Hindawi
Wireless Communications and Mobile Computing
Volume 2022, Article ID 8889718, 15 pages
https://doi.org/10.1155/2022/8889718

Research Article

Network Coding-Based D2D Transmission for Public Safety Networks over LTE HetNets and 5G Networks

Chafika Tata and Michel Kadoch

Department of Electrical Engineering, École de Technologie Supérieure, Montreal, Quebec, Canada

Correspondence should be addressed to Chafika Tata; cha_aoudia@yahoo.fr

Received 13 April 2020; Revised 23 December 2021; Accepted 8 January 2022; Published 14 March 2022

Academic Editor: Chakchai So-In

Device to Device (D2D) communications appear like an emergency solution for the Public Safety Network (PSN) when the LTE cell range is limited. D2D networks can use the unlicensed frequency bands, as this makes their transmissions cheaper and easier to deploy. Therefore, the development of this technology must deal with the security challenge. On the one hand, it is important to know how to design a secure D2D solution within the small cells, and on the other hand, the new scheme needs to deal with the problem of radio resources limit, since it will be used during emergency situations. This paper develops a new algorithm, named Generalized Secure Network Coding-based Data splitting algorithm (G-SNCDS), to ensure a secure data transmission for Public Safety D2D communications over LTE Heterogeneous Networks (HetNets) and 5G networks, without using additional radio resources. Our approach consists of performing Network Coding (NC) data packets transmissions based on a new Data Splitting (DS) technique, which we developed, based on a constructed butterfly effect that uses a new Butterfly network algorithm that we propose. Our solution enhances the security without affecting the level of Quality of Service (QoS). Thus, it is more suitable when network resources are limited. The simulation results show that our approach provides a secure D2D communication without increasing the overhead in the network.

1. Introduction

Disaster management is certainly an important issue that attracts public attention. During a crisis, any information is vital to save lives. That's why the Public Safety Networks (PSNs) are deployed. It facilitates the first responders' communications through exclusive frequencies. Therefore, it allows them to make critical decisions when it lets them to get good information quality. In North America, the 700 MHz spectrum bands are dedicated to these networks.

Nowadays, PSN may also use Commercial Network (CN) resources over LTE Networks when the resources are limited or lacking. This may enhance its performance during a crisis. Therefore, sometimes, the nodes within the disaster area are unreachable, and sometimes the resources are limited. Both of these situations can affect seriously the efficiency and the reliability of the disaster management process. Thus, the Device-to-Device (D2D) [1, 2] communication, deployed in LTE Heterogeneous Networks (HetNets) [3] and 5G networks using the unlicensed frequencies have become more relevant to the Public Safety (PS) data transmission, because of its availability and the lower cost of radio resources that it uses, also for its easy deployment within the unreachable areas.

Many studies show the benefit of using local wireless networks, as Wireless Mesh Network (WMN), Wireless-Fidelity (WiFi), and Ad hoc, for D2D communications over LTE HetNets and 5G networks [4–10]. WMN is one of the unlicensed networks used within the LTE HetNets and 5G networks, to perform D2D communications for PSN. However, WMN vulnerability due to its security issue makes it continuously exposed to both internal and external security attacks. The internal attacks occur when the hacker is a legitimate node belonging to the WMN. A foreigner-misbehaving node performs the external attacks.

The different attacks can affect deeply the confidentiality, the integrity, and the availability of the transmitted information in the wireless network. The data confidentiality means that data are only reachable and known by authorized users. In other words, no information is delivered or divulged to a nonauthorized node. Data integrity means that the data have not been corrupted or changed during the transmission from the source to the destination nodes. Thus, the destination must receive the unchanged information sent from the source. Finally, the information availability consists of making the information available to the users at any time.

The transmissions within multi-hops networks are performed by broadcasting data packets. This will increase the vulnerability level and the probability of attacks in these networks. One solution, for this issue, is to use the network coding mechanism. It improves the security level by mixing symbols before transmitting them through the network. Figure 1 illustrates a network coded data transmission with the presence of an eavesdropper inside the transmission area. In such cases, the hacker can intercept the native packet B, and all other packets transmitted through the same path.

Many studies are performed to enhance the wireless networks security and to overcome the Confidentiality, Integrity, and Availability (CIA) attacks. One suitable solution to ensure a secure communication within the wireless networks is to use encryption mechanisms [11–14]. However, it is hard to overcome the additional control traffic generated by the encryption algorithms. Consequently, the level of the Quality of Service (QoS) will absolutely deteriorate because of the additional consumption of the radio resources. Furthermore, WMN networks are known for using redundancy transmissions. In fact, the network resources will become quickly saturated during disasters.

Moreover, authentication mechanism is an efficient solution to avoid unauthorized nodes to access the network. Many solutions are proposed to ensure the authentication process. Transport Layer Security (TLS) [15]; Extensible Authentication Protocol (EAP) [16]; authentication, authorization, and accounting (AAA) [17]; and Message Digest 5 (MD5) [18] are all mechanisms that are proposed in the literature to avoid eavesdroppers acceding networks. Note that this solution is unable to overcome the internal attacks, and it causes generation of additional traffic in the system.

Other proposals are given by Refs. [19–25] to increase the security level in wireless networks. Unfortunately, all of them generate additional traffic in the network. These approaches are not suitable for managing an emergency, when the resources are lacking, and where the first responders require more resources, because of the urgent need to rapid decisions, to save lives.

The authors in Ref. [26] develop a multi-part authentication solution with encryption of personal data to preserve the identity of the transmitters. This helps in reducing attacks using other users' authentication information collected during the transmission of authentication packets. Like the previous solutions, this approach generates more transmitted traffic because of the encryption process, which adds bits to each packet before transmitting it.

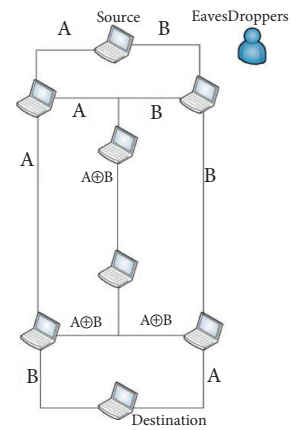


Figure 1: Network coding data packets forwarding with the presence of an eavesdropper.

The article [27] represents a solution to secure the IoT traffic transmitted between the objects to guarantee the confidentiality of private life and to preserve personal information. The solution is based on double authentication. In fact, each object must authenticate with the other object with which it communicates, this is a mutual authentication. In addition, this process includes key exchange between communicators. Although, this approach ensures a good level of security of personal data, it generates additional traffic, during authentication, exchanging keys and during data encryption operations.

The study in Ref. [28] proposes an interesting idea, which is based on the use of a central surveillance system. This one will supervise the behavior of the nodes in the transmission path and locate malicious nodes. Indeed, when a vulnerable route is discovered, this mechanism will redirect packet paths to another secure route. As a result, packets will be routed while ensuring information security. Therefore, this solution generates additional control traffic because of the surveillance process. Furthermore, during crisis situations, it becomes unlikely to find an alternative path because of the limited resources. Thus, this solution may not be efficient for these cases. It is important to mention that if no alternative route exists, the packet will either be blocked or transmitted through the native path. In the first case, the rate of blocked packets will be increased, while in the second case, information security will be compromised. Thus, in both situations, the communication will be affected.

The solution proposed in Ref. [29] uses network coding within Software-defined networking (SDN). This scheme is very promising. However, during situations of a crisis, the resources will still be limited or lack lacking.

Our objective is to develop a solution that may enhance the security level in the network without generating an extra traffic through the network. We do not aim to give the optimal solution that avoid all attacks, but just improve the security in the network by using the available resources. Therefore, our main objective is to avoid the use of more than the available resources to ensure a secure

communication. No additional resources will be used within the network to improve the security of D2D communications. This is our challenge when we propose a new secure D2D transmission mechanism based on Network Coding mechanism. Our approach is suitable for the case of disaster management, when the resources are usually limited, and when the first responders belonging to the Public Safety Networks (PSN) need to communicate well to manage the situation and make urgent decisions to save lives. Remember that in such cases, the use of radio resources by both PSN and commercial Networks (CN) increases, which make them limited.

This study develops a new algorithm, named Generalized Secure Network Coding Data Splitting algorithm (G-SNCDS), to provide a secure Data transmission for Public Safety D2D communications over LTE HetNets and 5G networks. Our approach consists of performing Network Coding Data packets transmissions based on the Data Splitting technique that we define in this paper. We develop this approach initially for avoiding only the confidentiality attacks in Ref. [30]. The native algorithm is then extended, in this article, to avoid integrity and availability attacks. Furthermore, the NC transmissions are carried out over Butterfly effects. Hence, a new approach for constructing the butterfly effect is proposed and developed in this paper. We called it Reliable Butterfly effect Construction (RBC) algorithm. The RBC mechanism allows constructing many butterfly effects in the same WMN network. In this scheme, we show how and why the use of more than one butterfly effect may efficiently avoid the integrity and the availability attacks. Joined to a new Data Splitting and Data shuffling techniques, the transmission becomes more secure. Therefore, an innovative Data Splitting scheme is proposed in this research. It is based on dividing packets into several fragments and shuffling the bit positions in the same fragment, before sending it through the transmission channel.

As mentioned above, the objective of G-SNCDS is to enhance the security level without adding a considerable quantity of control traffic even if solution is not optimal. Therefore, our simulation is performed for showing that G-SNCDS improves the security level by providing a new transmission scheme, without affecting the QoS level. Thus, it makes it harder to get the initial information by the hacker even if he or she intercepts the packets. Note that G-SNCDS is recommended when the resources are limited or lacking.

Besides, the main contribution of this paper is the development of G-SNCDS algorithm, which guarantees a secure data transmission within a mesh network without adding any control traffic, to make a D2D communication by the first responders of the Public Safety Networks. It means that the security level in the network is enhanced without affecting the QoS of the whole network. This is made possible, on the one hand, thanks to Data Splitting and the Data Shuffling schemes, which minimize the probability of intercepting meaningful information by the hackers, and on the other hand, by the simultaneous use of several butterfly effects to transmit data to avoid the integrity and availability attacks. The second contribution consists of the butterfly effects construction. Remember that not all network topologies allow decoding packets when using Network Coding scheme to enhance the network QoS, because of a lack of specific paths within these networks. Therefore, performing network coding transmissions over a butterfly network assures that decoding operation will be done successfully. Thus, building such a network in WMN is very relevant to the execution of the G-SNCDS algorithm. Moreover, the butterfly effects construction issue is addressed by only a few articles in the literature [31, 32]. As said, the use of RBC algorithm allows the construction of several butterfly networks in the WMN networks. This is very important to overcome the integrity and the availability attacks.

This paper is organized as follows. Section 2 presents the RBC algorithm. Section 3 details the G-SNCDS scheme. Section 4 summarizes the more important results of our performed simulations to validate RBC and G-SNCDS mechanisms. Section 5 concludes this article.

2. Reliable Butterfly Effect Construction

Network Coding is an efficient solution that is used to improve the wired and wireless Quality of Service networks, thanks to its capability of increasing the throughput and decreasing the end-to-end delay and packet loss in the whole network. Established by Ahlswede [33], the network coding allows simultaneous transmissions of multiple data streams arriving from one or more sources to one or more destinations. The benefits of the use of network coding in wired and wireless networks were largely studied in the literature [34–38].

The challenge of the Network Coding technology consists of finding routes and connecting the source to the destination with higher coding and decoding opportunities. Sometimes, even if the coding process is possible, the decoding scheme may not be achieved because of a lack of feasible routes. One solution to this issue is to construct a butterfly network within the wireless network before performing the network coding transmissions. Thus, the decoding process will surely be done.

Many papers explore the use of network coding in butterfly networks [39–41]; however, as mentioned above, few researches have been conducted to create a butterfly effect in a network.

The Reliable Butterfly Effect Construction (RBC) solution that we propose in this work consists of constructing a butterfly effect between a single source S and a single destination D. Figure 2 shows a Butterfly Effect implementation to connect a single source S and single destination D within a mesh network. The objective is to achieve a successful network coded data transmission within the WMN.

In this network pattern, the one hop neighbors from the source and the destination are called source's children and destination's children, respectively. Also, the two-hop nodes from the source and the destination are called grandchildren. Some nodes belong to the WMN, but they are not members of the butterfly network. The coder node in this model is a source's grandchild and the decoder is one of the destination's children set.

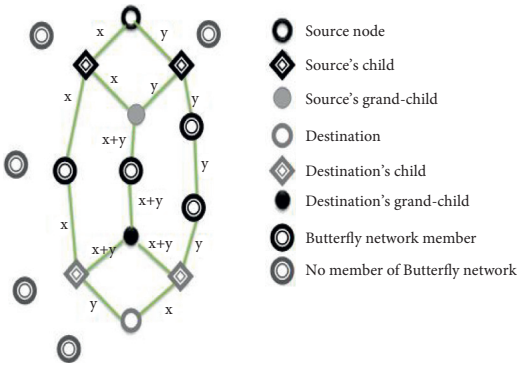


Figure 2: Butterfly effect within a wireless mesh network.

RBC algorithm is based on defining three shortest routes. The first path connects one source's child with one destination's child. The second one connects the other source's child with the second destination's child. Finally, the third path connects one source's grandchild with one destination's grandchild. The three paths need to be disjointed and the grandchildren must be the children of the source or destination's children. Several disjoined butterfly effects may be created between the same nodes pair (S, D), where S is the source node and D is the destination one. This allows for performing a load balancing of data and assures a backup mechanism in case of a butterfly effect failure.

The detailed RBC algorithm is given below.

Step 1: choose S and D randomly, from $G = (V,E)$

Step 2: find all source children

$$C(s) = \{v \in V, \text{Distance}(v, S) \leq R\}, \tag{1}$$

where $\text{Distance}(v, S)$ is the distance between the node v and the source S, and R is the coverage radius of nodes in G.

Step 3: for all $u, v \in C(S)$, find the common children of u and v, denoted by $\text{Cc}(u, v)$

$$\text{Cc}_s(u, v) = C(u) \cap C(v). \tag{2}$$

Each $w \in \text{Cc}_s(u, v)$ has two common parents denoted

$$\text{Pr}_s(w) = \{u, v \in C(S)\}. \tag{3}$$

The set of grandchildren of S, having each two parents, is denoted as $\text{GCc}(s)$

$$\text{GCc}(s) = \bigcup_{u,v \in C(S)} \text{Cc}_s(u, v). \tag{4}$$

Step 4: repeat steps 1 to 3 for the destination D to get the following equations

$$C(D) = \{v \in V, \text{Distance}(v, D) \leq R, \tag{5}$$

$$\text{Cc}_d(u, v) = C(u) \cap C(v), \tag{6}$$

$$\text{GCc}(D) = \bigcup_{u,v \in C(D)} \text{Cc}_D(u, v), \tag{7}$$

$$\text{Pr}_d(w) = \{u, v \in C(D). \tag{8}$$

Step 5: set $\alpha = 0$, where α is the number of butterfly effects in the wireless mesh network, initialized to 0.

Step 6: for all nodes $\in \text{GCc}(s)$.

(1) Find the shortest path relaying $w_1 \in \text{GCc}(S)$ to $w_2 \in \text{GCc}(D)$, denoted as e_1.

(2) If e_1 exists, find e_2, the shortest path relaying $u_1 \in \text{Pr}_s(w_1)$ to $u_2 \in \text{Pr}_d(w_2)$.

(3) If e_1 and e_2 exist, find e_3, the shortest path relaying $v_1 \in \text{Pr}_s(w_1)$ to $v_2 \in \text{Pr}_d(w_2)$.Where $v_1 \neq u_1$ and $v_2 \neq u_2$.

(4) If e_i , $i = \{1, 2, 3\}$ exist and disjoint, so set $\alpha = \alpha + 1$

(5) Construct the α^{th} butterfly network, by relaying

(i) w_1 to u_1 and v_1, u_1 and $v_1 \in \text{Pr}_s(w_1)$
(ii) w_2 to u_2 and v_2, u_2 and $v_2 \in \text{Pr}_d(w_2)$
(iii) S to u_1 and v_1
(iv) D to u_2 and v_2

(6) Representation of the α^{th} butterfly network.

$$G^{\alpha}_{\text{Bfly}} = \left(V_{\text{Bfly}}, E_{\text{Bfly}}\right), \tag{9}$$

$$V_{\text{Bfly}} = \{S, D, w_1, w_2\} \cup \text{Pr}_s(w_1) \cup \text{Pr}_d(w_2) \cup \{V_1, V_2, V_3\}, \tag{10}$$

$$V_i = \{v, (u, v) \in e_i, i = 1, 2, 3\}. \tag{11}$$

Figure 3 shows an application scenario of RBC algorithm. It illustrates the case of constructing one butterfly effect.

The Reliable Butterfly Effect Construction (RBC) solution consists of constructing a butterfly effect connecting a single source S and a single destination D.

The main objective of the RBC algorithm is to find one or more Butterfly Effects in the WMN connecting a source node S to a destination node D. Note that it is possible that no butterfly effect is present in the WMN; in such cases, no butterfly network is built by the RBC scheme. Another solution may be applied to transmit Data in this case, even if the network coding mechanism will not be achieved; our study performed in Ref. [42] may be used to find a multipath connecting a couple of source and destination nodes. This last solution assures a load balancing routing through a node-disjoined multipath.

As we had already specified in Ref. [43], our reliable approach constructs a set of butterfly effects with the same network connecting a single pair of source and destination nodes. In fact, this solution is efficient when the network suffers from links and nodes failures. The continuous availability of several backup butterfly networks guarantees the topology recovery scheme. Furthermore, the strength of our scheme appears when applying the load balancing in the mesh network. More than one butterfly effect may collaborate to transmit data by sharing the load within the

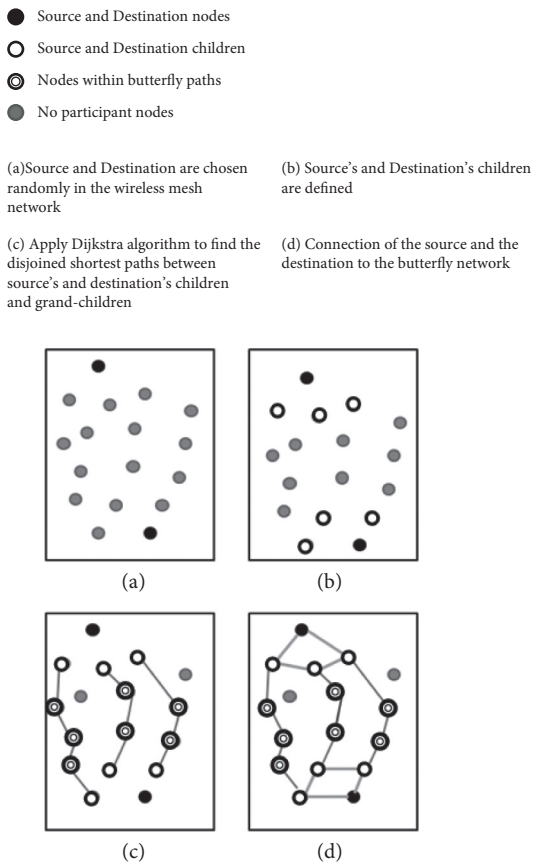


Figure 3: Steps of butterfly network construction.

same wireless mesh network. Besides, one constructed butterfly network avoids the confidentiality attack by performing a network coding data transmission based on a Data Splitting (DS) mechanism that we develop and implement in this study. Moreover, the use of two or more butterfly effects to transmit data overcomes the integrity and availability attacks. Note that CIA Attacks avoidance is assured by the G-SNCDS algorithm; this will be detailed later in this paper.

3. Generalized Secure Network Coding-Based Data Splitting Algorithm

In this work, a new approach is developed for secure network coded data transmission for PS D2D communications over LTE HetNets networks and 5G networks. The objective of this approach was to maintain the confidentiality, the integrity, and the availability of the transmitted Data over the network when resources are limited or lacking. Our solution consists of developing and applying the Data Splitting mechanism for forwarding symbols from the source to the destination nodes, over a butterfly network that we construct within the WMN network. In other words, instead of sending all packets through each path of the butterfly network, each packet will be divided, by the source node, into fragments of six bits. Thereafter, each bit position within the fragment will be changed in the same fragment according to Random Sequence Position (RSP) selected by the source, to get a shuffled sequence of bits. Finally, the bits of the same fragment will be transmitted from the source to the destination through two distinct routes. The source transmits the first bit of the shuffled sequence using the first path, the second bit by the second one, and so on until sending the whole bits of the current fragment. The process is then executed again with the next fragment, and it will be repeated until all packets are sent. We assume that the random sequence position, RSP, is encrypted by the source and sent to the destination at the beginning of the transmission by using trust modes. Otherwise, we suppose that the coding matrix format is known by the destination, but not the matrix codes values. The destination node uses the RSP to construct the coded matrix. In fact, each value of the RSP is used one or more times to construct the coding matrix. In this way, our solution reduces the quantity of encrypted data, as the RSP length is lower than that of the coding matrix.

Below, details of our DS mechanism are defined. Next, DS development and application is given. Figure 4 gives an example of Data Splitting process.

Let C be the coding matrix used for coding and decoding data by the network coding scheme.

$$C = \begin{pmatrix} c_1 & c_2 \\ c_3 + c_4 c_1 & c_4 * c_2 \\ c_5 * c_1 & c_5 c_2 + c_6 \end{pmatrix}. \tag{12}$$

With c_i, for $i = 1$ to 6 are the codes used by the three coding nodes to perform the coding operation, as shown in Figure 5. Remember that when the network coding scheme is used, two symbols are sent simultaneously by a coding node. Thus, the coding node needs to mix the two symbols together after combining each symbol with a code.

Otherwise, let $P = (p_1 p_2 p_3 p_4 p_5 p_6)$ be the Random Sequence Position vector, RSP, randomly generated by the source. Note that $p_i \in [1, 6]$, with $i = 1$ to 6, represent the positions of bits within the original fragment of the native packet. For example, for a fragment $f = 100011$, we use $P = (1,3,5,2,6,4)$, then the shuffled fragment is $f_s = 101010$. As mentioned below, the sequence RSP = P is encrypted by the source node and after that, sent to the destination. In addition, the source may send a new RSP vector each time it wants to change the shuffling sequence. This may happen when a hacker attack can succeed, or after a periodic time specified by the source. The periodic change of the RSP sequence reduces the probability of its resolution by the attackers. Hence, this may improve the robustness of our solution.

Besides, the destination gets the coding matrix C by substituting each code C_i with the value of p_i, with $i = 1$ to 6.

This approach avoids the hackers to get meaningful information by intercepting confidential Data. The eavesdropper cannot get all the bits of the packet sent because some of them are sent through another path, very probably out of its range. Furthermore, the hacker ignores the existence of RSP used by the source to shuffle the sent data. Then, this will certainly complicate the reconstruction of the native fragment. The G-SNCDS can thus reduce the impact of the confidential attacks.

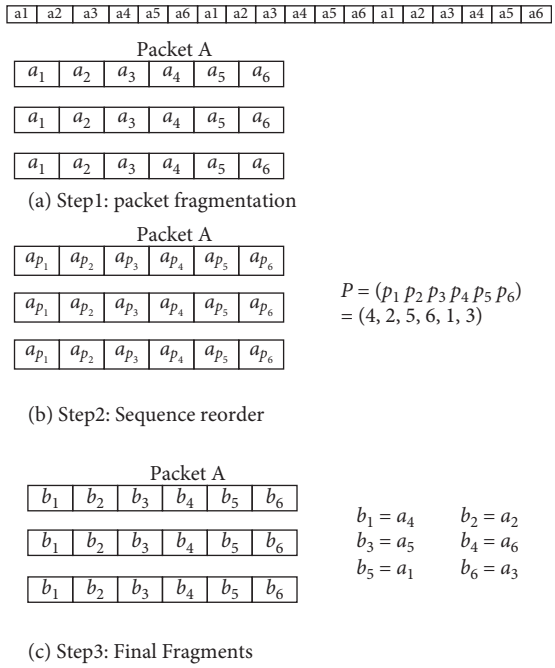


Figure 4: Example of data splitting.

In addition, the algorithm G-SNCDS uses the RBC scheme to get a set of Butterfly Effects. The transmission of Data through more than one butterfly effect allows the avoidance of the integrity and availability attacks. This will be detailed later in this paper. Note that DS scheme is applied for each Butterfly network as explained below in this article.

In the following, the DS mechanism and decoding packets will be defined and explained.

3.1. Data Splitting and Coding Operation. Figure 6 illustrates the native packet divided into fragments and transmitted by using the G-SNCDS algorithm. The choice of the value six as number of bits in one fragment is not done randomly. Our objective is to make a relationship between the number of positions of bits in the fragment and the number of codes used to code symbols in the butterfly network. In fact, the coding matrix is built by using the six codes employed by the coding nodes to generate symbols. Therefore, we propose to use the six new bit positions within the sent fragment as codes to perform the network coding operation. Note that these six new positions are represented by the sequence RSP. Furthermore, RSP gives the native position of each received bit by the destination, such that the source has to just transmit the RSP sequence to the destination, and in this one may, first, define the initial positions of bits and then construct the coding matrix used by the network coding process.

After getting the fragments of the one packet, the source shuffles each fragment in accordance to a random sequence position, RSP (Figure 6(c)). Then, the shuffled generated fragment will be transmitted from the source to the destination (Figure 6(d)).

Figure 5 illustrates the data transmission by using network coding and DS mechanisms, for a general case. Note that all bits, which are located on odd positions, will be sent

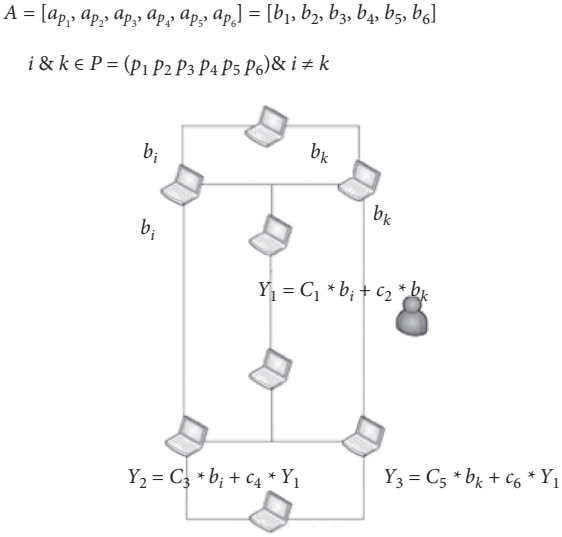


Figure 5: Network coding transmission with splitting data mechanism.

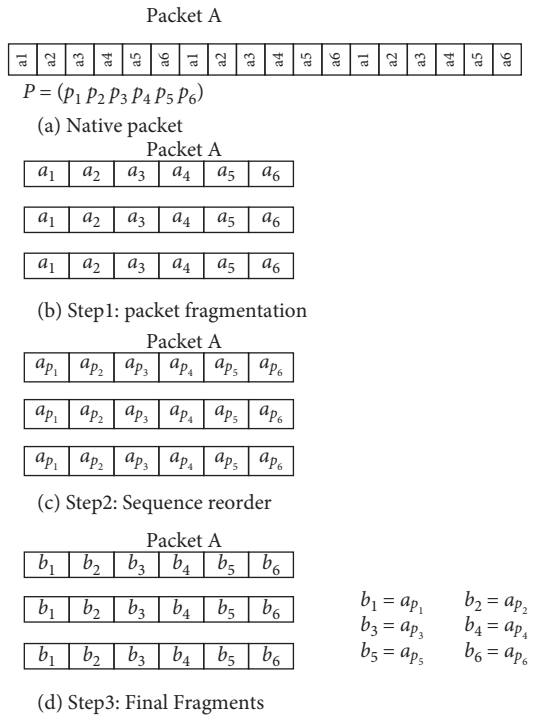


Figure 6: Data splitting mechanism. (a) Native packet. (b) Step 1: packet fragmentation. (c) Step 2: sequence reorder. (d) Step 3: final fragments.

through one path. Besides, all bits located on even positions will be sent through the second path. This approach makes our scheme capable of avoiding the confidentiality attack and reduces the number of affected packets when an integrity attack is performed.

The DS mechanism avoids the confidentiality attack since it does not allow attackers to get the whole data, because some packets are transmitted through a path, which is out of reach of the hackers. Moreover, the impact of the

integrity attack is reduced for the same reason as the confidentiality attack. In fact, 50% of packets sent do not pass by the hacker's zone. Therefore, it will be impossible for the attacker to affect this data packet. Note that *G*-SNCDS gives a solution to overcome the integrity attack, namely, the use of several butterfly effects when data are transmitted. This technique will be explained later in this paper.

Let b_i, b_k be the sent bits from the source to the destination over the butterfly network, with $i\&k \in P = (p_1p_2p_3\ p_4p_5p_6)\&i \neq k$. Let C be the coding matrix used by the network coding process. C is given by formula (12) above.

Finally, let y_j be the coded symbols, with $j \in (1, 2, 3)$. Then, the mathematical formulation of this network-coded transmission is given as follows:

$$\begin{aligned} Y_1 &= c_1 * b_i + c_2 * b_k, \\ Y_2 &= c_3 * b_i + c_4 * Y_1, \\ Y_3 &= c_5 * b_k + c_6 * Y_1. \end{aligned} \tag{13}$$

When only Y_2 and Y_3 are received by the destination, we will consider only these symbols for coding-decoding scheme. Therefore, we need to substitute Y_1 by its computed value given in (13).

So, we get the following linear system of the two equations

$$\begin{aligned} Y_2 &= c_3 * b_i + c_4 * Y_1 = (c_3 + c_4 * c_1)b_i + c_4 * c_2 * b_k, \\ Y_3 &= c_5 * b_k + c_6 * Y_1 = c_1 * c_6 * b_i + (c_5 + c_6 * c_2). \end{aligned} \tag{14}$$

Finally, we can write:

$$\begin{aligned} Y_2 &= (c_3 + c_4 * c_1)b_i + c_4 * c_2 * b_k, \\ Y_3 &= c_1 * c_6 * b_i + (c_5 + c_6 * c_2)b_k. \end{aligned} \tag{15}$$

Then, the coding scheme will be represented as follows:

$$\begin{pmatrix} y_2 \\ y_3 \end{pmatrix} = \begin{pmatrix} c_3 + c_4c_1 & c_4 * c_2 \\ c_5 * c_1 & c_5c_2 + c_6 \end{pmatrix} * \begin{pmatrix} b_i \\ b_k \end{pmatrix}. \tag{16}$$

With $i\&k \in P = (p_1p_2p_3p_4p_5p_6)\&i \neq k$
And $c_j = p_j$ for. $j \in [1, 6], p_j \in P$

3.1.1. Coding Process with DS Mechanism. An example of the application of the DS mechanism to the network coding is shown in Figure 4. The random sequence adopted for the shuffling bits position is as follows:

$$P = (p_1p_2p_3p_4p_5p_6) = (4, 2, 5, 6, 1, 3). \tag{17}$$

Consequently, the bits transmission will be done as follows:

$$(b_1, b_2, b_3, b_4, b_5, b_6) = (a_4, a_2, a_5a_6, a_1, a_3), \tag{18}$$

where b_i, $i = 1$ to 6, are the sent bits by the sources using the RSP sequence.

The source sends bits via its two paths alternatively, so that the source sends b_1, b_3 and b_5 through the first path, and b_2, b_4 and b_6 through the second one. Figure 7 shows the

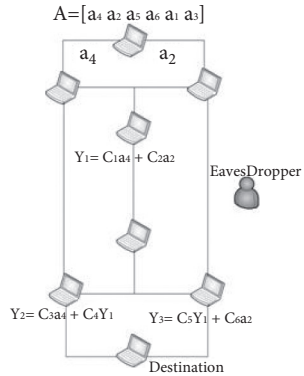


Figure 7: Example of the network coding transmission with DS mechanism.

network coding and the transmission of the bits of a fragment of the packet A, represented in Figure 7, with presence of eavesdroppers.

Mathematical formulation of this network-coded transmission is given as follows:

$$\begin{aligned} y_1 &= c_1 * a_4 + c_2 * a_2, \\ y_2 &= c_3 * a_4 + c_4 * Y_1 = (c_3 + c_4c_1)a_4 + c_4c_2a_2, \\ y_3 &= c_5 * Y_1 + c_6 * a_2 = c_5c_1a_4 + (c_5c_2 + c_6)a_2. \end{aligned} \tag{19}$$

So, the coding scheme for y_2 and y_3 will be represented as follows:

$$\begin{pmatrix} y_2 \\ y_3 \end{pmatrix} = \begin{pmatrix} c_3 + c_4c_1 & c_4c_2 \\ c_5c_1 & c_5c_2 + c_6 \end{pmatrix} * \begin{pmatrix} a_4 \\ a_2 \end{pmatrix}. \tag{20}$$

By the same way, when a_5 and a_6 are sent, we get the coded packets, namely, y_1, y_2, and y_3 as follows:

$$\begin{aligned} y_1 &= c_1 * a_5 + c_2 * a_6, \\ y_2 &= c_3 * a_5 + c_4 * Y_1 = (c_3 + c_4c_1)a_5 + c_4c_2a_6, \\ y_3 &= c_5 * Y_1 + c_6 * a_6 = c_5c_1a_5 + (c_5c_2 + c_6)a_6. \end{aligned} \tag{21}$$

So, the coding scheme will be represented as follows:

$$\begin{pmatrix} y_2 \\ y_3 \end{pmatrix} = \begin{pmatrix} c_3 + c_4c_1 & c_4c_2 \\ c_5c_1 & c_5c_2 + c_6 \end{pmatrix} * \begin{pmatrix} a_5 \\ a_6 \end{pmatrix}. \tag{22}$$

And, when both a_1 and a_3 are sent, we get the following coded packets:

$$\begin{aligned} y_1 &= c_1 * a_1 + c_2 * a_3, \\ y_2 &= c_3 * a_1 + c_4 * Y_1 = (c_3 + c_4c_1)a_1 + c_4c_2a_3, \\ y_3 &= c_5 * Y_1 + c_6 * a_3 = c_5c_1a_1 + (c_5c_2 + c_6)a_3. \end{aligned} \tag{23}$$

So, the coding scheme will be represented as follows:

$$\begin{pmatrix} y_2 \\ y_3 \end{pmatrix} = \begin{pmatrix} c_3 + c_4c_1 & c_4c_2 \\ c_5c_1 & c_5c_2 + c_6 \end{pmatrix} * \begin{pmatrix} a_1 \\ a_3 \end{pmatrix}. \tag{24}$$

Remember that $c_j = p_j$ for $j \in [1, 6], p_j \in P = (p_1p_2p_3\ p_4p_5p_6)$.

Furthermore, each time the destination gets the three coded packets y_i, with $i = 1$ to 3, it proceeds to decode them to get the couple of native symbols. The following section explains the decoding mechanism and the Data Gathering scheme.

3.2. Data Gathering and Decoding Operation. The decoding mechanism is performed by the destination. This assures that only the source and the destination may get the meaningful transmitted data.

The following mathematical model shows how the linear system of equations represents the decoding data.

The coded symbols obtained by the destination are represented by formula (16). The three following matrixes are considered:

$$Y = \begin{pmatrix} y_2 \\ y_3 \end{pmatrix},$$
$$C = \begin{pmatrix} c_3 + c_4c_1 & c_4c_2 \\ c_5c_1 & c_5c_2 + c_6 \end{pmatrix}, \quad (25)$$
$$A = \begin{pmatrix} a_1 \\ a_3 \end{pmatrix}.$$

Then, formula (22) may be adapted as follows:

$$Y = C * A. \quad (26)$$

By applying the properties of linear algebra, we can get the joined formula (27).

$$\begin{cases} C - 1 * Y = C - 1 * C * A, \\ C - 1 * Y = \mathrm{Id} * A \text{ with Id is the Identity matrix}, \\ C - 1 * Y = A, \\ \text{Then}, \\ A = C - 1 * Y. \end{cases} \quad (27)$$

So that, we define system (28) obtained by substituting A, C, and Y by the corresponding matrix according to equation (27).

$$\begin{pmatrix} a_i \\ a_j \end{pmatrix} = \begin{pmatrix} c_3 + c_4c_1 & c_4c_2 \\ c_5c_1 & c_5c_2 + c_6 \end{pmatrix}^{-1} * \begin{pmatrix} y_2 \\ y_3 \end{pmatrix}. \quad (28)$$

Besides, the C^{-1} matrix has to be defined in order to get the final values of a_i and a_j.

$$\text{Let } M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}. \quad (29)$$

In linear algebra, the invert matrix M^{-1} of M is calculated as follows:

$$M^{-1} = \frac{1}{\mathrm{Det}(M)} (\mathrm{CoFactors}(M))^t. \quad (30)$$

With Det (M) being the determinant of the matrix M and $(\mathrm{CoFactors}(M))^t$ being the transpose of the cofactor's matrix of M.

The determinant of the matrix M is given by formula (31)

$$\mathrm{Det}(M) = a * d - c * b. \quad (31)$$

Besides, the cofactors matrix of M is given as follows:

$$\mathrm{CoFactors}(M) = \begin{pmatrix} d & -c \\ -b & a \end{pmatrix}. \quad (32)$$

Then,

$$(\mathrm{CoFactors}(M))^t = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}. \quad (33)$$

Note that a Matrix M is invertible if and only if

$$\mathrm{Det}(M) \neq 0. \quad (34)$$

So, by considering formulas (30), (31), and (33), the invert matrix of C will be given by formula (35).

$$C^{-1} = \frac{1}{\mathrm{Det}(C)} (\mathrm{CoFactors}(C))^t, \quad (35)$$

$$\mathrm{Det}(C) = (c_3 + c_4 * c_1) * (c_5 * c_2 + c_6) - (c_5 * c_1) * (c_4 * c_2), \quad (36)$$

$$(\mathrm{CoFactors}(C))^t = \begin{pmatrix} c_5c_2 + c_6 & -c_4c_2 \\ -c_5c_1 & c_3 + c_4c_1 \end{pmatrix}. \quad (37)$$

Remember that $c_j = p_j$ for. $j \in [1, 6]$, $p_j \in P = (p_1p_2p_3p_4p_5p_6)$

Once the destination gets and decodes one sequence of subsequent six bits, it will put the bits in the initial order. To do this, it uses the RSP sequence $P = (p_1p_2p_3p_4p_5p_6)$, obtained from the source at the beginning of the data transmission. Therefore, the initial position of the first received bit is equal to p_1, the native position of the second one is p_2, and so on. Finally, each fragment will be joined to the previous one to get the native transmitted packet.

3.2.1. Example of Decoding Operation. We consider the example given in Figure 7. In this section, we detail only the decoding process of the two sent bits, namely, a_4 and a_2. The coded packets are given above, by formula (20)

The decoded symbols a_4 and a_2 are obtained by using formula (38).

$$\begin{pmatrix} a_4 \\ a_2 \end{pmatrix} = \begin{pmatrix} c_3 + c_4c_1 & c_4c_2 \\ c_5c_1 & c_5c_2 + c_6 \end{pmatrix}^{-1} * \begin{pmatrix} y_2 \\ y_3 \end{pmatrix}. \quad (38)$$

With $(c_1c_2c_3c_4c_5c_6) = (p_1p_2p_3p_4p_5p_6) = (4, 2, 5, 6, 1, 3)$ Then, we may write:

$$\begin{pmatrix} a_4 \\ a_2 \end{pmatrix} = \frac{1}{97} * \begin{pmatrix} 5 & -12 \\ -4 & 29 \end{pmatrix} * \begin{pmatrix} y_2 \\ y_3 \end{pmatrix}. \quad (39)$$

3.3. Generalized Secure Network Coding-Based Data Splitting Algorithm. In this section, we present the G-SNCDS algorithm. The previous sections explain the definitions and the mechanisms used within the G-SNCDS algorithm and cited in this section.

Step 1: the source applies RBC Algorithm to find the set of the butterfly effect in the WMN network. If no butterfly network is found, so go to step 6.

Step 2: the source defines and encrypts the RSP sequence and sends it to the destination.

Step 3: the sources split the data to sequences of six bits and shuffles them following the RSP sequence.

Step 4: the splitting and shuffling data are sent to the destination by using network coding mechanism through the butterfly networks, constructed by the RBC algorithm.

Step 5: once the destination gets and decodes a sequence of six bits, it will put the sequence in the initial order. To do this, it uses the RSP sequence $P = (p_1p_2p_3p_4p_5p_6)$, which it obtains from the source at the beginning of the data transmission. Therefore, the position of the first received bit is equal to p_1, the position of the second one is p_2, and so on. Finally, each fragment will be added to the previous one to get the native transmitted packet.

Step 6: use multipath algorithm that we have developed in Ref. [42].

3.4. G-SNCDS for Confidentiality Attack Avoidance. G-SNCDS solution can overcome a confidentiality attack in a mesh network. In this case, it proceeds as our previous solution is called the SNCDS algorithm [30]. The objective of G-SNCDS when it is applied to avoid a confidentiality attack is to keep the eavesdroppers away from the confidential information transmitted through the WMN.

To show the G-SNCDS efficiency on confidentiality attack avoidance, we consider the attacks illustrated in Figure 8. This figure represents two kinds of attacks in a butterfly network. An internal attack performed by the eavesdropper 1 and an external one accomplished by the eavesdropper 2.

In both situations, eavesdroppers cannot get the full information sent by the source to the destination. Even if the eavesdropper 1 may intercept the coded symbol Y1, certainly, he or she cannot resolve this symbol since he or she does not have the codes belonging to the encrypted coded matrix. In such a case, we assume that the eavesdroppers have no capabilities to resolve the encryption keys used by the source and the destination. Besides, eavesdropper 2 may only get to send the bits relevant to odd positions. In addition, positions of captured bits are not the same for these bits in the native packet, so that it will be complicated for him or her to reconstruct the native packet.

3.4.1. G-SNCDS for Data Integrity Attack Avoidance. Figure 9 illustrates an internal integrity attack within a WMN. Two legitimate nodes are assumed to be hackers. The considered attack in this case is a packet drop by the hackers. In other words, instead of forwarding packets arriving to their hosts, they will partially or totally drop them. Such a situation modifies the integral data transmitted from the source to the destination. In fact, the integrity of the transmitted data will be affected.

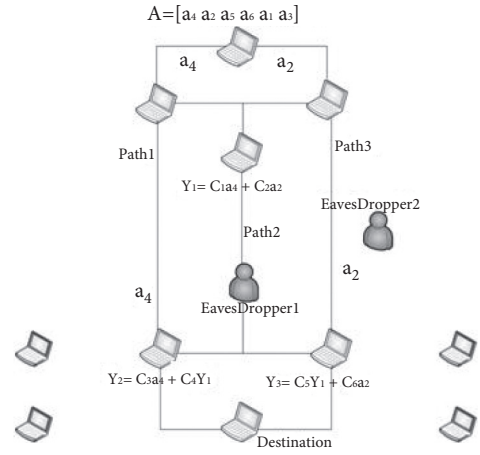


FIGURE 8: Confidentiality attack: internal and external attacks in the WMN.

When one butterfly effect is used to forward data within the WMN (Figure 9(a)), the integrity of the information is not guaranteed, because when the DS mechanism is applied, part of the data is sent through the first path and the other part takes the second path. Consequently, some or all data arriving at the two hackers will be lost. Thus, the destination may not have the whole information and the decoding process will be blocked because of the lack of some information depending on the decoding scheme. A solution is to apply G-SNCDS to this D2D transmission. G-SNCDS uses two butterfly effects to perform double NC operation (Figure 9(b)), and the data are transmitted by applying a redundancy mechanism. Each packet forwarded through the first butterfly network is duplicated and sent via the second butterfly in the same manner, so the G-SNCDS uses the same shuffled sequence to transmit the packets. If an integrity attack occurs in the network, the destination will detect it after the duration of time by realizing that some packets are dropped. Therefore, the network will use the redundant data to correct the information corruption. Note that in the case of an external integrity attack, the same process as the one applied to the internal integrity attack will be applied to overcome the packet corruption issue.

3.4.2. B. G-SNCDS for Data Availability Attack Avoidance. Figure 10 represents Deny of Service (DoS) attack as an example of internal availability attack in WMN. The two hackers are assumed to be legitimated nodes belonging to one butterfly effect. The first situation (Figure 10(a)) illustrates the use of one butterfly effect to transmit data with two misbehaving nodes. The other situation (Figure 10(b)) represents the case of use of two butterfly effects by G-SNCDS for transmitting D2D data. The second butterfly

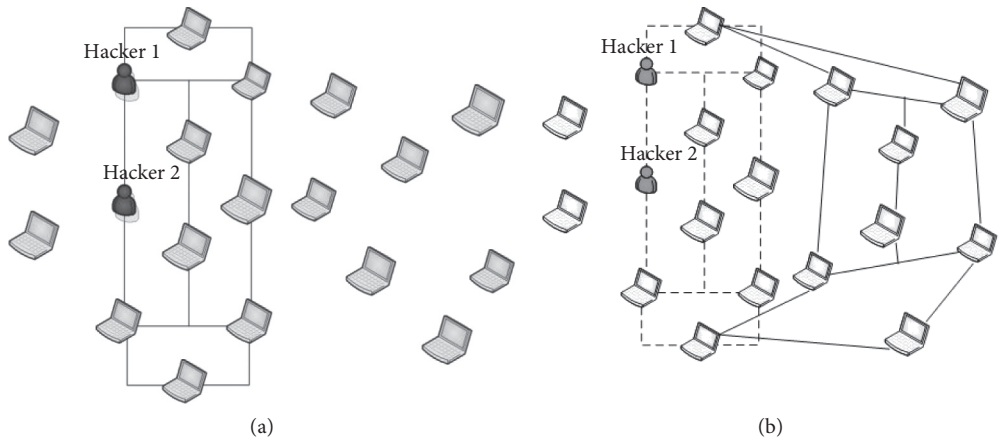


Figure 9: Integrity attack: Internal attack within the WMN. (a) Hackers drop packets: Information integrity is not guaranteed. (b) Hackers drop packets, G-SNCDS applied: Information availability is guaranteed.

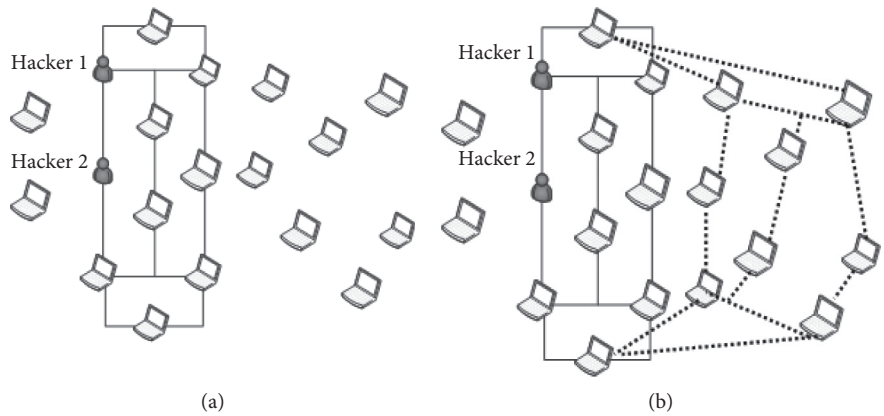


Figure 10: Availability attack (DoS attack): internal attack within the WMN. (a) Without G-SNCDS: information availability is not guaranteed. (b) G-SNCDS is applied: information availability is guaranteed.

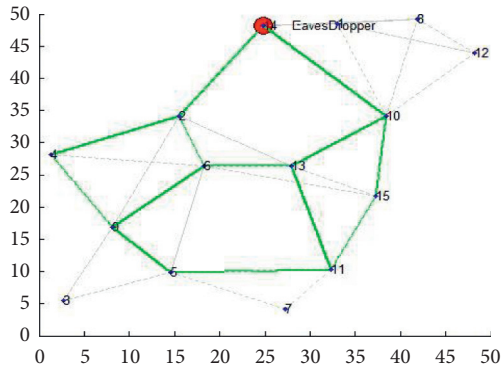
network is considered as a backup network; it will not be used until the first one becomes unavailable. Therefore, when hackers perform a DoS attack, the solution in Figure 10(a) may not guarantee the availability of the data. In fact, the transmission within the butterfly will be blocked because of the DoS attack. Besides the use of G-SNCDS allows for overcoming the availability attack, as soon as the principal butterfly stops delivering the packet to the destination because of the DoS attack, G-SNCDS will activate the backup butterfly network and switch the transmission operation from the first butterfly network to the second one. Note that the application of the RBC algorithm allows for constructing a set of butterfly effects for each couple of nodes needing to exchange data between them. So, G-SNCDS has a high probability to address the availability attack issue.

Note that the backup network can use the same or a different RSP. When the source decides to use a new RSP sequence, it has to notify the destination about the new RSP vector. Otherwise, the destination may not perform a decoding operation. As the integrity attack avoidance is carried out by G-SNCDS, the availability attack avoidance is applied in the same way for both external attack and the internal one.

4. Simulation and Results

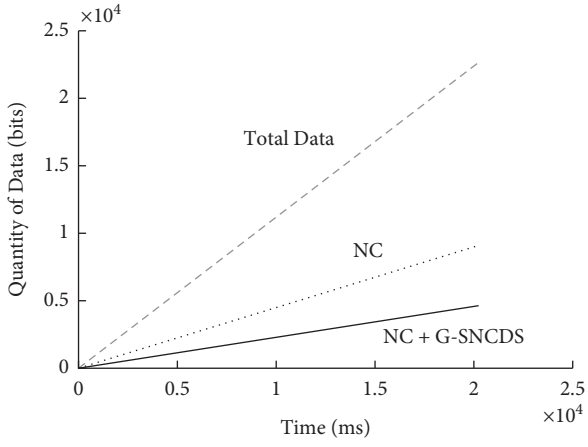
In this section, we show the results of the G-SNCDS algorithm implementation carried out in Matlab. The aim of our experiments is to illustrate that our scheme enhances the security level in the mesh network without adding significant additional control traffic. Three kinds of attacks are implemented, namely, the confidentiality attack, the integrity attack, and the availability one. All these attacks are addressed by the G-SNCDS. The use of the DS mechanism during the network coding transmission may overcome the confidentiality attacks. Otherwise, the use of the butterfly backup network combined with the DS mechanism avoids the availability and the integrity attacks.

For each experiment, the source, the destination, and the eavesdropper nodes are chosen randomly among all forwarding nodes in the WMN network. The RBC algorithm is applied to construct the set of butterfly networks between the source and the destination nodes (Figures 11 and 12). The first kind of security attack experimented in this work is the confidentiality attacks. Two scenarios are simulated, the internal attack and the external attack scenarios. Note that



- Node 1: Source node.
- Node 15: Destination node.
- Red node: eavesdropper.
- Green links: Butterfly network links.
- Dushed links: WMN links

Figure 11: Internal eavesdropping attack.



Total Data
NC + G-SNCDS
NC

Figure 12: External eavesdropping attack.

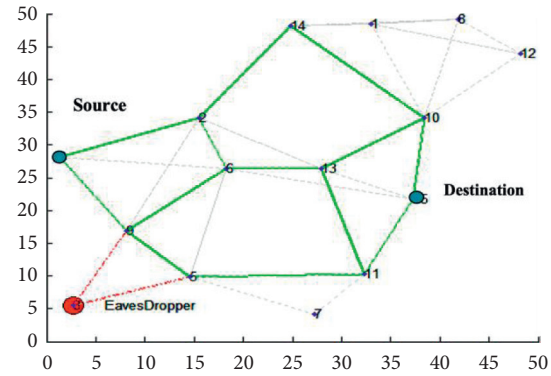
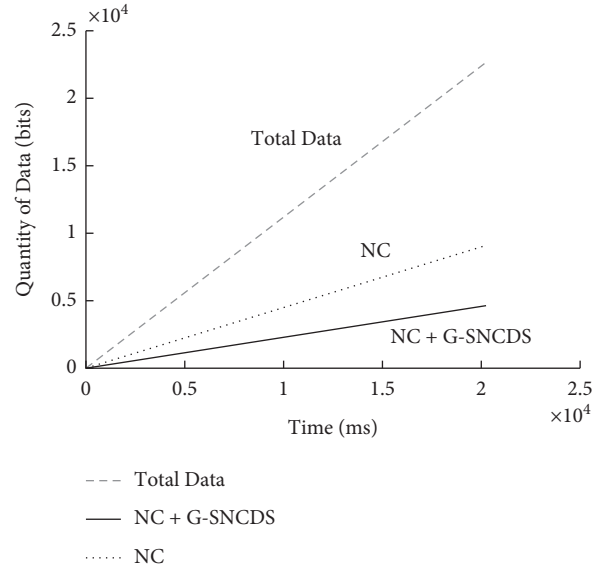


Figure 13: Transmitted data vs. intercepted data (internal attack).



Total Data
NC + G-SNCDS
NC

Figure 14: Transmitted data vs. intercepted data (external attack).

for confidentiality attack, the G-SNCDS algorithm can use only one butterfly effect to overcome this situation.

Figure 11 illustrates the butterfly network constructed by the RBC algorithm. This scenario is performed to analyze the internal attack. The eavesdropping node is a member of the butterfly network. In such cases, the hacker may have part of the transmitted data from its neighbors. The captured information may be sent to it or intercepted among the data transmitted to its neighbors, which are in its transmission range.

Therefore, the application of the G-SNCDS decreases the number of the intercepted data by the eavesdropper node in both internal and external attacks (Figures 13 and 14). This is made possible thanks to the application of the DS mechanism. Remember that the DS scheme consists of dividing each sent packet into two parts; one part is transmitted through a path of the butterfly network and the second part through the other path. This approach decreases the number of bits obtained by any eavesdropping nodes as compared to the scheme when sending the whole packets through the two lateral paths of the butterfly network.

Based on the Butterfly effects constructed by the RBC algorithm and represented by Figures 11 and 12, respectively, we notice that the number of intercepted data is higher in the case of the internal attack (Figure 13) than in the case of external data (Figure 14). This is because of the location of the hacker in the network. Figure 13 shows that the eavesdropper may get the information sent to it from node 2 and intercept the information sent to node 10, which is a coded symbol. The number of the intercepted bits may be greater with the internal eavesdropping attack than the external one.

Note that our solution avoids the eavesdropped node to get any meaningful information thanks to the splitting operation, which makes a part of the packet unreachable for this node and complicates the bits gathering process since it does not know about the data shuffling mechanism adopted

by the source node. This benefit is not given by the classical NC transmission, where the source forwards the whole packet bits using the same path. Data eavesdropping in the classical NC transmissions becomes easy for the hacker, since the information is not encrypted.

The second attack type considered in this simulation is the integrity attack (Figure 15). It is realized through packet drops by the hacker. As it is explained in Section 3.4, G-SNCDS realizes a split network coded data transmission through at least two butterfly effects, to overcome the integrity attack. The first one is the main butterfly network and the second one is the backup one. When the hacker performs an attack through one butterfly network, the data transmitted over it will be immediately corrupted. The information arrived at the destination via the two butterfly networks will be certainly different. Thus, the destination will use correction mechanism to get the native data. In this simulation, we carried out three scenarios (Figure 15).

The first scenario, called the NC scenario, is realized by using only a network coding scheme through one butterfly network.

The second scenario consists of applying the SNCDS solution interpreted by performing Network Coding transmission over one butterfly effect combined with DS mechanism. This experiment is called the SNCDS scenario.

The last scenario applies to the G-SNCDS algorithm. This solution is realized by transmitting data through two butterfly networks and using network coding combined with DS schemes. It is named the G-SNCDS scenario.

The simulation results show, on one hand, that applying the SNCDS algorithm enhances the security level compared to the case of using only the network coding mechanism to transmit packets. This is made possible thanks to the use of the DS approach. When the DS scheme is applied, only half of the data is forwarded via the path including the malicious node. We show that the application of the G-SNCDS assures total integrity attack avoidance with the presence of hackers in the network. The implementation of two butterfly networks transmitting redundant data allows the destination node to detect the packet corruption, so that correction algorithms can be executed to get the native data.

The availability attack is the last type of attacks we consider. In this study, we consider the Denial of Service (DoS) to simulate the availability attack. Our simulation results are illustrated in Figure 16. Like the integrity attack, three scenarios are implemented. A network coding transmission, a NC solution combined with DS mechanism (SNCDS), and a G-SNCDS algorithm. The two first solutions are applied as in the integrity attack scenario. The last solution is applied by using NC mechanism with the DS one over one butterfly network. As soon as availability attack occurs, the second butterfly network is used to transmit data instead of the first.

Figure 16 shows that the NC solution and SNCDS solution give the same results for this experiment. In fact, the two approaches use one butterfly network and when a DoS attack happens, the whole network is affected, and all transmissions are blocked. Besides, the G-SNCDS may avoid a DoS attack, thanks to the butterfly network backup. Thus, as soon as the attack is detected in the network, the principal

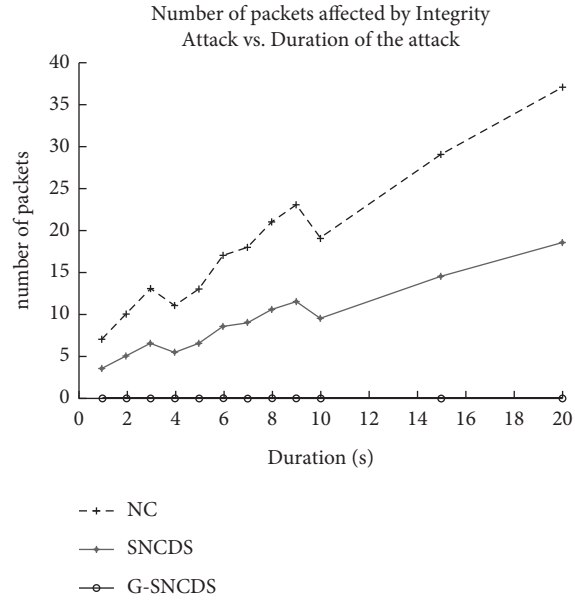


Figure 15: Number of affected packets in a mesh network by an integrity attack vs. the duration of the attack.

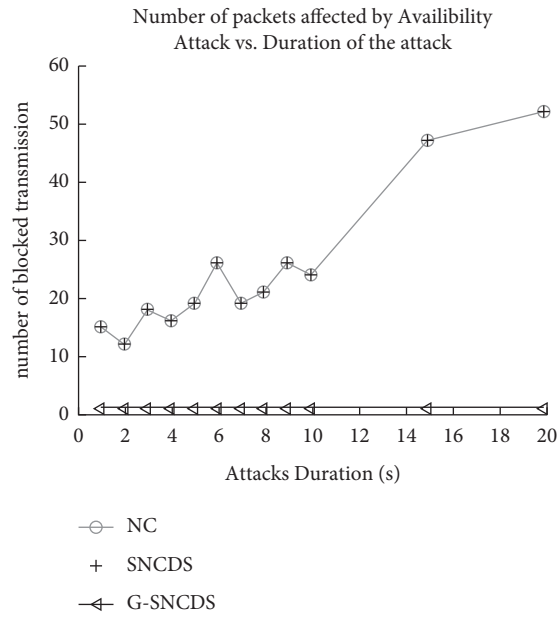


Figure 16: Number of blocked packets in a mesh network by an availability attack vs. the duration of the attack.

butterfly network is disabled and the backup is activated to rescue the data transmission in the network.

Otherwise, the encryption is an interesting solution to preserve the routed data in the network, but it needs to add some bits to the native packet to encrypt it. Authors in Refs. [44, 45] evaluate the encryption overhead for many encryption algorithms. In fact, the combined added bits serving the encryption scheme will increase the overhead in the butterfly network and will use additional network resources, even in situation of congestion, where the radio and bandwidth resources are limited. One important

contribution of the G-SNCDS is the guarantee of a secure data transmission for the PS D2D transmission without adding any control traffic other than the one used by the Network Coding scheme. This is made possible since the G-SNCDS does not add any bit to the transmitted one. It rather uses a Data Splitting mechanism combined with bit Shuffling process to avoid the confidentiality, integrity, and availability attacks in the WMN networks.

Furthermore, the proposed approach, namely, the G-SNCDS algorithm combined to RBC one is a scalable solution for secure routing within the WMN network for ensuring a reliable Public Safety D2D communications, over HetNets and 5G networks. In fact, the Butterfly effects' construction is relevant to the availability of paths connecting the children and the grandchildren of the source and the destination nodes; this will assure the decoding process in the network. It is evident that the greater the number of nodes in the WMN network, the greater the number of butterfly effects constructed by RBC. In addition, whatever the number of nodes in the WMN network, the G-SNCDS solution is suitable to assure a good level of security, while the construction of butterfly networks is possible.

Remember that in this work, we try to secure Data while prioritizing communication in situations of crises, where resources are limited. Indeed, with the same amount of traffic we will increase the level of security, so no additional traffic will be added. In fact, we are trying to secure communications, because it could be confidential data exchanged between first responders, so we ensure confidentiality. It could also be important information; there we must ensure the availability of Data, it is also necessary to have the information in its totality, so we need to guarantee the integrity of this information. Therefore, the three aspects: availability, confidentiality, and integrity, must be ensured during D2D communications made by first responders, as well as the guarantee of data transmission.

Finally, the article complements studies we made in other papers [46, 47], improving QoS in LTE networks and LTE HetNets networks. The objective here is to improve the security of D2D communications in local networks. Remember that D2D communications are part of HetNets networks and 5G networks. D2D communications are relevant when LTE resources become limited and eNodeB coverage does not reach the disaster zone.

5. Conclusion

D2D technology is an attractive solution to enhance the performance of Public Safety communications over LTE Heterogeneous networks and 5G networks, particularly when the Public Safety access to the shared commercial radio bands over LTE cannot overcome the lack of PS resources during crisis. D2D communications allow direct transmission of data between hosts, without passing through an eNodeB. The nodes may operate within public frequencies, as in Ad hoc, WiFi, or WMN wireless networks. Unfortunately, the use of the unlicensed bands cannot provide the same security level as with the licensed ones.

In this work, we investigate the security issue in a Device-to-Device Public Safety communications over LTE Heterogeneous networks and 5G networks. The D2D communications are performed within a mesh network deployed in small cells and used for offloading the macro cell during congestion situations. The Transmission data uses the Splitting Data mechanism and the Network Coding scheme over a butterfly network. The butterfly effect is defined within the WMN network to connect the source node to its destination. Besides, three kinds of attacks are considered in this study, namely, the confidentiality attack, the integrity attack, and the availability one.

A new solution is implemented to deal with the security problem within the WMN networks, namely, the Generalized Secure Network Coding-based Data splitting algorithm (G-SNCDS). G-SNCDS is based on Network Coded Data splitting mechanism. It is an inherent solution to avoid confidentiality, integrity, and availability attacks.

Furthermore, this paper presents two other principal contributions; the first one is the implementation of a new Data Splitting mechanism. It is applied to the network coding transmission, in order to overcome the confidentiality attacks in the WMN networks. The second contribution consists of the implementation of a novel algorithm, namely, Reliable Butterfly Construction algorithm (RBC), to construct a reliable butterfly effect in the WMN networks and to connect the source to the destination node. Remember that using butterfly effect to perform network coding transmissions guarantees the success of the coding-decoding process. Note that the RBC scheme is applied by G-SNCDS to avoid both the integrity and the availability attacks in WMN networks.

The simulation results show that the confidentiality attacks are avoided since the data packet intercepted by the eavesdropper is no meaningful information. The two other types of attacks are completely avoided by G-SNCDS when more than one butterfly effects are used for the data transmission. The G-SNCDS advantage is reflected by the security level improvement within the WMN networks. This is without adding any traffic control in the network.

Data Availability

Data used to support the findings of this study are available from the corresponding author (chafika.tata.1@ens.etsmtl.ca) upon request and are obtained from the previous study (http://www.wseas.us/e-library/conferences/2014/Tenerife/INFORM/INFORM-35.pdf).

Conflicts of Interest

The authors declare that they have no conflicts of interest.

References

[1] X. Lin, J. G. Andrews, A. Ghosh, and R. Ratasuk, "An overview on 3GPP device-to-device proximity services," 2013, https://arxiv.org/abs/1905.03969.

[2] B. Raghothaman, E. Deng, R. Pragada, G. Sternberg, T. Deng, and K. Vanganuru, "Architecture and protocols for LTE-

based device to device communication," in *Proceedings of the 2013 International Conference on Computing, Networking and Communications (ICNC)*, pp. 895–899, San Diego, CA, USA, January 2013.

[3] G. Wu, Q. C. Li, R. Q. Hu, and Y. Qian, *Heterogeneous Cellular Networks*, , Wiley, Hoboken, Ny, USA, 2013pp. 1–25, Overview of Heterogeneous Networks.

[4] S. Mumtaz, H. Lundqvist, K. M. S. Huq, J. Rodriguez, and A. Radwan, "Smart Direct-LTE communication: an energy saving perspective," *Ad Hoc Networks*, vol. 13, pp. 296–311, 2014.

[5] D. H. Hagos, "The performance of WiFi offload in LTE networks," Master's Thesis, Lulea University of Technology, Sweden, Europe, 2012.

[6] V. Nagpal, S. Choudhury, and K. Doppler, *Offloading Traffic to Device-To-Device Communications*, 2013.

[7] A. Pyattaev, K. Johnsson, S. Andreev, and Y. Koucheryavy, "3GPP LTE traffic offloading onto WiFi direct," in *Proceedings of the IEEE WCNC*, Shanghai, China, April 2013.

[8] G. Fodor, S. Sorrentino, and S. Sultana, "Network assisted device-to-device communications: use cases, design approaches, and performance aspects," in *Smart Device to Smart Device Communication*, pp. 135–163, Springer, Berlin, Germany, 2014.

[9] S. Andreev, A. Pyattaev, K. Johnsson, O. Galinina, and Y. Koucheryavy, "Cellular traffic offloading onto network-assisted device-to-device connections," *IEEE Communications Magazine*, vol. 52, no. 4, pp. 20–31, 2014.

[10] L. Lei, Y. Zhang, X. Shen, C. Lin, and Z. Zhong, "Performance analysis of device-to-device communications with dynamic interference using stochastic petri nets," *IEEE Transactions on Wireless Communications*, vol. 12, 2013.

[11] J. Zhou, "Efficient and secure routing protocol based on encryption and authentication for wireless sensor networks," *International Journal of Distributed Sensor Networks*, vol. 2013, Article ID 108968, 2013.

[12] S. Zhao, R. Kent, and A. Aggarwal, "A key management and secure routing integrated framework for Mobile Ad-hoc Networks," *Ad Hoc Networks*, vol. 11, no. 3, pp. 1046–1061, 2013.

[13] Z. Tang, "On link encryption against wiretapping attack in network coding," *Networking Science*, vol. 2, no. 3, pp. 81–90, 2013.

[14] N. B. Shah, K. Rashmi, and K. Ramchandran, "Secure network coding for distributed secret sharing with low communication cost," in *Proceedings of the 2013 IEEE International Symposium on Information Theory Proceedings (ISIT)*, pp. 2404–2408, Istanbul, Turkey, July 2013.

[15] S. Fischer, C. Rensing, and U. Rödig, "Transport layer security," in *Open Internet Security*, pp. 215–248, Springer, Berlin, Germany, 2000.

[16] B. Aboba, L. Blunk, J. Vollbrecht, J. Carlson, and H. Levkowetz, "Extensible authentication protocol (EAP)," *RFC*, vol. 3748, 2004.

[17] C. Metz, "AAA protocols: authentication, authorization, and accounting for the Internet," *IEEE Internet Computing*, vol. 3, no. 6, pp. 75–79, 1999.

[18] R. Rivest, *The MD5 Message-Digest Algorithm {RFC-1321}*, RFC Editor, US, 1992.

[19] J. Sen, S. Koilakonda, and A. Ukil, "A mechanism for detection of cooperative black hole attack in mobile ad hoc networks," in *Proceedings of the 2011 Second International Conference on Intelligent Systems, Modelling and Simulation (ISMS)*, pp. 338–343, Phnom Penh, Cambodia, January 2011.

[20] N. Shah and S. Valiveti, "Intrusion detection systems for the availability attacks in ad-hoc networks," *International Journal of Electronics and Computer Science Engineering (IJECSE)*, vol. 1, pp. 1850–1857, 2012.

[21] D. Prasad and M. Giri, "Efficient lightweight hybrid cryptography solution to secure mobile ad hoc networks," *IJRCCT*, vol. 3, pp. 325–332, 2014.

[22] A. D. Kent and L. M. Liebrock, "Secure communication via shared knowledge and a salted hash in Ad-hoc environments," in *Proceedings of the 2011 IEEE 35th Annual Computer Software and Applications Conference Workshops (COMPSACW)*, pp. 122–127, Munich, Germany, July 2011.

[23] D. He, S. Zeadally, N. Kumar, and J.-H. Lee, "Anonymous authentication for wireless body area networks with provable security," *IEEE Systems Journal*, vol. 11, no. 99, pp. 1–12, 2016.

[24] K. Gai, M. Qiu, L. Tao, and Y. Zhu, "Intrusion detection techniques for mobile cloud computing in heterogeneous 5G," *Security and Communication Networks*, vol. 9, no. 16, pp. 3049–3058, 2016.

[25] K. Xiao, L. Gong, and M. Kadoch, "Opportunistic multicast NOMA with security concerns in a 5G massive MIMO system," *IEEE Communications Magazine*, vol. 56, no. 3, pp. 91–95, 2018.

[26] Y. Zhang, F. Ren, A. Wu, T. Zhang, J. Cao, and D. Zheng, "Certificateless multi-party Authenticated encryption for NB-IoT terminals in 5G networks," *IEEE Access*, vol. 7, pp. 114721–114730, 2019.

[27] D. Shin, K. Yun, J. Kim, P. V. Astillo, J.-N. Kim, and I. You, "A security protocol for route optimization in DMM-based smart home IoT networks," *IEEE Access*, vol. 7, pp. 142531–142550, 2019.

[28] V. Priya and B. Sakthisaravanan, "Information centric network for secure data transmission in DTN," in *Proceedings of the International Confernce on Innovation Information in Computing Technologies*, pp. 1–4, Chennai, India, February 2015.

[29] J. Hansen, D. E. Lucani, J. Krigslund, M. Medard, and F. H. P. Fitzek, "Network coded software defined networking: enabling 5G transmission and storage networks," *IEEE Communications Magazine*, vol. 53, no. 9, pp. 100–107, 2015.

[30] C. Tata and M. Kadoch, "Secure network coding based data splitting for public safety D2D communications over LTE heterogeneous networks," in *Proceedings of the CIT 14*, Tenerife, Spain, January 2014.

[31] A. Shalaby, V. Goulart, and M. E.-S. Ragab, "Study of application of network coding on NoCs for multicast communications," in *Proceedings of the 2013 IEEE 7th International Symposium on Embedded Multicore Socs (MCSoC)*, pp. 37–42, Tokyo, Japan, September 2013.

[32] A. Shalaby, M. Ragab, and V. Goulart, "Intermediate nodes selection schemes for network coding in network-on-chips," *NORCHIP*, vol. 2012, pp. 1–5, Article ID 6403130, 2012.

[33] R. Ahlswede, N. Ning Cai, S.-Y. R. Li, and R. W. Yeung, "Network information flow," *IEEE Transactions on Information Theory*, vol. 46, no. 4, pp. 1204–1216, 2000.

[34] C. Fragouli, J. Widmer, and J. L. Boudec, "A network coding approach to energy efficient broadcasting: from theory to practice," in *Proceedings of the IEEE Infocom*, pp. 1–11, Barcelona, Spain, April 2006.

[35] C. Gkantsidis and P. R. Rodriguez, "Network coding for large scale content distribution," in *Proceedings of the INFOCOM 2005. 24th Annual Joint Conference of the IEEE Computer and Communications Societies*, pp. 2235–2245, Miami, FL, USA, March 2005.

[36] T. Ho, R. Koetter, M. Medard, D. R. Karger, and M. Effros, "The benefits of coding over routing in a randomized setting," in *Proceedings of the IEEE International Symposium on Information Theory*, Yokohama, Japan, June 2003.

[37] S. Katti, H. Rahul, W. Hu, D. Katabi, M. Médard, and J. Crowcroft, "XORs in the air," *ACM SIGCOMM - Computer Communication Review*, vol. 36, no. 4, pp. 243–254, 2006.

[38] Z. Li and B. Li, *Network Coding in Undirected Networks*, CiteSeer, Princeton, NJ, USA, 2004.

[39] T. Matsuda, T. Noguchi, and T. Takine, "Survey of network coding and its applications," *IEICE Transactions on Communications*, vol. E94-B, no. 3, pp. 698–717, 2011.

[40] S. Katti, H. Rahul, W. Wenjun Hu, D. Katabi, M. Medard, and J. Crowcroft, "XORs in the air: practical wireless network coding," *IEEE/ACM Transactions on Networking*, vol. 16, no. 3, pp. 497–510, 2008.

[41] T. Duong-Ba, T. Nguyen, and P. Chiang, "Network coding in multicore processors," in *Proceedings of the 2011 IEEE 30th International Performance Computing and Communications Conference (IPCCC)*, pp. 1–7, Orlando, Florida, USA, November 2011.

[42] C. Tata and M. Kadoch, "Multipath routing algorithm for device-to-device communications for public safety over LTE heterogeneous networks," in *Proceedings of the 1st International Conference on Information and Communication Technologies for Disaster Management ICT-DM'2014*, Algiers, Algeria, 2014.

[43] C. Tata and M. Kadoch, "RBC: reliable butterfly network construction algorithm for network coding in wireless mesh network," in *Proceedings of the 13th WSEAS International Conference on Applied Informatics and Communications (AIC'13)*, Valencia, Spain, 2013.

[44] P. Ganesan, R. Venugopalan, P. Peddabachagari, A. Dean, F. Mueller, and M. Sichitiu, "Analyzing and modeling encryption overhead for sensor network nodes," in *Proceedings of the 2nd ACM international conference on Wireless sensor networks and applications*, pp. 151–159, San Diego CA USA, September 2003.

[45] A. Hossain, B. Hossain, S. Uddin, and S. Imtiaz, "Performance analysis of different cryptography algorithms," *International Journal of Advanced Research in Computer Science and Software Engineering*, vol. 6, no. 3, pp. 659–665, 2016.

[46] C. Tata and M. Kadoch, "Efficient Priority Access to the shared commercial radio with offloading for public safety in LTE heterogeneous networks," *Journal of Computer Networks and Communications*, vol. 2014, Article ID 597425, 2014.

[47] C. Tata and M. Kadoch, "Courteous priority access to the shared commercial radio for public safety in LTE heterogeneous networks," in *Proceedings of the 2014 International Conference on Future Internet of Things and Cloud*, pp. 246–252, Barcelona, Spain, August 2014.