Secure Network Coding based Data Splitting for Public Safety D2D communications over LTE Heterogeneous Networks

CHAFIKA TATA, MICHEL KADOCH
Department of electrical engineering
École de Technologie Supérieure
1100, rue Notre-Dame Ouest, Montréal (Québec) H3C 1K3
CANADA
chafika.tata.1@ens.etsmtl.ca, michel.kadoch@etsmtl.ca, www.etsmtl.ca

Abstract: - This paper investigates the issue of secure Network Coding (NC) routing for Public Safety (PS) Device to Device (D2D) communications over LTE Heterogeneous Networks (HetNets). A new approach, named Secure Network Coding based Data splitting algorithm (SNCDS), is presented to construct secure network coded symbols by using Data Splitting (DS) mechanism when transmitting NC symbols. The objective of this solution is to assure the confidentiality in the network, by avoiding eavesdroppers to get any meaningful information about the source node. Our work concerns both of internal and external attacks. DS mechanism avoids Hackers to get the whole symbol sent by the source. Furthermore, when the eavesdropper gets information, he ignores that it is only part of the sent symbol, and also that the data is transmitted in random order. Only the source and the destination know the sequence order of the sent packets. The simulation results show that our approach assure a secure D2D communication without increasing the overhead in the network.

Key-Words: - Macro cells, Small cells, HetNets, Public safety, D2D, Security, Splitting Data.

1 Introduction

HetNets networks [1] have become an interesting solution for improvement of network resources management for the Public Safety (PS) D2D communications [2, 3]. This kind of network combines a macro cells, small cells and unlicensed networks as Wi-Fi, WMN and Ad hoc networks, which allows increasing throughput and decreasing delays and packet loss. Small cells and unlicensed networks are used to offload the macro cell, so reducing pre-emption of active bearers and decreasing the number of blocking incoming bearers to the Macro cell [4]. On the other hand, the network resources have to be well managed and shared between the offloaded bearers in order to assure a good Quality of Service (QoS) for the different offloaded traffics. The application of the Network Coding (NC) [5] is one relevant solution for improving the QoS for the wireless D2D communication for the data routing. It allows simultaneous transmission of multiple data streams arriving from one or more sources to one or more destinations. Therefore, number of timeslots needed to transmit information decreases and so the delays decreases too. Moreover, the throughput rises. However, the nature of forwarding data in the multi-hops wireless networks is characterised by a broadcasting transmission. This steps up the vulnerability of the network to the attacks and weakens its security level. Certainly, the coding mechanism reduces the threat risks by mixing symbols, but some other packets can reach the destination without being encoded. Figure 1 illustrates the case of a network coded data transmission with the presence of an eavesdropper. In such case, the hacker is able to intercept the native packet B, and all packets transmitted through the same path used for sending the packet B.

To address this issue and to increase the security level in the network, encryption may be shown as a relevant solution [6-8]. Therefore, this approach is susceptible to rise the overhead in the network, which may deteriorate the QoS in the network because of the consumption of the radio and bandwidth resources. Especially, WMN networks are known for using redundancy transmissions. In fact, the network resources become limited.

This paper investigates the issue of secure Network Coding (NC) routing for Public Safety (PS) Device to Device (D2D) communications

ISBN: 978-960-474-361-2

over LTE Heterogeneous Networks (HetNets). A new approach, named Secure Network Coding based Data splitting algorithm (SNCDS), is presented to construct secure network coded symbols by using Data Splitting (DS) mechanism when transmitting NC symbols. The objective of this solution is to assure the confidentiality in the network, by avoiding eavesdroppers to get any meaningful information about the source node, without increasing the overhead in the wireless network. Our work concerns both of internal and external attacks. DS mechanism avoids Hackers to get the whole symbol sent by the source. Furthermore, when the eavesdropper gets information, he does not know that it is only part of the sent symbol, and also that the data is transmitted in a random order. Only the source and the destination know the sequence order of the sent packets. The simulation results show that our approach assure a secure D2D communication without increasing the overhead in the network

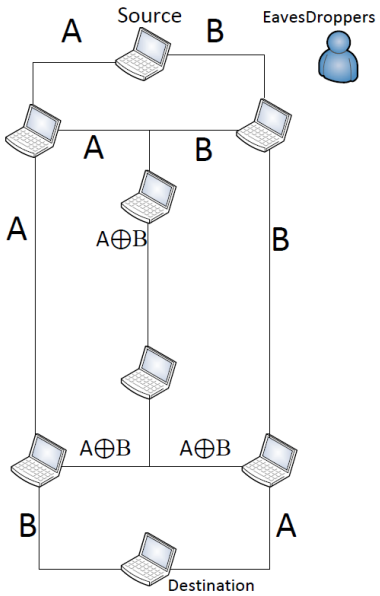

Fig.1 Network Coding data packets forwarding with the presence of an eavesdropper

This paper is organized as follows. Section II presents the SNCDS algorithm. Section III summarizes the most important simulation results and their interpretation. Section IV concludes this article.

2 Secure Network Coding Base Data splitting Algorithm

In this work, a new approach is developed for secure network coded data transmission for PS D2D communication over LTE HetNets networks. The objective of this approach is to keep the confidentiality of the transmitted data over the network, only the source and the destination can get the meaning of the transmitted information. Our solution consists of applying the Data Splitting mechanism for forwarding symbols from the source to the destination over a butterfly network. In other words, instead of sending whole packets through a network coding path, each packet will be divided by the source into segments of six bits. Thereafter, each fragment will be reordered according to sequence selected by the source. Finally, the different bits of the same fragment will be transmitted to the destination via two distinct paths from the source. The source transmits the first bit of the disordered sequence via the first path, the second bit via the other one and so on. The operation is initialized with the next segment up sending all packets. We assume that the random sequence position is encrypted by the source and sent to the destination at the beginning of the transmission. Otherwise, we suppose that the coded matrix format is known by the destination, but not the matrix codes values. The destination node uses the random sequence position to construct the coded matrix.
Let C be the coded matrix used for coding and decoding data by the network coding scheme.

$$C = \begin{pmatrix} c1 & c2 \\ c3 + c4c1 & c4c2 \\ c5c1 & c5c2 + c6 \end{pmatrix} \quad (3)$$

Let $P = (P_1P_2P_3P_4P_5P_6)$ the random sequence position generated by the source. The destination gets the matrix C by substituting each code $C_i$by the position numbers P_i

This approach avoids the eavesdropper to get meaningful information by intercepting data. The attacker cannot get the whole bits of the packet sent, because some bits take another path

out of his coverage. Furthermore, the hacker does not know that sent data is shuffled by the source. Then, this will complicate for him the reconstruction of the native packet. In the following, the splitting data mechanism and decoding packets, adopted in this study will be detailed.

2.1 Data Splitting and Coding operation

The figure 2 presents the packet dividing into six bits segments adopted for the SNCDS algorithm. The packet to send is dividing into segment of 6 bits each (figure 2.a). After that the source shuffles each fragment with respect random sequence position of the bit in the fragment (figure 2.b).

Packet A

a1	a2	a3	a4	a5	a6
a1	a2	a3	a4	a5	a6
.					
.					
a1	a2	a3	a4	a5	a6

a). Step1: packet fragmentation

Packet A

a4	a2	a5	a6	a1	a3
a4	a2	a5	a6	a1	a3
.					
.					
a4	a2	a5	a6	a1	a3

b). Step2: Sequence reorder

Fig.2 Packet dividing into six bits segments

For example, in the case illustrated in the figure 2, the random sequence adopted for the shuffling bits position is:
(p1,p2,p3,p4,p5,p6) = (4,2,5,6,1,3) (1)

Where pi are the bits positions, and i= 1 to 6.

And
b1 = a4, b2 =a2, b3 = a5, b4= a6, b5 = a1, b6 =a3. (2)

Where bi are the sent bits by the sources with respect of bits the sequence order.

The source sends bits to each of the two paths alternatively. So that, the source sends a1, a3 and a5 through the first path, and a2, a4 and a6 through the second one.

Figure 3 illustrates the network coding and the transmission of the bits of a segment of the packet A with the presence of an eavesdropper

Let $a_{i,}a_j$, $iand\ j \in [1,6]$ be the send bits from the source to the destination over the butterfly network, and C the coded matrix used to coding and decoding transmitted bits given by the formula (3).

Finally, let y_i be the coded symbols

.

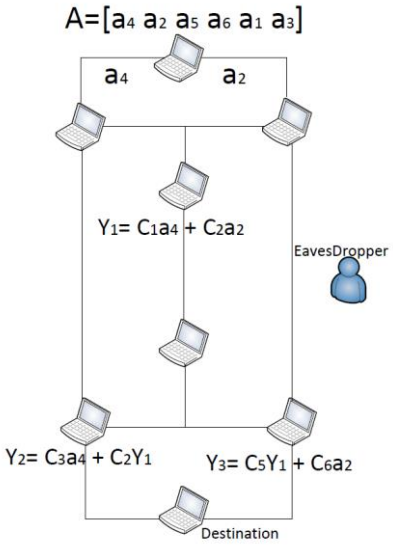

Fig.3 Network Coding transmission with Splitting Data mechanism

The mathematical formulation of this network coded transmission is given as follows

$$y1 = c1*ai + c2*aj$$
$$y2 = c3*ai + c4*Y1 = (c3 + c4c1)ai + c4c2\ aj \quad (4)$$
$$y3 = c5*Y1 + c6*aj = c5c1\ ai + (c5c2 + c6)\ aj$$

So, the coding scheme will be represented as follows

$$\begin{pmatrix} y1 \\ y2 \\ y3 \end{pmatrix} = \begin{pmatrix} c1 & c2 \\ c3 + c4c1 & c4c2 \\ c5c1 & c5c2 + c6 \end{pmatrix} * \begin{pmatrix} ai \\ aj \end{pmatrix} \quad (5)$$

2.2 Decoding operation

The decoding mechanism is performed by the destination. This assures that only the source and the destination may get the meaningful data transmitted. For decoding data, the destination resolves the formula (6)

$$\begin{pmatrix} ai \\ aj \end{pmatrix} = \begin{pmatrix} c1 & c2 \\ c3 + c4c1 & c4c2 \\ c5c1 & c5c2 + c6 \end{pmatrix} * \begin{pmatrix} y1 \\ y2 \\ y3 \end{pmatrix}^{-1} \quad (6)$$

Then, the decoding scheme relative of the example shown in the figure 3 is given by resolving the system of the formula (7).

$$\begin{pmatrix} a_4 \\ a_2 \end{pmatrix} = \begin{pmatrix} c1 & c2 \\ c3 + c4 * c1 & c4 * c2 \\ c5 * c1 & c5 * c2 + c6 \end{pmatrix} * \begin{pmatrix} y1 \\ y2 \\ y3 \end{pmatrix}^{-1} \quad (7)$$

When the destination gets the sequence of six bits, it will put the sequence in the initial order. For this aim, it uses encrypted bits sent sequence given by the source.

2.3 Simulation of eavesdropping attacks

We assume the attacks illustrated in the figure 4. This figure represents two kinds of attacks in a butterfly network. An internal attack performed by the eavesdropper 1 and an external attack done by the eavesdropper 2. In the both situation eavesdroppers cannot get the whole information sent by the source to the destination. The eavesdropper1 may intercept the coded symbol Y1. Certainly, he cannot resolve this symbol since he has not 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. On the other hand, eavesdropper 2 may only get the send bits relevant to odd positions. In addition, the order of bits got is not the same for the order of bits in the native packet, so that, it will be complicate for him to reconstruct the native packet.

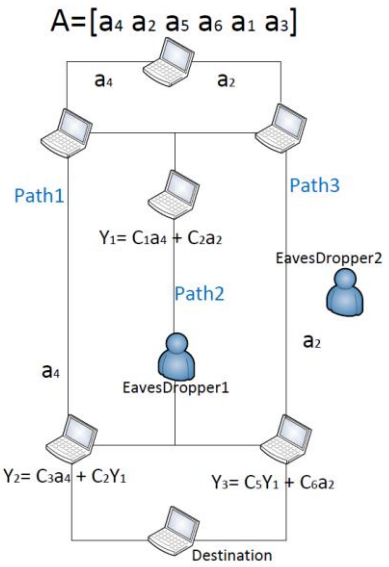

Fig.4 Internal and external attack in the butterfly network

3 Simulation And Results

In this section we show the results of the implementation of SNCDS algorithm. The aim of our simulation, carried out in Matlab, is to illustrate that splitting data mechanism, used by SNCDS, provides secure transmission in Network Coding networks for the PS D2D transmission over LTE HetNets networks. SNCDS algorithm is designed for preserving data from being obtained by any eavesdropper node. Our solution considers both internal and external eavesdropping attacks. The contribution of our work is to avoid eavesdroppers to get meaningful information sent from the source to the destination without adding any additional overhead than the one added by the coding operation.

For each experiment, the source, the destination and the eavesdropper nodes are chosen at random among all forwarding nodes in the WMN network. The RBC algorithm [9] is applied to construct the butterfly network between the source and the destination nodes (figure 5 and figure 7). Two scenarios are simulated, the internal attack scenario and the external attack one. In both cases the eavesdropping attack is experimented by transmitting 40 packets with size of 512 Bytes.

ISBN: 978-960-474-361-2

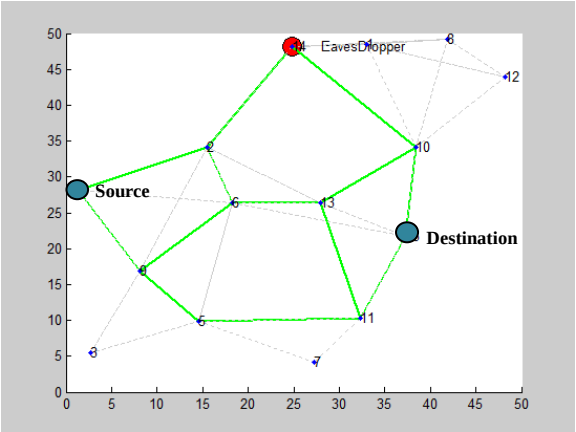

Fig.5 Internal Eavesdropping Attack

The figure 5 illustrates the butterfly network constructed by the RBC algorithm. This scenario is performed to examine the internal attack. The eavesdropper node is a member of the butterfly network. In such case, the hacker may have a part of transmitted data from its neighbours. The captured information may be sent to it or intercepted among the data sent to its neighbours, which are in its transmission coverage.

Therefore, the application of the SNCDS decreases the number of the intercepted data by the eavesdropper node in both internal and external attacks (figures 6 and 8). This is made possible thanks of the application of the splitting mechanism. The splitting scheme consists of dividing each sent packet into two parts; one part is transmitted through one path of the butterfly network and the second part through the other path. This approach decreases the number of bits obtained by any nodes comparing to number of bits captured when the scheme of sending the whole packets through the two lateral paths of the butterfly network is applied.

Note that the number of intercepted data is higher in the case of the internal attack (figure 6) than in the case of external data (figure 8). This is because of the location of the hacker in the network. Figure 6 shows that the eavesdropper may get the information sent to it from the node 2 and also intercepts the information sent to the node 10, which is a coded symbol. This may increase the bits quantity of the obtained information comparing to the other scenario (figure 8).

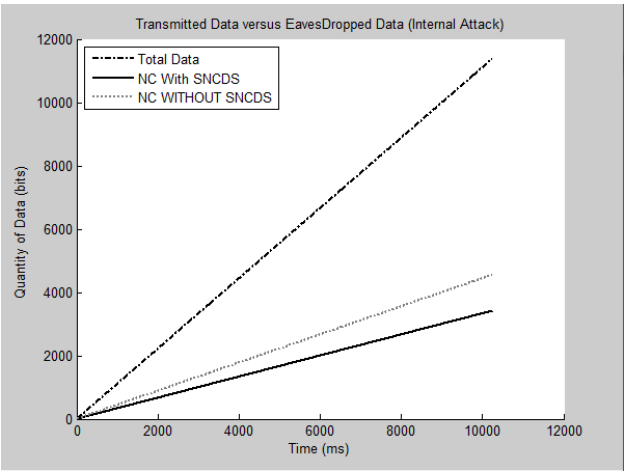

Fig.6 Transmitted Data vs. Eavesdropped Data (internal Attack)

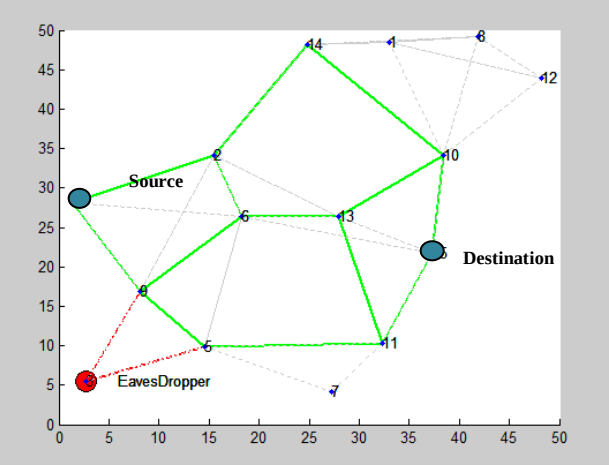

Fig.7 External Eavesdropping Attack

Also, it is evident that our solution avoids the eavesdropped node to get any meaningful information thanks of the splitting operation on one hand, which makes unattainable for him a part of the packet by applying the splitting scheme, and, on the other hand, complicate the bits gathering process since he don't know about the data shuffling mechanism adapted by the sources node to transmit the PS network coded D2D information through the butterfly network. This advantage is not given by the classical NC transmission, where the source forwards the whole packet bits using the same path. Data eavesdropping becomes easy for the hacker, since the information is not encrypted.

ISBN: 978-960-474-361-2

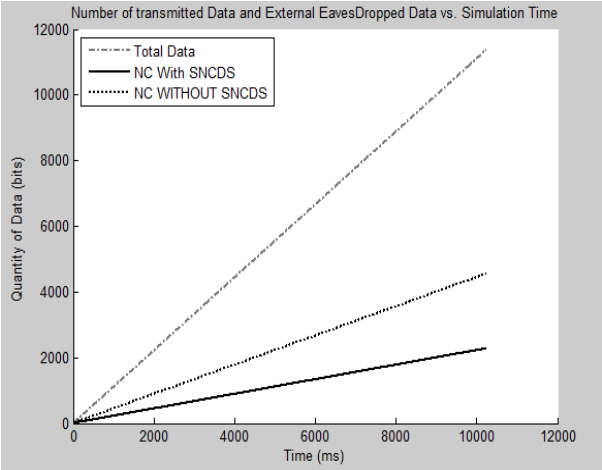

Fig.8 Transmitted Data vs. Eavesdropped Data (External Attack)

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 in order to encrypt it. Authors in [10] evaluate the encryption overhead for many encryption algorithms. In fact, the combined added bits serving to 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 SNCDS is that it assures a secure data routing for the PS D2D transmission without adding any overhead traffic other than the one used by the Network Coding scheme.

4 Conclusion

The application of the network coding scheme for Public Safety D2D communications over LTE HetNets networks is a pertinent solution to enhance the data routing scheme, since it improves the performance of the whole network by increasing the throughput and decreasing the end to end delay and the packet lost rate. Therefore, the nature of the PS communications requires a high level of security routing, mainly in term of confidentiality. This paper defined a new model for security routing in the butterfly network applied to PS D2D communication over LTE HetNets networks. The simulation results showed that the information intercepted by the eavesdroppers is less important than the one obtained by them in case of a classical network coding data transmission. Furthermore, no meaningful data has been obtained by the attackers. Besides that, the increases in the routing security level doesn't arise the overhead already existing in the network and caused by network coding process.

References:

[1] O. Stanze and A. Weber, "Heterogeneous Networks With LTE-Advanced Technologies," *Bell Labs Technical Journal*, vol. 18, pp. 41-58, 2013.

[2] X. Lin, J. G. Andrews, A. Ghosh, and R. Ratasuk, "An Overview on 3GPP Device-to-Device Proximity Services," *arXiv preprint arXiv:1310.0116*, 2013.

[3] B. Raghothaman, E. Deng, R. Pragada, G. Sternberg, T. Deng, and K. Vanganuru, "Architecture and protocols for LTE-based device to device communication," in *Computing, Networking and Communications (ICNC), 2013 International Conference on*, 2013, pp. 895-899.

[4] V. Nagpal, S. Choudhury, and K. Doppler, "OFFLOADING TRAFFIC TO DEVICE-TO-DEVICE COMMUNICATIONS," ed: US Patent 20,130,073,671, 2013.

[5] T. Ho, R. Koetter, M. Medard, D. R. Karger, and M. Effros, "The benefits of coding over routing in a randomized setting," 2003.

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

[7] 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, pp. 1046-1061, 2013.

[8] Z. Tang, "On link encryption against wiretapping attack in network coding," *Networking Science*, pp. 1-10, 2013.

[9] C. Tata and M. Kadoch, "RBC: Reliable Butterfly Network Construction Algorithm for Network Coding in Wireless Mesh Network," 2013.

[10] 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*, 2003, pp. 151-159.