Esfahani *et al. EURASIP Journal on Wireless Communications and Networking* (2016) 2016:113
DOI 10.1186/s13638-016-0601-9

EURASIP Journal on Wireless Communications and Networking

RESEARCH Open Access

# An efficient MAC-based scheme against pollution attacks in XOR network coding-enabled WBANs for remote patient monitoring systems

Alireza Esfahani*, Georgios Mantas, Hélio Silva, Jonathan Rodriguez and Jose Carlos Neves

**Abstract**

Wireless Body Area Networks (WBANs) play a pivotal role to remote patient monitoring which is one of the main applications of m-Health. However, WBANs comprise a subset of wireless sensor networks (WSNs), and thus, they inherit the limitations of WSNs in terms of communication bandwidth, reliability, and power consumption that should be addressed so that WBANs can reach their full potential. Towards this direction, XOR network coding (NC) is a promising solution for WBANs. Nevertheless, XOR NC is vulnerable to pollution attacks, where adversaries (i.e., compromised intermediate nodes) inject into the network corrupted packets that prevent the destination nodes from decoding correctly. This has as a result not only network resource waste but also energy waste at the intermediate nodes. In this sense, pollution attacks comprise a serious threat against WBANs (i.e., resource-constrained wireless networks) that should be addressed so that WBANs can reap the benefits of XOR NC.

Therefore, in this paper, we propose an efficient message authentication code (MAC)-based scheme that provides resistance against pollution attacks in XOR NC-enabled WBANs for remote patient monitoring systems. Our proposed scheme makes use of a number of MACs which are appended to the end of each native packet. Our results show that the proposed MAC-based scheme is more efficient compared to other competitive schemes for securing XOR NC against pollution attacks in resource-constrained wireless networks, in terms of communication bandwidth and computational complexity.

**Keywords:** Secure XOR network coding, Pollution attacks, MAC-based scheme, Key management, m-Health, WBANs, Remote patient monitoring

## 1 Introduction

Over the past decade, advances in Wireless Body Area Networks (WBANs) have contributed significantly to the evolution of remote patient monitoring, which is one of the main applications of m-Health. It is an m-Health application that could enhance the quality of people's life and also reduce the costs of national healthcare systems [1–3]. For instance, remote patient monitoring could improve the quality of life of individuals with special needs, such as people with chronicle diseases, who wish to lead an independent way of life staying at their own home with minimum intervention from healthcare professionals. Particularly, remote patient monitoring could play a pivotal role towards individual's treatment, proactive actions, and provision of emergency assistance [4–6]. In this context, WBANs are a key component to remote patient monitoring systems, since they enable continuous monitoring of patient's physiological parameters and real-time feedback to the patient and the healthcare professional (e.g., doctors) that allow greater mobility and flexibility to the patient. In addition, healthcare professionals can have a clearer view of the patient's status, thanks to WBANs which are able to obtain data from the patient's natural environment during a large time interval [3, 7].

*Correspondence: alireza@av.it.pt
Instituto de Telecomunicações - Pólo de Aveiro, Aveiro 3810-193, Portugal

WBANs consist of multiple small low-power wireless devices attached on clothing or on the human body or even implanted in the human body. These devices, which are the nodes of a WBAN, are categorized into two types: sensors and actuators. The sensors measure various vital signs (e.g., blood pressure, heart rate) or external parameters (e.g., motion patterns) and process their readings, if necessary. Then, they transmit this information to a central device, playing the role of the coordinator, directly or through other nodes (i.e., sensors or actuators) that act as relays [7–9]. This device, which is more powerful than a sensor or actuator, is located on or near the patient and is responsible to collect all the information acquired by the sensors or actuators and passes it to another network (e.g., WLAN, 3G/4G), so that the information will reach the remote healthcare professional's side (e.g., medical server). Furthermore, the central device can provide information to the patient or the healthcare professionals (e.g., nurse, doctor), located close to the patient, via a display/LEDS on it. Moreover, it is worthwhile to mention that the central device, which is also called as body gateway (BG), body control unit (BCU), hub or a sink, in some implementations can be a smartphone or a personal digital assistant (PDA). On the other hand, the actuators take actions according to the information received from the sensors or through interaction with the patient or the healthcare professionals, which is usually handled by the central device as well [7, 8, 10].

However, WBANs comprise a subset of wireless sensor networks (WSNs), and thus, they inherit the limitations of WSNs in terms of communication bandwidth, reliability, and power consumption that should be addressed so that WBANs can reach their full potential [3, 11–14]. In this sense, the application of network coding (NC) technology in WBANs has emerged as a promising solution to address these limitations, since it provides significant benefits including network capacity improvement, robustness to packet losses, and lower energy consumption [15–18]. NC was presented for the first time by Ahlswede et al. in [19] in 2000 and, in contrast to traditional store-and-forward networks, its core principle is to allow the incoming packets at the intermediate nodes, in NC-enabled networks, not only to be routed or replicated but also recoded. Within the few years after 2000, different approaches of linear NC appeared for wired networks [20, 21]. For instance, the approach of random linear network coding (RLNC) was proposed by Ho et al. in [22] as a fully distributed approach for performing NC. According to RLNC, each node selects randomly a set of coefficients and uses them to make linear combinations of the incoming packets. In these approaches, NC is operated over large finite fields, and thus, they are not efficient for wireless networks. However, a more efficient type of NC, based only on XOR operations, was introduced in [23] and targets applications in wireless networks [24].

Nevertheless, similar to linear NC-enabled networks, XOR NC-enabled networks are vulnerable to pollution attacks, where adversaries (i.e., compromised intermediate nodes) inject into the network corrupted packets that prevent the destination nodes from decoding correctly. Even a small proportion of corrupted packets can quickly propagate into other packets via re-recoding, occurred at the intermediate nodes, and lead to infection of a larger number of packets. This has as a result not only network resource waste but also energy waste at the nodes. In this sense, pollution attacks comprise a serious threat against WBANs (i.e., resource-constrained wireless networks) that should be addressed so that WBANs can reap the benefits of XOR NC [24]. Therefore, in this paper, we propose an efficient message authentication code (MAC)-based scheme providing resistance against pollution attacks in XOR NC-enabled WBANs for remote patient monitoring systems. Our proposed scheme makes use of a number of MACs which are appended to the end of each native packet. Our results show that the proposed MAC-based scheme is more efficient compared to the scheme proposed in [24], in terms of communication bandwidth and computational complexity. To the best of our knowledge, the proposed scheme in [24] is the most competitive scheme in the literature for securing XOR NC against pollution attacks in resource-constrained wireless networks.

The remainder of this paper is organized as follows. In Section 2, we give an overview of the background and related work on XOR NC and secure XOR NC in wireless networks. A WBAN scenario in a remote patient monitoring system is described in Section 3. Section 4 provides the network model of the WBAN scenario, where XOR NC is applied. In addition, in this section, we present the adversary model of this XOR NC-enabled WBAN, as well as the key distribution model which is adopted by our proposed scheme. In Section 5, our proposed scheme is provided. Subsequently, the security analysis of our proposed scheme is given in Section 6. In Section 7, the performance evaluation of the proposed scheme is analyzed. Finally, Section 8 concludes the paper.

## 2 Background and related work

### 2.1 XOR network coding in wireless networks

A practical XOR NC scheme which can be applied on wireless networks was presented for the first time by Katti et al. in [23]. The proposed scheme, called COPE, can improve wireless throughput, including more accurate congestion control, better routing, and efficient MAC protocols. However, COPE takes into consideration only

wireless networks with resource-unconstrained nodes. Mostly, COPE is considered as the base of XOR NC schemes. The idea underlying XOR NC schemes is usually illustrated using the famous butterfly example [19, 23]. According to the butterfly topology, we consider the network in Fig. 1 including one source node (i.e., node 1), a few intermediate nodes (i.e., nodes 2, 3, 4, and 5), and two sink nodes (i.e., nodes 6 and 7). The source node wants to deliver the native packets $x_1$ and $x_2$ to both sink nodes (i.e., nodes 6 and 7) through the intermediate nodes (i.e., nodes 2, 3, 4, and 5). In this regard, node 4 XORing the two received packets ($x_1$ and $x_2$) from the two incoming nodes (i.e., nodes 2 and 3) sends the result of $x_1 \oplus x_2$ to node 5. Then, node 5 retransmits result of $x_1 \oplus x_2$ to the sink nodes (i.e., nodes 6 and 7). Finally, the two sink nodes decode the received result of $x_1 \oplus x_2$ and obtain $x_1$ and $x_2$, as it is depicted in Fig. 1.

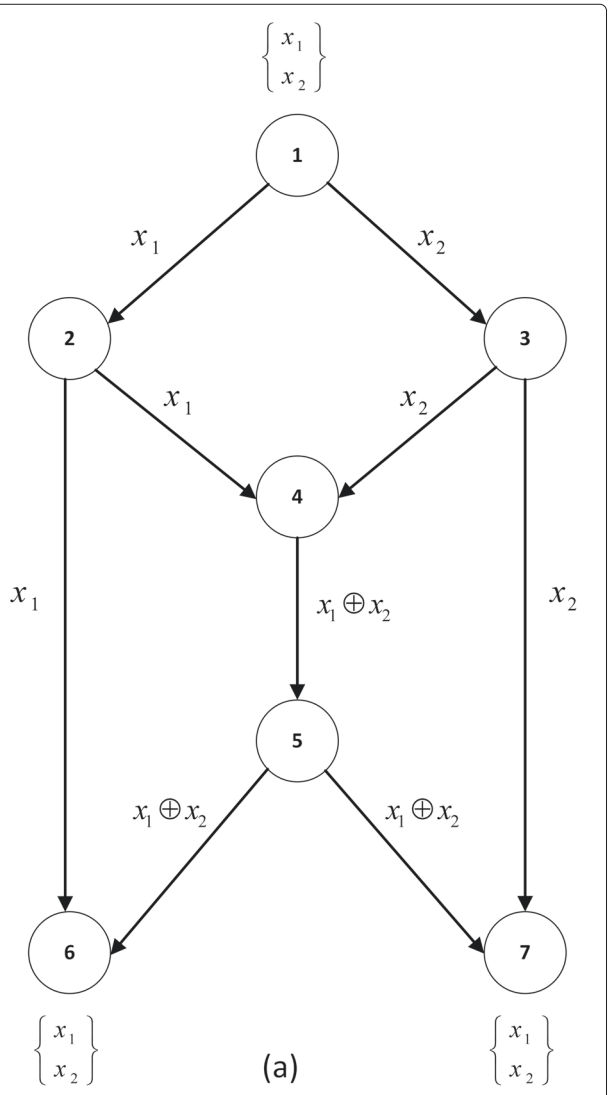


**Fig. 1** XOR network coding based on the butterfly topology

### 2.2 Secure XOR network coding in wireless networks

The first scheme securing XOR NC against pollution attacks was presented in [24]. In this scheme, a source node calculates and appends a number of MACs to the end of each native packet. Each MAC is the output of a hash function taking as inputs a random number of codewords of the native packet. According to the proposed scheme, the probability of the corrupted packets to travel many hops is reduced. In the best case, a corrupted packet can be detected after traveling around 3 hops, and in the worst-case, it can be detected after traveling around 11 hops. Moreover, the authors in [25] propose a trusted NC scheme, based on COPE, for wireless ad hoc networks. This scheme allows an intermediate node to judge whether other nodes are reliable according to its previous observations. However, their performance analysis showed that the proposed scheme significantly outperforms in terms of network throughput. In addition, the proposed scheme cannot detect a pollution attack where an adversary has corrupted a packet. In 2012, the authors in [26] proposed a scheme called CodeGuard. The CodeGuard is a wireless interflow defense pollution scheme which uses node attestation to detect adversary nodes. Finally, the authors in [27] proposed an efficient MAC-signature scheme for securing XOR NC against pollution attacks. According to their scheme, the source node generates a number of MACs and a signature, which are appended to the end of each native packet and allow the detection of a corrupted packet in the next hop.

## 3 WBAN scenario in remote patient monitoring

We consider a WBAN scenario in a remote patient monitoring system as it is shown in Fig. 2, where sensors are attached on the patient's clothing or placed on the patient's body and measure various vital signs (e.g., blood pressure, heart rate, respiration rate, cholesterol level) or external parameters (e.g., patient's location, motion patters). In addition, the sensors process their readings, if necessary, and transmit this information to the BG, implemented on the patient's smartphone, through other relay nodes (i.e., sensors or actuators). The nodes are interconnected to each other and to the BG through a short-range wireless technology (e.g., IEEE 802.15.6, ZigBee) [7–9]. The BG then forwards the received data to a cellular base station (e.g., 4G), through a long-range wireless technology (e.g., LTE), so that the data will reach the medical server at the healthcare professional's side. Finally, the actuators of the WBAN play the role of drug delivery systems. Hence, they inject the medicine when it is triggered by the healthcare professional through the

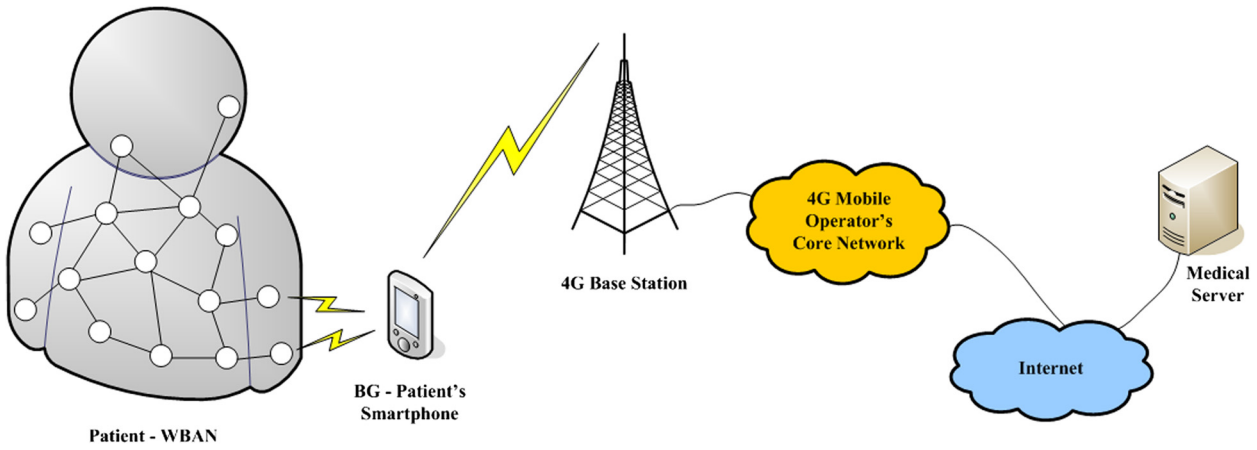


**Fig. 2** WBAN scenario in remote patient monitoring

central device or immediately when a sensor detects a problem [7, 10].

## 4 Models and assumptions

In this section, we provide the network model of the above WBAN scenario (Section 3), where XOR NC is applied. Moreover, we provide the adversary model of this XOR NC-enabled WBAN, as well as the key distribution model which is adopted by our proposed scheme.

### 4.1 Network model

Our XOR NC-enabled WBAN can be modeled as a directed multigraph $(S, I, e)$ which consists of the following components, as it is also shown in Fig. 3:

- **Source node *S***: We have a source $S$ (i.e., a sensor node) which wants to multicast its messages. To achieve that each message is divided into a sequence of packets and these packets are multicasted. Each packet consists of a number of codewords.
- **Non-source node set *I***: This set includes the intermediate nodes (i.e., relay nodes) and the destination node (i.e., smartphone) which recode and decode packets. In Fig. 3, the set of non-source nodes is represented as: $I = \{I_1, \ldots, I_j, D\}$.
- **Link set *e***: This set consists of all the links in the network. As a link is defined the connection between each pair of two nodes. In Fig. 3, the set of links is represented as: $e = \{e_1, \ldots, e_w\}$.

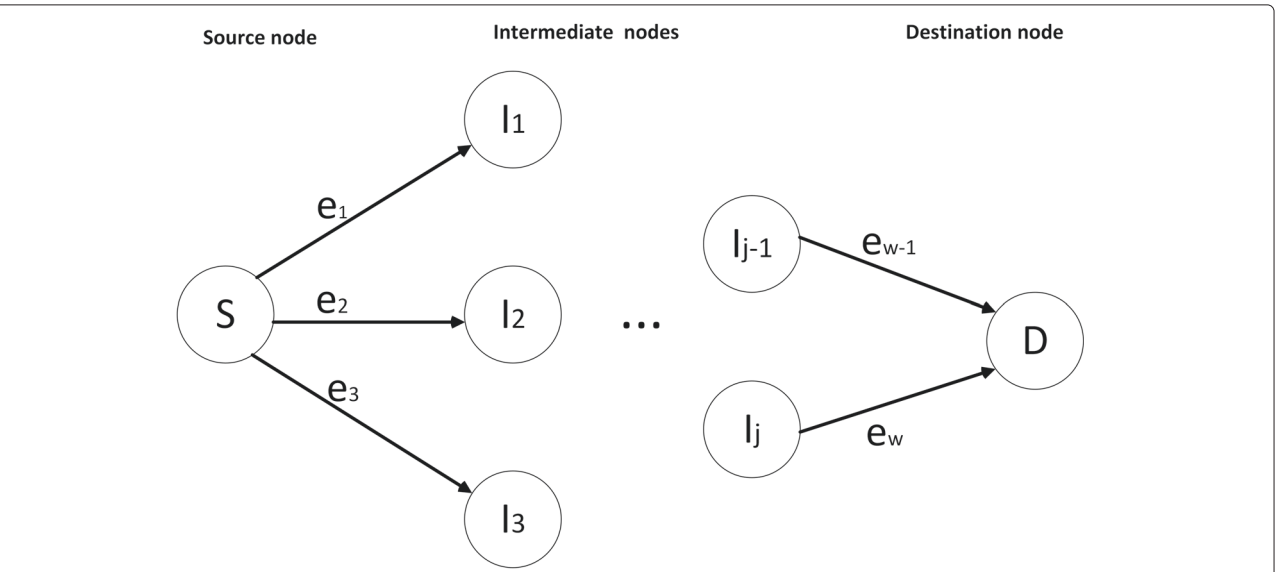


**Fig. 3** The network model of our XOR NC-enabled WBAN

We consider two types of packets: native packets and coded packets. Native packets are packets generated at the source node. On the other hand, coded packets are packets which are encoded and recoded at the source and intermediate nodes. However, for simplicity, we call them as packets when it is not required to distinguish them to native and coded packets. At the setup phase and according to the assumption made by the most existing schemes [28, 29], the source divides each message into a sequence of native packets and partitions them into generations.

In our model, the source $\mathcal{S}$ wants to send a number of native packets (i.e., $M_1, M_2, \cdots, M_n$) to the destination $D$. Each native packet $M_i$, which is divided into $m$ codewords, can be represented as a row vector as follows:

$$M_i = \left(m_{i,1}, m_{i,2}, \cdots, m_{i,m}\right), \tag{1}$$

where $i = 1, \cdots, n$.

Each codeword stands in a finite field $\mathbb{F}_p$, where $p$ is a power of prime number. Our model encodes the codewords over the field of size 2. Typically, each codeword is 256-bit long ($\lfloor \log_2 p \rfloor$).

Additionally, we denote the coded packet as $E$, which can be represented as the following

$$E = \alpha_1 M_1 \oplus \alpha_2 M_2 \oplus \cdots \oplus \alpha_n M_n, \tag{2}$$

where $\alpha_i \in \{0, 1\}$ for $i = 1, \cdots, n$. The intermediate and destination nodes use the received coded packets $E$ to verify the native packets.

### 4.2 Adversary model

In this paper, we assume that the source node and the destination node are always trusted and there is not any possibility to be forged. However, the intermediate nodes can be compromised. A compromised node can play the role of an adversary that is able to wiretap all the data packets that are transmitted over the network. The adversary's goal is to achieve pollution attack. Moreover, it is considered that the adversaries have limitations in computation power, and thus, they can only perform in polynomial time.

### 4.3 Key distribution model

We assume that a set of keys are distributed to all participant nodes in a secure and authenticated manner by a key distribution center (KDC) according to our key distribution model. In this section, we provide a brief description of our key distribution model that we have adopted for our proposed MAC-based scheme against pollution attacks in XOR NC-enabled WBANs. This key distribution model has been presented in detail in our previous work [30].

According to our key distribution model, if the keys are distributed properly, then no coalition of $c$ compromised nodes can deceive another node. It is shown in [31] that in order to resist against $c$ compromised nodes, the number of the keys at the source must be $c + 1$ times larger than the number of the shared keys at the relay/destination nodes. This model allows each verifier to obtain a number of shared keys in order to verify the coded packets. In our proposed scheme, this key distribution model assigns only one key to the intermediate and destination nodes so that they verify the received coded packet. Only one key is assigned to each intermediate and destination node, since in case that more than one key is assigned, then there is the possibility to verify the coded packet more than once. However, this possibility needs more computational complexity.

## 5 Proposed MAC-based scheme

In this section, we present the proposed MAC-based scheme against pollution attacks in XOR NC-enabled WBANs. Our scheme is defined as a triple of probabilistic polynomial time (PPT) algorithms (*Setup*, *MAC*, *Verify*):

- Setup: The KDC distributes the required keys to all nodes, and the source node sets the security parameters and uses the assigned keys to generate the corresponding MACs.
- MAC: The source node calculates and appends a number of MACs to the end of each native packet.
- Verify: Verification is based on the coded packets, the appended MACs, and the shared keys. If verification succeeds, the received packets will be accepted and used for further recoding or decoding. Otherwise, the received packets are discarded.

The summary of notations is presented in Table 1.

### 5.1 The construction of the MAC-based scheme

The construction of the proposed MAC-based scheme consists of the following:

**Table 1** Summary of notations

| Parameter | Meaning |
|---|---|
| $n$ | The number of native packets per generation |
| $m$ | The number of codewords of each native packet |
| $l$ | The number of MACs |
| $p$ | The size of finite field and each codeword |
| $M_i$ | Each native packet |
| $m_j$ | Each coded packet |
| $h$ | The hash function |
| $K_{i,j}$ | The key |
| $id_{i,j}$ | The index of the key |
| $r_j$ | The index of $u$ codewords |
| $u$ | The number of codewords used for each MAC |
| $c$ | The number of compromised nodes |

- Setup
  Initially, the source node defines the number of MACs appended to the end of each native packet. This number of MACs is denoted as $l$. Then, the source node chooses randomly a value $u$ which is the number of codewords that will be used in the generation process of each MAC. To define the codewords that will be used in the generation of the $l$ MACs, the source node makes use of $l$ random integers $r_1, r_2, \ldots, r_l$, where $r_j \in [1, m]$ for $j = 1, \ldots, l$. These random integers are calculated based on a pseudo-random function. Each $r_j$ represents the indexes of the $u$ codewords that will be used in the generation process of each MAC. Also, a hash function $h : \mathbb{F}_p^u \rightarrow \mathbb{F}_p$, where $\mathbb{F}_p$ is a finite field of size $p$, is defined by the source node. This hash function will be used by the source node to create the hash value of the $u$ codewords. Then, based on the number of MACs (i.e., $l$), the KDC distributes $l$ keys $k_1, k_2, \ldots, k_l$ to the source node. Finally, the KDC selects, based on the key distribution model, described in Section 4.3, one key from those $l$ keys and distributes it to each non-source node.
- MAC
  The source node calculates $l$ MACs and appends them to the end of each native packet. Each MAC is calculated as follows:

$$MAC_{i,j} = E\left(id_{i,j}, r_j, h_{i,j}\right)_{k_{i,j}}, \tag{3}$$

  where $i = 1, \ldots, n$ and $j = 1, \ldots, l$.
  Moreover, in Eq. 3, $E(.)$ denotes encryption using the key $k_{i,j}$, which is one of the $l$ keys, distributed by the KDC. In addition, $id_{i,j}$ denotes the index of this key, $r_j$ is the index of $u$ codewords, and $h_{i,j}$ is the output of the hash function $h$ taking as input $u$ codewords.
  More precisely, for XOR NC, the hash function $h$ is defined as follows:

$$h_{i,j} = m_{i,r_{j,1}} \oplus \ldots \oplus m_{i,r_{j,u}}, \tag{4}$$

  where $i = 1, \ldots, n$ and $j = 1, \ldots, l$.
  Then, the source node transmits the following:

$$\left(M_i, id_{i,1}, MAC_{i,1}, \ldots, id_{i,l}, MAC_{i,l}\right), \tag{5}$$

  where $i = 1, \ldots, n$.
  We illustrate an example of the MAC generation in Fig. 4.
- Verify
  Each non-source node (i.e., intermediate and destination nodes) holds a key which was distributed by the KDC as it has been mentioned in the Setup phase. Using this key, the non-source node decrypts the corresponding MAC of the received coded packet. Thus, the non-source node obtains the indexes of the $u$ codewords and the value of the hash function $h$ that was calculated in the source node. Afterwards, the non-source node calculates the hash value $h'$ of the codewords that correspond to the obtained indexes, according to Eq. 4, and compares it with the obtained hash value $h$. If they are equal, the received coded packet is considered as uncorrupted and is accepted; otherwise, the received coded packet is discarded.

## 6 Security analysis

In this section, we analyze the security of our proposed scheme in terms of the probability that a corrupted packet cannot be detected by the next hop and how this probability can be affected by the number of codewords ($u$) as well as the number of MACs ($l$).

We have considered that the adversary (i.e., the compromised node) knows the distributed key, and thus, based on Eqs. 3 and 4, he is able to identify which codewords are

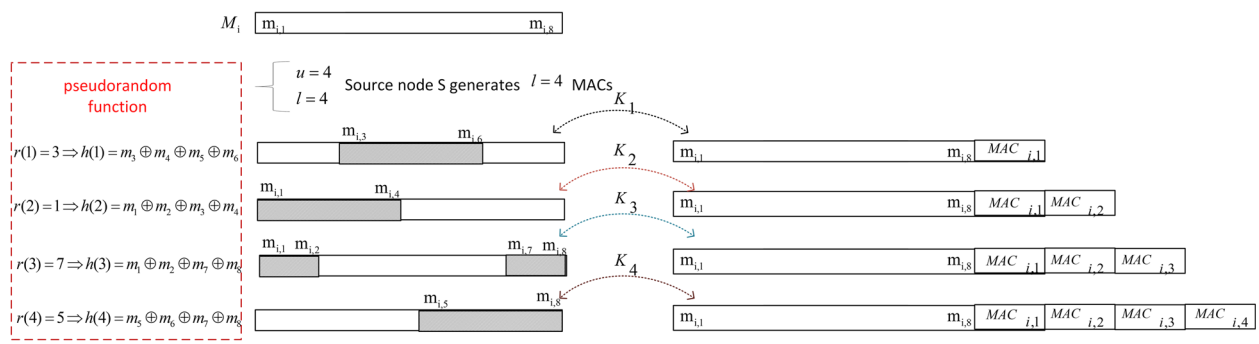


**Fig. 4** The source node has to calculate and append 4 MACs to the end of the native packet $M_i$, which consists of eight codewords (i.e., $m_i, \ldots, m_8$). To generate the 4 MACs, a pseudo-random function is used firstly to generate four random values (i.e. $r_1, \ldots, r_4$), one for each MAC. Based on these random values, the source node defines the indexes of the codewords, which will be the input to the hash function $h$ in order to calculate the corresponding hash values $h(1), \ldots, h(4)$

verified by the corresponding MAC. Hence, he can corrupt these codewords and generate a false MAC for the corrupted packet. However, the corrupted codeword can be detected by the next node with a high probability.

**Theorem 1.** *The probability that a corrupted codeword in one MAC is not detected by the next node is not greater than* $\left(1-\frac{u}{m}\right)^{l-1}$.

*Proof.* In our proposed scheme, each MAC verifies the integrity of $u$ codewords out of $m$ codewords. Therefore, the probability that each codeword can occur in one MAC is $\frac{u}{m}$. However, the probability that this codeword does not occur in other MACs is calculated as follows:

$$p_{\text{occur}} = \left(1-\frac{u}{m}\right)^{l-1} \tag{6}$$

Consequently, if an adversary corrupts a codeword of a MAC, then the probability that the corrupted codeword will not be detected by the next node is given by Eq. 6. □

From Theorem 1, it is clear that the probability of a corrupted packet not to be detected by the next node is given by Eq. 6 as well. In Fig. 5, based on Eq. 6, we illustrate this probability in terms of the number of codewords for different number of MACs. As it is shown in Fig. 5, by increasing the number of codewords, the probability of a corrupted packet not to be detected by the next node decreases.

In addition, the probability of a corrupted packet not to be detected by the next node is also affected by the number of MACs.

**Theorem 2.** *By increasing the number of MACs, the probability that a corrupted packet not to be detected by the next hop decreases.*

*Proof.* Suppose that the total number of compromised nodes is $c$. Consequently, the adversary can totally obtain $c$ keys. Thus, the probability that the adversary can decrypt one MAC of the coded packet is denoted as $p_k$ and defined as follows:

$$p_k = \frac{c}{l} \tag{7}$$

Hence, adopting Eq. (12) proposed in [24], the probability that the adversary, holding $c$ keys, can decrypt $c$ MACs out of the $l$ MACs, is the following:

$$p_{\text{dec}}(c) = \binom{l}{c} p_k^c \left(1-p_k\right)^{l-c} \tag{8}$$

where $c \ll l$.

As a result, the probability that a corrupted packet not to be detected by the next hop is given by Eq. 8 as well. According to this equation, it is clear that by increasing the number of MACs, the probability that the corrupted packet not to be detected by the next hop decreases. □

In Fig. 6, based on Eq. 8, we illustrate this probability in terms of the number of MACs for different number of compromised nodes.

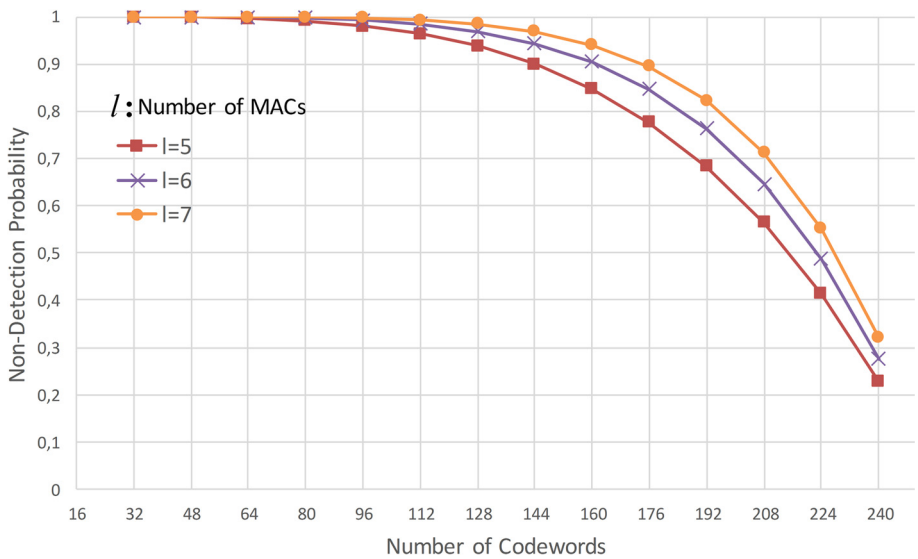


**Fig. 5** Corrupted packet non-detection probability in terms of the number of codewords

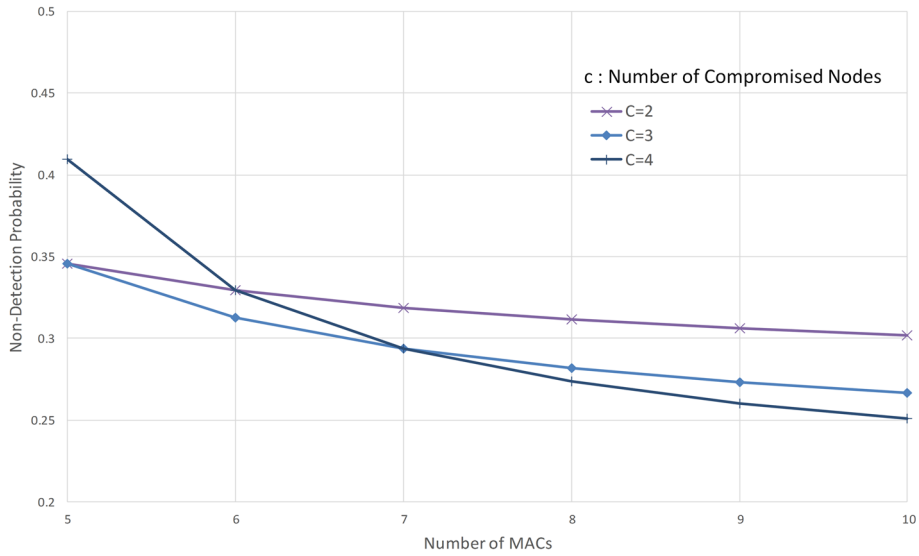


**Fig. 6** Corrupted packet non-detection probability in terms of the number of MACs

## 7 Performance evaluation

In this section, we analyze the performance of our MAC-based scheme in terms of communication bandwidth and computational complexity.

### 7.1 Communication bandwidth

To calculate the communication overhead of our proposed scheme, we take into consideration (a) the number of codewords of the native packet, (b) the $l$ MACs appended to the end of each native packet, and (c) the $l$ key indexes appended to the end of each native packet as well.

Each native packet has $m$ codewords and each codeword requires $\log_2 p$ bits. Thus, the bit length of each native packet is $m * \log_2 p$ bits.

On the other hand, according to Eq. 3, each MAC consists of a hash value, a random number, and the key index. Based on Eq. 4, the hash value is the XOR result of $u$ codewords and thus, it requires $\log_2 p$ bits.

Moreover, the random number, used to identify the indexes of the codewords, requires $\log_2 m$ bits. Finally, the index of the key requires $\log_2 |l|$ bits. Consequently, the bit length of $l$ MACs is $l * (\log_2 p + \log_2 m + \log_2 |l|)$ bits.

In addition, each key index appended to the end of each native packet requires $\log_2 |l|$ bits. Therefore, the bit-length of $l$ key indexes is $l * (\log_2 |l|)$ bits. However, similar to [24], in order to reduce the length of the coded packets in our scheme, only one key index can be appended to the end of each native packet.

Thus, our MAC-based scheme has the following communication overhead:

$$\frac{l * (\log_2 p + \log_2 m + \log_2 |l|) + \log_2 |l|}{m * \log_2 p} \quad (9)$$

Assuming that the number of MACs (i.e., $l$) is constant, $m$ is equal to 256, and $p$ is 256-bit long, the value of $\log_2 |l|$ and the value of $\log_2 m$ are negligible compared to the value of $\log_2 p$. Hence, from Eq. 9, the communication overhead is calculated as $\frac{l}{m}$, which means that our scheme has the same communication overhead as the proposed scheme in [24]. However, our proposed scheme can detect the corrupted packets earlier (i.e., next node), and thus, communication bandwidth is saved.

### 7.2 Computational complexity

According to Eqs. 3 and 4, $(u - 1)$ XOR operations are needed to generate each MAC in our scheme. Thus, the generation of $l$ MACs requires $l * (u - 1)$ XOR operations. Nevertheless, the proposed scheme in [24] requires $l * u$ XOR operations to generate $l$ MACs.

Moreover, to verify a coded packet in each non-source node, $(u - 1)$ XOR operations are required in our scheme, since each non-source node calculates the hash value of the codewords that corresponds to the obtained indexes, according to Eq. 4. On the other hand, the scheme proposed in [24] requires $l * u$ XOR operations for verification. In Fig. 7, we illustrate the number of XOR operations required to verify the coded packet in our scheme and the scheme proposed in [24]. It is worthwhile to mention that, in contrast to the scheme proposed in [24],

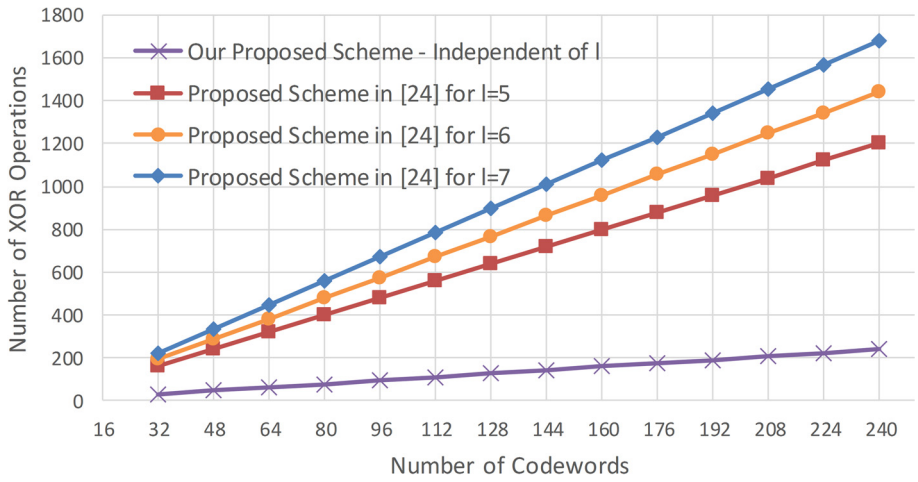


**Fig. 7** The number of XOR operations required to verify a coded packet in terms of the number of codewords in our proposed scheme and the scheme proposed in [24]

our scheme does not depend on the number of MACs (i.e., $l$).

Table 2 summarizes the number of XOR operations required for MAC generation and verification in our proposed scheme and the scheme proposed in [24]. According to Table 2, our scheme requires less XOR operations in total than the scheme proposed in [24], and thus, our scheme is more efficient in terms of computational complexity.

## 8 Conclusions

In this paper, we have been proposed an efficient MAC-based scheme providing resistance against pollution attacks in XOR NC-enabled WBANs for remote patient monitoring systems. Our proposed scheme makes use of a number of MACs which are appended to the end of each native packet. Our results show that the proposed MAC-based scheme is more efficient compared to the scheme proposed in [24], in terms of communication bandwidth and computational complexity. The proposed scheme in [24] is the most competitive scheme in the literature for securing XOR NC against pollution attacks in resource-constrained wireless networks. Particularly, our scheme saves communication bandwidth, since it detects corrupted packets in the next hop with high probability, and its computational complexity is lower because it requires less XOR operations than the scheme proposed in [24].

**Table 2** Number of XOR operations

| | Proposed scheme | [24] |
|---|---|---|
| MAC | $l * (u - 1)$ | $l * u$ |
| Verify | $u - 1$ | $l * u$ |

**Competing interests**
The authors declare that they have no competing interests.

**Authors' contributions**
All authors contributed extensively to the work presented in this paper.

**Acknowledgements**
The research leading to these results has received funding from the European Community's Seventh Framework Program [FP7/2007-2013] under grant agreement number 285969 [CODELANCE]. The first author would like to acknowledge support from the Fundacão para a Ciência e a Tecnologia (FCT - Portugal), through grant number: SFRH/BD/102029/2014.

Received: 1 November 2015 Accepted: 4 April 2016
Published online: 22 April 2016

**References**

1. A Solanas, C Patsakis, M Conti, I Vlachos, V Ramos, F Falcone, O Postolache, P Perez-martinez, R Pietro, D Perrea, et al., Smart health: a context-aware health paradigm within smart cities. Commun. Mag. IEEE. **52**(8), 74–81 (2014)
2. RS Istepanaian, Y-T Zhang, Guest editorial introduction to the special section: 4g health—the long-term evolution of m-health. Inf. Technol. Biomed. IEEE Trans. **16**(1), 1–5 (2012)
3. S Movassaghi, M Abolhasan, J Lipman, D Smith, A Jamalipour, Wireless body area networks: a survey. Commun. Surv. Tutorials IEEE. **16**(3), 1658–1686 (2014)
4. M Fengou, G Mantas, D Lymberopoulos, N Komninos, S Fengos, N Lazarou, A new framework architecture for next generation e-health services. Biomed. Health Inf. IEEE J. **17**(1), 9–18 (2013)
5. U Varshney, Pervasive healthcare: applications, challenges and wireless solutions. Commun. Assoc. Inf. Syst. **16**(1), 3 (2005)
6. G Mantas, D Lymberopoulos, N Komninos, in *Engineering in Medicine and Biology Society, 2009. EMBC 2009. Annual International Conference of the IEEE, Minneapolis, Minnesota, USA*. Integrity mechanism for ehealth tele-monitoring system in smart home environment (2009), pp. 3509–3512
7. B Latré, B Braem, I Moerman, C Blondia, P Demeester, A survey on wireless body area networks. Wireless Netw. **17**(1), 1–18 (2011)

8. E Kartsakli, A Antonopoulos, L Alonso, C Verikoukis, A cloud-assisted random linear network coding medium access control protocol for healthcare applications. Sensors. **14**(3), 4806–4830 (2014)
9. E Kartsakli, AS Lalos, A Antonopoulos, S Tennina, MD Renzo, L Alonso, C Verikoukis, A survey on M2M systems for mHealth: a wireless communications perspective. Sensors. **14**(10), 18009–18052 (2014)
10. M Chen, S Gonzalez, A Vasilakos, H Cao, VC Leung, Body area networks: a survey. Mobile Netw. Appl. **16**(2), 171–193 (2011)
11. J Sen, A survey on wireless sensor network security. Int. J. Commun. Netw. Inf. Secur. **1**, 55–78 (2009)
12. A Boulis, D Smith, D Miniutti, L Libman, Y Tselishchev, Challenges in body area networks for healthcare: The mac. Commun. Mag. IEEE. **50**(5), 100–106 (2012)
13. E Kartsakli, A Antonopoulos, A Lalos, S Tennina, M Renzo, L Alonso, C Verikoukis, Reliable mac design for ambient assisted living: Moving the coordination to the cloud. Commun. Mag. IEEE. **53**(1), 78–86 (2015)
14. S Tennina, M Di Renzo, E Kartsakli, F Graziosi, A Lalos, A Antonopoulos, PV Mekikis, L Alonso, WSN4QoL: a WSN-oriented healthcare system architecture. Int. J. Distributed Sensor Netw. **2014**, 1–16 (2014)
15. S Movassaghi, M Shirvanimoghaddam, M Abolhasan, D Smith, in *Local Computer Networks (LCN), 2013 IEEE 38th Conference On, Sydney, NSW*. An energy efficient network coding approach for wireless body area networks (2013), pp. 468–475
16. AS Lalos, E Kartsakli, A Antonopoulos, S Termina, M Di Renzo, L Alonso, C Verikoukis, in *Global Communications Conference (GLOBECOM), 2014 IEEE*. Cooperative compressed sensing schemes for telemonitoring of vital signals in wbans (IEEE, 2014), pp. 2387–2392
17. I-H Hou, Y-E Tsai, TF Abdelzaher, I Gupta, in *INFOCOM 2008. The 27th Conference on Computer Communications. IEEE*. Adapcode: Adaptive network coding for code updates in wireless sensor networks (IEEE, 2008)
18. A Antonopoulos, C Verikoukis, Network-coding-based cooperative ARQ medium access control protocol for wireless sensor networks. Int. J. Distributed Sensor Netw. **2012** (2011). Article ID 601321, 9 pages
19. R Ahlswede, N Cai, S-Y Li, RW Yeung, Network information flow. Inf. Theory IEEE Trans. **46**(4), 1204–1216 (2000)
20. S-YR Li, RW Yeung, N Cai, Linear network coding. Inf. Theory IEEE Trans. **49**(2), 371–381 (2003)
21. T Ho, R Koetter, M Medard, DR Karger, M Effros, in *Proc. IEEE Int. Symp. Information Theory, Yokohama, Japan, Jun./Jul. 2003*. The benefits of coding over routing in a randomized setting (2003), p. 442
22. T Ho, M Médard, R Koetter, DR Karger, M Effros, J Shi, B Leong, A random linear network coding approach to multicast. Inf. Theory IEEE Trans. **52**(10), 4413–4430 (2006)
23. S Katti, H Rahul, W Hu, D Katabi, M Médard, J Crowcroft, XORs in the air: practical wireless network coding. IEEE/ACM Trans. Netw. (ToN). **16**(3), 497–510 (2008)
24. Z Yu, Y Wei, B Ramkumar, Y Guan, in *INFOCOM 2009, IEEE*. An efficient scheme for securing XOR network coding against pollution attacks (IEEE, Rio de Janeiro, 2009), pp. 406–414
25. W Cheng, L Yu, F Xiong, W Wang, in *Global Telecommunications Conference (GLOBECOM 2010), 2010 IEEE*. Trusted network coding in wireless ad hoc networks (IEEE, Miami, FL, 2010), pp. 1–5
26. J Dong, R Curtmola, C Nita-Rotaru, DK Yau, Pollution attacks and defenses in wireless interflow network coding systems. Dependable Secure Comput. IEEE Trans. **9**(5), 741–755 (2012)
27. A Esfahani, A Nascimento, J Rodriguez, JC Neves, in *Computers and Communication (ISCC), 2014 IEEE Symposium On*. An efficient MAC-signature scheme for authentication in XOR network coding (IEEE, Funchal, Madeira, 2014), pp. 1–5
28. MN Krohn, MJ Freedman, D Mazieres, in *Security and Privacy, 2004. Proceedings. 2004 IEEE Symposium On*. On-the-fly verification of rateless erasure codes for efficient content distribution (IEEE, 2004), pp. 226–240
29. C Cheng, T Jiang, Q Zhang, TESLA-based homomorphic MAC for authentication in p2p system for live streaming with network coding. Selected Areas Commun. IEEE J. **31**(9), 291–298 (2013)
30. A Esfahani, D Yang, G Mantas, A Nascimento, J Rodriguez, Dual-homomorphic message authentication code scheme for network coding-enabled wireless sensor networks. Int. J. Distributed Sensor Netw. **2015**, 510251 (2015). doi:10.1155/2015/510251. Accessed 2015-02-06
31. R Canetti, J Garay, G Itkis, D Micciancio, M Naor, B Pinkas, in *INFOCOM'99. Eighteenth Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings. IEEE*. Multicast security: a taxonomy and some efficient constructions, vol. 2 (IEEE, New York, NY, USA, 1999), pp. 708–716