	49.8281	49.4297	49.3359	49.8203	50.1406	49.8203	50.1406
E5’	50.4609	49.8672	50.0781	49.7813	49.7656	49.9922	50.0156	49.3047
E6’	49.9297	50.1953	50.0313	50.1094	49.8438	49.6016	50.0625	49.3516
E7’	49.9453	50.6953	50.0938	50.0469	50.2500	50.2891	49.7344	49.7578
E8’	49.5078	49.3359	50.2031	50.1406	50.3281	50.3359	49.8594	50.0703

5.4. Brute force attacks

The size of the master session key (*MK*) can be equal to 128, 196 or 256, and the proposed secret key (*SK*) has a length of 512 bits which is sufficient to guard against brute force attacks.

All of the presented results prove that a communication session, between any two legitimate entities, is secured using the proposed scheme. The dynamic secret key is based on multiple factors, a secret and a channel-based parameter, which makes the scheme robust against *passive* and *active* adversaries.

6. Performance analysis

In this section, the performance of the proposed scheme is assessed in terms of computational complexity, execution time, communication overhead, efficiency, transparency, flexibility and error propagation.

6.1. Computational complexity and cost

The proposed scheme is based on a single round and simple operations, mainly binary matrix multiplication, substitution and permutation, to secure and encode binary input data. More specifically, data is first divided over n rows, and then each row is divided into n columns. Hence, the scheme lends itself to parallel computing, which reduces substantially the computational complexity and associated delays; each data sub-matrix can be encrypted/encoded independently from the others.

In order to validate the efficiency and simplicity of the proposed solution, we evaluated its performance in comparison to the AES scheme according to several parameters such as the associated delays of both schemes. To assess the total computational delay, we identify different types of delays as follows:

1. T_S denotes the time required by the substitution operation for one message block (iteration rounds).
2. T_P denotes the time required by the permutation operation for one message block.
3. T_D denotes the time required by the binary diffusion operation for a sub-matrix having a dimension of $(n \times n)$. It also represents the time required by the mix-column operation in AES.

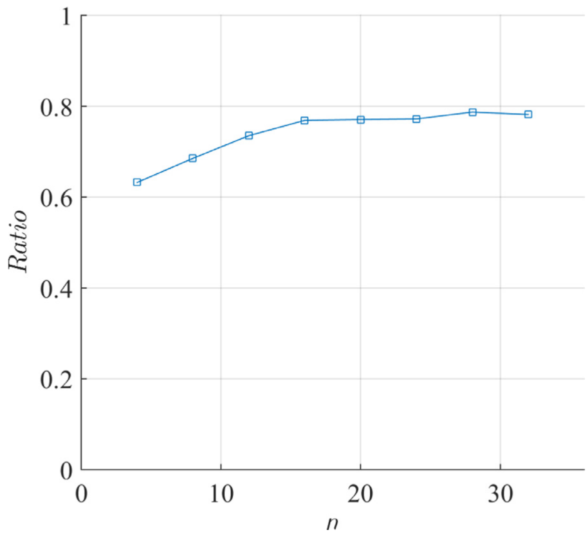


Fig. 10. The percentage reduction in execution time using binary RLNC in comparison to the conventional integer RLNC.

4. T_{SB} denotes the time required to shuffle (select) input blocks.
5. T_{xor} denotes the time required by the XOR operation.
6. T_{SR} denotes the time required by the shift row operation in AES.

The total Computational Delay (CD), required to encrypt one input block using the proposed scheme, with and without the chaining operation mode, is:

$$CD_{Proposed} = T_S + T_P + T_D + T_{SB}. \tag{9}$$

In contrast, the total CD required to encrypt one block using the standard AES [19] is:

$$CD_{AES} = rT_S + (r+1)T_{xor} + (r-1)T_D + rT_{SR}, \tag{10}$$

where r represents the number of rounds in AES. The minimum value of r is 10 for a 128-bit secret key, hence, the minimum AES computation delay is given by:

$$CD_{AES(r=10)} = 10T_S + 11T_{xor} + 9T_D + 10T_{SR}. \tag{11}$$

Clearly, the AES computational delay is larger than that of the proposed scheme, which avoids multi-diffusion operations towards reducing the required delay. Specifically, it requires only one diffusion operation in comparison to the AES algorithm, which includes 9 diffusion operations.

As a result, the computational complexity of the proposed scheme is considered acceptable compared to existing security solutions which utilize standard cryptographic algorithms [20].

6.2. Execution time

Fig. 10 illustrates the time needed to execute the proposed solution and the time savings with respect to the traditional integer RLNC mechanism. This simulation was conducted in the following software and hardware environment: Matlab on 2018 and micro-computer Intel Core 2 Duet 2.1 GHZ CPU with 2 GB RAM Intel, under Windows Live 7.

The presented result shows the execution time ratio of the proposed solution over that of integer RLNC. It is evident that binary RLNC requires a lower execution time for all matrix dimensions. In particular, a time reduction that ranges between 20% ($n > 20$) and 40% ($n < 20$) is attained. These results prove that the proposed technique is suitable for multi-homed systems and applications.

6.3. Communication overhead

This overhead will be only introduced if users choose to send redundant data to ensure data availability ($n > t$). A subset $(n-t)$ of the n available sub-channels will be utilized to send redundant data. In this case, the encoding process will generate a data communication overhead of $((n-t) \times \frac{N}{t})$ bytes. However, this overhead will increase the availability degree and the resistance against link failure and channel errors. These $(n-t)$ redundant rows are transmitted to overcome data loss, damage or alteration. Specifically, source data is encoded at the sub-matrix level. The dimension of each sub-matrix, before and after the RLNC binary encoding/decoding process, will be $(t \times t)$. A set of dynamic binary encoding matrices is used instead of a static one to enable the parallelism of the encoding/decoding process and to complicate the crypatanalysis process. The remaining $(n-t)$ sub-channels are used for the transmission of redundant rows to surpass lossy sub-channels. Whenever t is close to n, the communication overhead and availability level would decrease. In contrast, when n is greater than t, high data availability is attained and high communication overhead is also introduced. The choice of t and n depends on the communication technology and the desired availability level, and a good balance between data availability and communication overhead should be always achieved.

6.4. Efficiency

The proposed scheme utilizes simple and hardware-efficient operations, mainly byte substitution, block permutation and binary matrix mixing, to secure resource-limited devices in multi-homed systems. These operations are executed at the source and destination, where no additional operations are required at intermediate nodes such as aggregators, if they exist. In addition, the proposed message authentication step allows both, the sender and receiver, to validate the correctness of the received message before decrypting it. Therefore, the proposed solution provides multiple security services, such as data confidentiality, source authentication and message integrity, in a simple and efficient manner and with acceptable overhead and complexity.

6.5. Flexibility and scalability

Another important property of the proposed solution is that it adapts to any change in the number of communication channels, n, as well as the message length, in a seamless manner.

6.6. Error propagation

In wireless networks, interference, noise and fading are the main causes of transmission errors. This issue is inevitable due to the broadcast nature of these channels. Consequently, new security solutions should enhance the security of transmitted data and account for error propagation, at the same time. In the proposed scheme, a byte-error is only limited to the erroneous row in the received matrix, which corresponds to the noisy sub-channel/RAT. In order to overcome this issue, users can transmit data on a subset $(t < n)$ of the available n rows, which corresponds to the channels having the best performance. The remaining $n-t$ rows would carry redundant data to overcome any link error or failure. As a result, original data is received correctly and the probability of error propagation decreases, greatly.

7. Conclusion

This paper presents a novel cryptographic solution for multi-homed systems, based on the modified binary Random Linear Network Coding mechanism. To the best of our knowledge, this is the first work that modifies the Random Linear Network Coding process from the integer Galois field to the binary field. Not only does this ensure low computational complexity, but also high throughput and low energy consumption. Thus, the proposed solution is suitable for energy-constrained devices that have low computational capabilities and limited resources (mobile phones and sensors), such as the case of multi-homed devices. Moreover, the proposed scheme exploits the random physical characteristics of wireless channels, along with a pre-shared master key, to generate a secret session key, which is used to derive the needed cryptographic and update cryptographic primitives. Hence, the proposed scheme achieves data confidentiality, source authentication, message integrity, in addition to availability. The safe and efficient deployment of the proposed scheme is validated using a set of security and performance tests.

Declaration of Competing Interest

Authors declare that they have no conflict of interest.

CRediT authorship contribution statement

Reem Melki: Conceptualization, Methodology, Software, Writing - original draft, Writing - review & editing, Visualization. **Hassan N. Noura:** Conceptualization, Methodology, Software, Writing - original draft, Writing - review & editing, Visualization, Project administration, Supervision, Investigation. **Ali Chehab:** Validation, Writing - original draft, Writing - review & editing, Resources, Supervision, Project administration.

References

[1] El-Qachchach I, Habachi O, Cances J, Meghdadi V. Efficient multi-source network coding using low rank parity check code. In: Wireless communications and networking conference (WCNC). IEEE; 2018. p. 1–6.
[2] Han X, Gao F. Homomorphic error-control codes for linear network coding in packet networks. China Commun 2017;14(9):178–89.
[3] Ho T, Leong B, Koetter R, Médard M, Effros M, Karger D. Byzantine modification detection in multicast networks with random network coding. IEEE Trans Inf Theory 2008;54(6):2798–803.

[4] Zhang J, Ma L, Cai Z, Wang X. Network coding-based multipath content transmission mechanism in content centric networking. In: Proc. IEEE international conference on communication software and networks (ICCSN). IEEE; 2017. p. 1012–15.
[5] Dandachi G. Multihoming in heterogeneous wireless networks. Evry, Institut National des Télécommunications; 2017. Ph.D. thesis.
[6] Melki R, Mansour MM, Chehab A. A fairness-based congestion control algorithm for multipath TCP. In: IEEE Proc. wireless commun. net. conf. (WCNC). IEEE; 2018.
[7] Heide J, Shi S, Fouli K, Medard M, Chook V. Random linear network coding (RLNC)-based symbol representation. Working draft, IETF secretariat, internet-draft draft-heide-nwcrg-rlnc-02; 2019.
[8] Gómez D, Garrido P, Rodríguez E, Agüero R, Muñoz L. Enhanced opportunistic random linear source/network coding with cross-layer techniques over wireless mesh networks. In: Wireless days (WD), IFIP. IEEE; 2014. p. 1–4.
[9] Guo H, Chen C, Gao Y, Li X, Jin J. A secure three-factor multiserver authentication protocol against the honest-but-curious servers. Wirel Commun Mob Comput 2018;2018:1–14.
[10] Ohtake G, Safavi-Naini R, Zhang L. Outsourcing scheme of ABE encryption secure against malicious adversary. Comput Secur 2019;86:437–52.
[11] Diba R, Yaacoub E, Al-Husseini M, Noura H, Abualsaud K, Khattab T, et al. A simple approach for securing IoT data transmitted over multi-rats. In: Proc. IEEE international wireless communications & mobile computing conference (IWCMC). IEEE; 2018. p. 249–54.
[12] Demir K, Suri N. SeReCP: a secure and reliable communication platform for the smart grid. In: Proc. IEEE pacific rim international symposium on dependable computing (PRDC). IEEE; 2017. p. 175–84.
[13] Shuminoski T, Janevski T, Risteski A, Bogdanoski M. Security and QoS framework for 5G and next generation mobile broadband networks. In: Proc. IEEE EUROCON international conference on smart technologies. IEEE; 2017. p. 104–9.
[14] Xu L, Xing H, Nallanathan A, Yang Y, Chai T. Security-aware cross-layer resource allocation for heterogeneous wireless networks. IEEE Trans Commun 2018;67(2):1388–99.
[15] Xu Q, Su Z, Zheng Q, Luo M, Dong B, Zhang K. Game theoretical secure caching scheme in multi-homing edge computing-enabled heterogeneous networks. IEEE Internet Things J 2018;6(3):4536–46.
[16] Atkinson R, Bhatti S, Hailes S. Site-controlled secure multi-homing and traffic engineering for IP. In: IEEE Military communications conference (MILCOM), 28; 2009.
[17] Namal S, Gurtov A, Bennis M. Securing the backhaul for mobile and multi-homed femtocells. In: 2011 Future network & mobile summit. IEEE; 2011. p. 1–15.
[18] Venkadesh P, Dhas J, Divya S. Techniques to enhance security in SCTP for multi-homed networks. In: 2015 Global conference on communication technologies (GCCT). IEEE; 2015. p. 468–73.
[19] Prasada P, Pinto A, Ranjith H. FPGA implementation of parallel transformative approach in AES algorithm. In: Information and communication technology for competitive strategies. Springer; 2019. p. 333–40.
[20] Melki R, Noura HN, Mansour MM, Chehab A. An efficient OFDM-based encryption scheme using a dynamic key approach. IEEE Internet Things J 2018;6(1):361–78.
[21] Clarkson J. Dense probabilistic encryption. In: Proceedings of the workshop on selected areas of cryptography; 1994. p. 120–8.
[22] Zhang P, Jiang Y, Lin C, Fan Y, Shen X. P-coding: secure network coding against eavesdropping attacks. In: Proc. IEEE int. conf. computer commun. (INFOCOM). IEEE; 2010. p. 1–9.
[23] Lima L, Médard M, Barros J. Random linear network coding: a free cipher?. In: IEEE International symposium on information theory. IEEE; 2007. p. 546–50.
[24] Najeem M, Murthy C. On enhancing the random linear network coding. In: IEEE International conference on networks (ICON). IEEE; 2011. p. 246–51.
[25] Jindal P, Makkar S. Modified RC4 variants and their performance analysis. In: Microelectronics, electromagnetics and telecommunications. Springer; 2019. p. 367–74.

Reem Melki received her BS degree in electrical and computer engineering from the Rafik Hariri University in 2013, and her MS degree in 2015. She is currently a Ph.D. student at the American University of Beirut (AUB). Her main areas of research interests include security and privacy in wireless and mobile communication.

Hassan Noura received his Ph.D. degree from Polytech Nantes in 2012, France. In 2013, Noura joined Paris-Sud XI University, as a postdoctoral researcher. He got his HDR in 2016. His research interests include cryptography, network security, secure network coding, secure multimedia and secure distributed system.

Ali Chehab received his Ph.D. degree in ECE from the University of North Carolina at Charlotte, in 2002. In 2014, he became a Full Professor at AUB. His research interests include: Wireless Communications Security, Cloud Computing Security, Multimedia Security.