HLDCA-WSN: Homomorphic Lightweight Data Confidentiality Algorithm for Wireless Sensor Network

Hassan Noura, Damien Couroussé
Univ. Grenoble Alpes, F-38000 Grenoble, France
CEA, LIST, MINATEC Campus, F-38054 Grenoble, France
Email: firstname.lastname@cea.fr

***Abstract*—Wireless Sensor Networks (WSN) has become more and more important in many applications especially those required a high level of security such as: commercial, military and telemedicine applications. However, security in WSN suffers from several kinds of attacks (ranging between passive and active attacks). Eavesdropping attack remains the most powerful attack, since it has the capability to compromise the confidentiality of the whole packet content. In this context, several solutions and techniques have been presented in the literature, to ensure a secure transmission of packets in a large scale WSN. Unfortunately, many of these solutions failed to meet the main characteristics of WSN (limited energy consumption, low power, large bandwidth), and are considered as not efficient candidates to deal with tiny devices. For this reason, a novel homomorphic lightweight security scheme HLDCA-WSN based on dynamic permutation layer that is performed on a set of packets (denoted by generation) is proposed and discussed in this paper. HLDCA-WSN scheme overcomes passive attacks and ensures a significant reduction of computational complexity, energy cost, and communication overhead. Moreover, the dynamic property of the proposed scheme adds more robustness against traditional and physical attacks. The efficiency of the HLDCA ciphering scheme is demonstrated by an extensive security analysis and simulation results.**

I. Introduction

Nowadays, WSN is employed in different applications such as environmental monitoring, smart houses, buildings, traffic monitoring, military surveillance, and health monitoring or even in bodies (patient monitoring). Typically, WSN consists of small devices (sensor nodes) that have the capability to gather information about their physical environments. These sensor nodes are connected with their sensor vicinity (the sink) to build a network topology. Currently, several kinds of WSNs are employed such as ZigBee [1] and WirlessHART [2]. these proptocols ensures a multi-hop routing communication among nodes through the use of wireless channels. The user in WSN (see Fig. 1) can be classified into two types:

1) **a sensor node** that generates and transmits stream data corresponding to a specific querier.
2) **a querier** that poses queries on the sensor reading, and periodically receives stream data from the sink.

In fact, WSN has unique characteristics that make its design different from traditional networks. These characteristics can be presumed by its limited resources, limited computing power, limited energy as well as limited battery lifetime, that can be depleted rapidly (depending on the transmission rate).

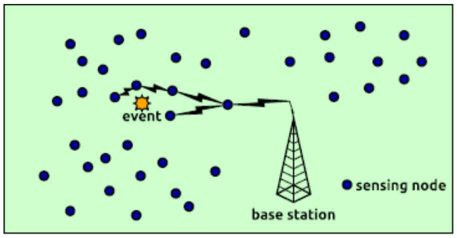


Fig. 1: Wireless sensor networks scheme

On the other hand, security in WSN is considered as an essential requirement and a crucial point that must be achieved in any practical implementation. However, in addition to the previous mentioned limitations, WSN is vulnerable to several forms of attacks such as passive and active attacks [3], [4], which can destroy the confidentiality of the network, if the adversary succeeds to extract some information about the transmitted packets. Moreover, in the way of building a robust and secure WSN, three fundamentals properties must be respected: **Data Confidentiality (DC)**, to ensure that the transmitted data is secure enough against any unauthorized access, hence prevents passive attacks. **Data Integrity** to preserve the packet content during transmission, so data exchange is occurring only between legitimated parties. And **Source Authentication** to ensure packet protection against active attacks. The conventional technique to ensure data confidentiality is to encrypt the payload of packets between sensor nodes and queriers. From here comes our idea, by proposing a new homomorphic DC algorithm called **HLDCA** that ensure the security of the system by encrypting the payload of each packet before transmission. This is achieved by the use of a simple permutation technique and a dynamic key. Hence, due to the lower computational cost that involved, the proposed scheme can be well integrated with limited devices.

A. Related work

Recently, several lightweight encryption solutions with different concepts and paradigms have been proposed in the literature to ensure data confidentiality in WSN. These algorithms can be classified into two main classes: symmetric and asymmetric ciphers. For **Symmetric ciphers**, only one key is exchanged between the transmitter and the receiver secretly and used for encryption and decryption processes. Many techniques are proposed based on this approach, such as SPINS [5], TinySec [6], MiniSec [7]. On the other hand, for **Asymmetric cipher** (based on elliptic curve cryptography [8]), two keys are used: one public key to encrypt the message, so anyone can encrypt the message, and one private key to decrypt the message, so only the person who possesses the private key can decrypt the message. Many techniques have been proposed based on this approach such as WMECC [9] and TinyECC [10]. However, asymmetric cipher is inappropriate for WSN due to its expensive computational operations and memory requirement. Moreover, symmetric cipher approach is divided into two different techniques: Stream Ciphers (SC) and Block Ciphers (BC). SC is based on the encryption of bit-by bit or byte-by byte input at one time. But BC is based on the encryption of a block (set of bits or bytes) at one time. In this context, SC is considered as more efficient to be used for resource-constrained environments, with one condition: the initialization vector IV should not be used more than once as explained in [11]. Consequently, a relatively long IV value must be introduced [12], which imposes a communication packet overhead (vary between 8 bytes and 30-byte length), and reduces the performance of the whole WSN. On the other side, if short IVs are used, the security of the system will be minimized [12]. For this reason, block cipher BC is used more than SC to achieve the encryption process with a high level of security. The most famous block cipher is the AES [13] with its operation modes such as: Output Feedback (OFB) and Counter (CTR) [14] that are the most suitable modes for WSN applications. Since, the block cipher in OFB and CTR mode behaves as a stream cipher that produces a key-stream of pseudo-random bytes. And, the encryption /decryption processes are just a XOR operation between the streams with the plain/cipher data.

However, within the high level of security offered by AES, a high computation complexity is required, since it is based on multi-round functions. In [15], a real implementation demonstrates that AES requires a high energy consumption and a short node lifetime. In addition, the average performance of AES has been compared to other block cipher's (Skipjack [16], or RC5 [17]) on a different range of sensor standard platforms. Thus, indicates that AES is not appropriate to be deployed in WSN. Furthermore, TinySec [18] technique is used, based on TinyOs security platforms, and provides a similar level of security of SPINS. TinySec uses other block cipher instead of AES, such as Skipjack, or RC5 that are tailored to integrate with WSN nodes. Moreover, Skipjack is used in the majority of well-known security platforms for WSN, such as in SenSec [19] and TinyKey-Man [20]. After that, MiniSec [7] technique is proposed based on offset codebook mode (OCB) [21] which reduces the energy consumption compared with TinySec whilst achieving the same level of security.

These WSN protocols ensure a secure data transmission over the network, but lack of a **high network performance**. Moreover, the limitations existed in WSN prevent these traditional security tools to achieve the security aspects. To overcome this problem, especially in constrained resources WSN, a new efficient cipher tailored to tiny devices is proposed. The proposed scheme achieves a high level of security whilst ensuring a good network performance. Hence, the proposed lightweight cipher technique can replace the use of multi-round functions or the use of recently dynamic diffusion schemes (integer or binary) that require computation complexity $O(l^3)$, where l is the payload packet length expressed in bytes, since it requires a low computation complexity $O(l)$.

B. Problem Statement

The existing challenges of DC schemes make its implementation in WSN a difficult task. In this context, two problems can be viewed:

1) The first problem is that data confidentiality is ensured by the use of block cipher with multiple iterations. Thus, necessities a high computational complexity.
2) The second problem is that data aggregation process is provided by the existing DC schemes, due to the decryption of received packets at each aggregator node.

For this reason, an efficient algorithm that ensures data confidentiality with a minimum number of rounds, low computational complexity, low energy consumption, and low communication overhead must be investigated for the deployment in WSN.

For this reason, and from our cryptographic view point, data confidentiality can be achieved based on the use of a dynamic diffusion layer, as proved in our previous work [22], [23], where a dynamic integer and binary diffusion layers are employed for a set of packets respectively. However, the diffusion process requires cubic Computation Complexity (CC). Consequently, the proposed algorithm must agree the CC property also.

Moreover, an end-to-end data confidentiality must be fulfilled, in order to employ data aggregation. This property is not discussed in previous approaches, but in our approach a homomorphic technique is used, where each indeterminate node aggregates the decrypted payloads together, and the resultant aggregated data is encrypted before forwarding. This technique reduces the transmission overhead. Briefly talking, the proposed solution is a **Homomorphic DC Algorithm (HDCA)**, based on a flexible, simple and dynamic permutation process, that attains the linear CC property and the homomorphic propriety. So, it ensures data confidentiality with the respect of data aggregation criterion. As result, it achieves a secure transmission of payloads with a low computational complexity and minimum energy consumption.

C. Contribution

Actually, WSN is intended to support the transmission of multimedia streams for the end users with a high data rates (image, videos). For that, it is desirable to realize a cipher scheme that ensures an end-to-end data confidentiality while satisfying the CC property to speed up data processing. Also, it is preferable to ensure an efficient implementation with aggregation process. All these properties are meeting in the realization of our proposed scheme. Briefly talking, in this paper, a robust and efficient HDCA with a low computational complexity is proposed. This scheme satisfies homomorphic property to overcome the problem of data aggregation occurred at each aggregator node, and based on a dynamic permutation technique that is changed for each generation, to prevent eavesdropping attack in a selective manner. Moreover, the proposed permutation process is very simple, consisting of a load and store operations, which require only a single cycle for the most embedded systems. Also, a dynamic key is used to attain Shannon famous properties (confusion and diffusion). All these characteristics make the scheme very suitable for limited resources sensors nodes. One main advantage of this proposed algorithm compared to the previous standardized solutions or recent lightweight cipher schemes is the good WSN performance that is provided within a high security level.

Furthermore, in this paper, three scenarios are discussed to deal with our scheme. And, the proposed algorithm consists of three steps: (i) key derivation function produces the initialization elements, which are used later in the permutation process. (ii) The permutation layer denoted by ψ, generated and applied with a single ψ for the first approach and with h different ψ for the second approach for each generation (one generation contains h payload packets) as in [24], [25]. The third approach is employed by the use of a **Dynamic Packet Length Scheme DPLC** as in [26], based on a set of packets having different length. Our work meet the objectifs of DPLC, which introduces a significant reduction in the transmission overhead (13%) and a reduction in the energy consumption (41.8%).

As results, five contributions can be highlighted by the use of our proposed scheme:

1) **Efficiency:** reduces the round iterations to one, and define a simple lightweight, key dependent, permutation algorithm that can ensure a better randomness degree.
2) **High Throughput:** By applying the permutation process on a set of packets instead of a single packet.
3) **Robustness:** Due to the use of a dynamic key, instead of static one, which prevents an eavesdropper to reveal any useful information about the packet content.
4) **Flexibility** The proposed scheme flexible in number of packets (h packets) and in length of packets l (third scenario).
5) **Transparency**: our scheme is transparent to intermediate aggregation processes due to the exchangeability of permutation encryption and packets combination (aggregation).

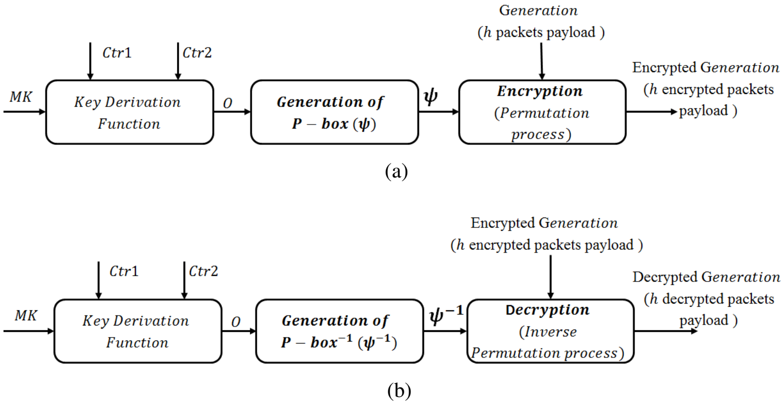

Generation
(h packets payload)
Ctr1
Ctr2
MK
Key Derivation Function
O
Generation of P − box (ψ)
ψ
Encryption (Permutation process)
Encrypted Generation (h encrypted packets payload)
(a)
Encrypted Generation
(h encrypted packets payload)
Ctr1
Ctr2
MK
Key Derivation Function
O
Generation of P − box^{-1} (ψ^{-1})
ψ^{-1}
Decryption (Inverse Permutation process)
Decrypted Generation (h decrypted packets payload)
(b)

Fig. 2: The general approach at the emitter (a) and receiver side (b)

D. Organization

The rest of this paper is organized as follows. Section II presents the model of adversary and the concept of our proposed HDCA. Then, Section III discussed the proposed secure scheme by its three scenarios, and defines a new construction technique of key dependent, and flexible permutation algorithm that uses GRP algorithm [27]. Performance and security of the proposed scheme are analyzed in Section IV. Finally, Section VI presents our conclusion.

II. Preliminary

A. Model of Adversary

In this paper, we look to the adversary as the one who aims to intercept packets to reveal some useful information. This eavesdropper can be viewed from two points:

1) External eavesdropper that interest in monitoring of network links.
2) Internal eavesdropper that interest in compromising intermediate nodes and reading their memories.

B. Goal

The proposed scheme has been designed with the following goals in mind:

1) **Efficacy and efficiency:** As our approach is designed to be applied on sensor nodes, then it has to cope with the limitations existed in WSN. In this context, one round of dynamic permutation operation is used to make our proposal efficient on a larger number of software platforms. Also, the absence of S-boxes for diffusion and key expansion rend our proposal efficient in hardware implementation as well.
2) **Security against traditional attacks :** In fact, the cipher should provide strong resistance against exhaustive search attacks. A relatively large key size (128 bits) was therefore chosen for our approach.
3) **High Resistance degree against physical attacks**: Moreover, the proposed approach was designed in a

way that it has a strong resistance against known weaknesses and security attacks. Thus is done by the use of a dynamic key approach rather than a static one.

C. Proposed cipher concept

As mentioned before, the proposed scheme is based on the use of a dynamic permutation approach. This is provided due to the following limitations:

1) WSN has several constraints, which requires to implement a lower data confidentiality scheme with a linear computation complexity ($O\ (l)$).
2) The problem of aggregation process at each aggregator node, necessities the use of another paradigm. From here, the homomorphic property is added to our proposal.

In fact, the used permutation process is derived from a special case of the classic transposition cipher [28]. To define this process, let ψ be a random permutation vector $P-box$ with length l that contains unique element of set $\{1,\ 2,\ \ldots,\ l\}$. Additionally, $\psi(i)$ is the i^{th} element of ψ , then the product of two permutations $\psi1$ and $\psi2$ can be defined by $\psi1 \odot \psi2$, and is calculated as: $\psi1 \odot \psi2(i) = \psi1(\psi2(i))$. Let ψ^{-1} be the inverse of ψ with respect to the product operation. Here, each packet is defined as a row vector $m_i = \{m_{i,1},\ m_{i,2},\ \ldots,\ m_{i,l}\}$ of length l, defined on Galois finite field F, where $i = 1,\ 2,\ \ldots,\ h$. Now, consider a general multicast case in which one source s needs to deliver a series of packets $m_1,\ m_2,\ \ldots,\ m_h$ to a set of sinks, where h is the capacity of this multicast session.

The Permutation Process (PP) π on m_i using ψ, used to encrypt the content of original vector is defined as following:

$$c_i = \pi(m_i, \psi) = \{m_{i,\ \psi(1)},\ m_{i,\ \psi(2)}\ \ldots,\ m_{i,\ \psi(l)}\} \tag{1}$$

Correspondingly, the inverse PP can be applied on c_i using ψ^{-1} to recover the original packet content, and is defined as following:

$$d_i = \pi(c_i, \psi^{-1}) = \{m_{i,\ \psi^{-1}(1)},\ m_{i,\ \psi^{-1}(2)},\ \ldots,\ m_{i,\ \psi^{-1}(l)}\} \tag{2}$$

The PP is homomorphic since the encrypted sequence corresponding to reordering the original sequence, without modifying any of their symbols. Let $\cdot$ and $*$ denote the addition and multiplication operations over the Galois finite field F. Indeed, PP can ensure the two main homomorphic properties:

1) Additively homomorphic: $\pi(m_i \cdot m_j) = \pi(m_i) \cdot \pi(m_j)$
2) Multiplicatively homomorphic: $\pi(\tau * m_i) = \tau * \pi(m_i)$

Thus due to the exchangeability with the aggregation process over F.

III. The Proposed Secure Scheme

The majority of existing traditional DC mechanisms demand a high resources and high complexity, and most of them require high energy consumption. Additionally, the recent homomorphic schemes require a complex key management process to provide the aggregation process. The aim here is to provide a scheme that ensures a lower computation complexity while preserving security aspects and aggregation property to deal with large scale WSN. This work defines a new kind of homomorphic DC scheme that is based on PP. The proposed DC scheme consists of three stages: (i) source encryption, (ii) intermediate forwarding, and (iii) destination decryption. Moreover, the proposed Cipher Scheme (CS) and the proposed Decipher Scheme (DS) are applied at the source and sink side as seen in Fig.2 (a)-(b), respectively.

```
procedure KEY_UPDATE($Mk,\ SK_{c1},\ adin,\ i, c1\ , c2$)
    if ($Ctr_2 \% w == 0$) then
                                                  ▷ Update the session key

        $Ctr_1 \leftarrow Ctr_1 + 1$
        $SK_{Ctr_1} \leftarrow SHA-512(MK||c1||adin)$
    end if
                                                  ▷ Produce the dynamic key

    $O_{Ctr_2} \leftarrow SHA-512(SK_{Ctr_1}||Ctr_1||Ctr_2)$
    $DK_{Ctr_2} \leftarrow LSB(O_i,\ 4 \times l)$
    return $DK_{Ctr_2}, SK_{Ctr_1},\ Ctr_1,\ Ctr_2$
end procedure
```

TABLE I: Key update's algorithm

First, a general description of the proposed scheme is presented in this section, and then a deep explanation of the three steps that composed the algorithm is performed. After that, three scenarios derived from the proposed schemes are explained in details.

A. The General Mechanism

A secret key is exchanged between sensor nodes and base station, before establishing any communication. Besides, a Homomorphic DC is presented to ensure security and efficiency utilization of WSN (permits to ensure better network performance). Also, a header extension denoted by H with 32 bit length is used, and consists of 24 bits for the Number of Generation, 4 bits for the Generation Size (GS), and 4 bits for the sequence number of packets (NP). Thus, provide protection against replay attack and adds more independence to the system, by using it as Nonce in the derivation function of the dynamic key. A process of re-new for session key is applied after $2^{32}-1$ generations.

B. The Proposed Secure Scheme at Source Side

The proposed cipher at the emitter side is illustrated in Fig. 2. Generally, in realistic WSN scenarios, such as multimedia data (compressed image or video), the source node may need to transmit a large volume of data M. Initially, the source divide the large amount of data M into different generations $M^1, M^2, \ldots, M^n$. Then, break up each generation into different packets $M^j = \{m_1^j, m_2^j, \ldots, m_h^j\}$. Two main steps are applied by each source node, and existed on the three proposed scenarios: **The Dynamic Key Generation** and **The proposed Permutation Layer**.

1) Dynamic Key Generation: The dynamic key of each generation is produced using HASH-CTR DRBG, to ensure a high randomness degree and a good performance level [29]. Besides, to overcome the fixed key problem, the **Dynamic**

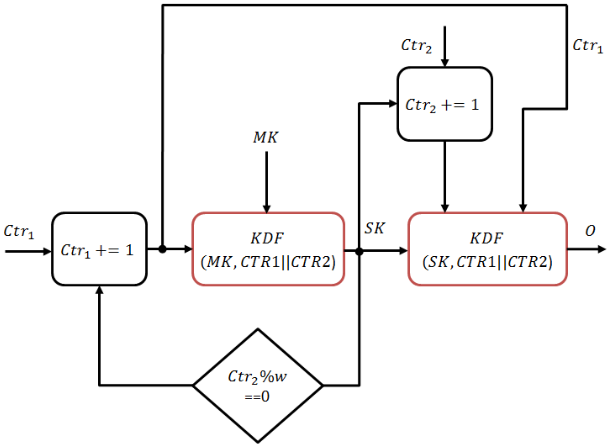


Fig. 3: Proposed key derivation function

```
procedure GRP($R1$, $R2$)
    $j \leftarrow 0$
                ▷ If the control register bit is zero, put it corresponding index at left

    for $i \leftarrow 0$ to $n-1$ do
        if $CR[i] == 0$ then
            $R3[j++] \leftarrow R1[i]$
        end if
    end for

    ▷ After that, if the control register bit is one, put it corresponding index at right

    for $i \leftarrow 0$ to $n-1$ do
        if $CR[i] == 1$ then
            $R3[j++] \leftarrow R1[i]$
        end if
    end for
                                        ▷ $R3$ is a the output permutation vector

    Return $R3$
end procedure
```

TABLE II: GRP permutation algorithm

```
procedure PERM($DK$, $l$, $rp$)
                                        ▷ $L$ is the length of input vector

    $\psi \leftarrow 1$ to $l$

    for $w \leftarrow 1$ to $rp$ do
        $CR_w \leftarrow CR[(w-1) \times l \ : \ (w) \times l - 1]$
        $\psi = GRP(\psi, \ \underline{CR_w})$
        $\psi = GRP(\psi, \ \overline{CR_w} \ )$
    end for
                                        ▷ $\psi$ is a dynamic $Pbox$

    Return $\psi$
end procedure
```

TABLE III: Proposed permutation algorithm

key approach is used in our scheme instead of static one. This process is explained in the pseudo code of TABLE I and illustrated in Fig.3. It begins by the generation of session keys, and ends by the generation of dynamic keys for each session key. First, a single private key called 'Master Key' and denoted by MK is shared between the source node and the sink, and a random counter Ctr_1 is used (and can be produced by LFSR [30]) and updated for each w number of generations ($w = 999$). MK and Ctr_1 are concatenated with the $adin$ parameter (address of the source node), then hashed using SHA-512 in order to perform at the end the session key for the Ctr_1^{th} interval which denoted by SK_{Ctr_1}. Then, for each generation, the output session key SK_{Ctr_1} is combined with Ctr_1 and Ctr_2 (another counter value that is incremented for each dynamic key) and hashed using SHA-512 hash function to perform the dynamic key O value. Noting that the size of the Master MK is 128 bits, while the size of session SK_{c1} keys and O is 512 bits.

2) Proposed Permutation Layer: After the dynamic key generation, a Key Dependent Permutation Layer (KDPL) on h packets payloads is fulfilled. The necessary condition as simplicity, flexibility and efficiency in software and hardware implementation, were the reasons to choose GRP permutation algorithm [27] as a basic element of the KDPL generation. Moreover, the GRP permutation algorithm is described in TABLEII and in Fig. 5, where $R1$ is the input vector, CR is the configuration vector (control register) and $R3$ is the output permutation vector. Noting that, $R1$, CR and $R3$ have the same length. The basic idea of the GRP instruction is to divide the index into two groups according to the pseudo-random bit sequence (CR). If the bit in CR is 0, this index is moved to the first group. Otherwise, the element is moved to the second group.

Original GRP algorithm suffers from lower cryptographic performance such as low degree of (recurrence) randomness, low number of different (unique) P-boxes, and high number of fixed points. For this reason, an enhancement of this algorithm is presented in this paper, by proposing a new permutation algorithm as described in TABLE III. This techniques consists of iterating two times the GRP's algorithm with CR and $\overline{CR}$ control register permutation for the first and second iterations respectively. Additionally, the round function is iterated for multi-round, and for each round, a different control CR_i, $i = 1, \ 2, \ \ldots, \ rp$ is used. By using this technique, a high randomness degree is ensured, and a big number of different P-box ($\approx 0.8 \times l!$) is provided with a lower fixed points (close to 1 in average) and an acceptable CC ($O(l)$).

This transformation is iterated for $rp = 4$ times as shown in Fig.10. And, the result output vector ψ represents the primary P-box that possess a high cryptographic performance.

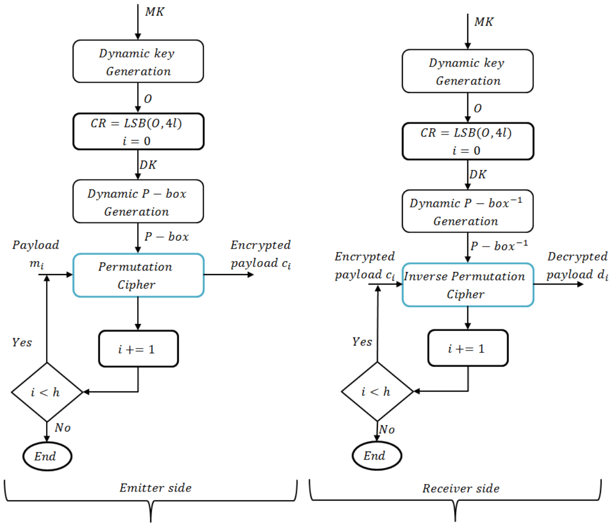
C. First Scenario: uses the same ψ

Initially, a set of payload packets is introduced, and a dynamic key denoted by DK is obtained directly by truncating $4 \times l$-bits of the Least Significant Bit (LSB) of the output O value (that produced as described previously). After that, the different CR_w can be obtained directly from DK. Each CR_i value is obtained from DK by the bits existed between $(w-1) \times l$ and $w \times l - 1$ {w=1, 2, 3, 4}.

Then, the proposed permutation generation algorithm with CR_w and w are used as input to produce the dynamic ψ value. Let us note that the size of dynamic key DK is variable depending of l. The length l here and in the second approach is fixed, to deal with fixed optimal length WSN schemes. the proposed permutation PP is applied in a byte-by-byte manner instead of bits-by-bits to provides a lower computation complexity. Hence, each packet in each generation (h corresponding to one generation) is permuted by using the produced ψ value, and defined as following:

$$c_i = \pi(m_i,\ \psi) \tag{3}$$

where m_i and c_i are the $i-th$ original and encrypted permuted packets payload respectively. The proposed HDCA at the emitter and receiver side for the first approach are illustrated in Fig. 4.



(a) (b)

Fig. 4: Architecture of the first approach (uses the same P-box for the overall packets payload) at the emitter (a) and receiver side (b)

D. Second Scenario: uses h different ψ

Here, in contrast to the first scenario, different P-boxes ($\psi_i,\ i = 1,\ 2,\ \dots,\ h$) instead of a single ψ are used. Ideally, those h different ψ values satisfy the following condition $\cap_{i=1}^{h} \psi_i = \emptyset$). In order to increase the security level, the generation of the h different P-box ψ_i is realized using a new technique that is based on two steps: the first step requires the primary P-box (ψ) that is generated similarly to the first scenario with h control parameters denoted as $X = \{x_1,\ x_2,\ \dots,\ x_h\}$. The set of control parameters $X = \{x_1,\ x_2,\ \dots,\ x_h\}$ is the produced key-stream obtained by iterating RC4 [31] with a seed value a, that is computed from O by truncating $512 - 4 \times l$ bits of Most Significant Bit (MSB) of O. While, the second step is based on a new linear transformation that consists of a random rotation process. Furthermore, the P-box of the i^{th} ψ_i is generated using a random value x_i as expressed in the following equation:

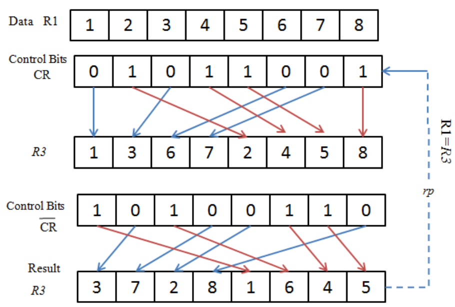


Fig. 5: Example of the proposed permutation $PERM$ algorithm with $l = 8$

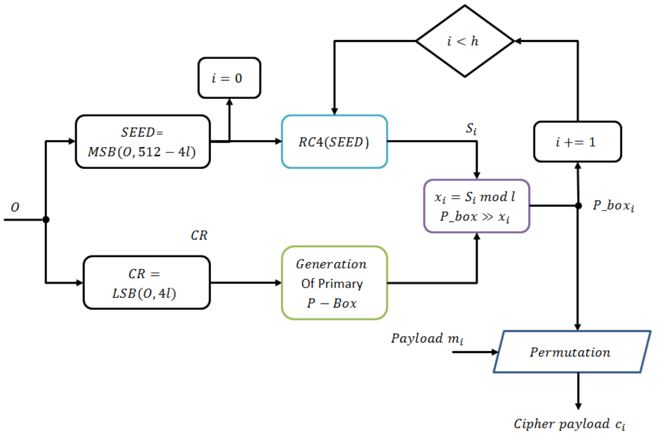


Fig. 6: Architecture of the second approach that uses h different P-boxes

$$\psi_i = \psi >> x_i,\ i = 1,\ 2,\ \dots,\ h \tag{4}$$

where $A >> B$ means that rotate A right for x_i times.

After that, the i^{th} P-box ψ_i is used to permute the i^{th} packet payloads as seen by this equation:

$$c_i = \pi(m_i, \psi_i) \tag{5}$$

This scenario increases the level of security by the new technique of permutation that it involved. Also, it reduces the whole cost, since the cost needed to apply h times of rotation vector, and generate h key-stream byte from RC4 cipher is low, due to the fact that RC4 is the most simple and fastest stream cipher(with linear complexity) and the rotation vector is not a complex operation. Consequently, The second scenario that is illustrated in Figure 7 is designed to respond to the main characteristics of WSN, and it achieves a lower CC with a high level of security.

E. Third scenario

This approach is presented to adapt our solution for WSN with dynamic packet length control scheme (DPLC) [32].

```
procedure ADAPTATION_OF_$\psi$($\psi$, $l\_i$, $l\_max$)
                                        ▷ $l$ is the length of corresponding input payload

                              ▷ $l\_max$ is the maximum length for the rest of payload packets
    for $j \leftarrow 1$ to $l\_max$ do
        if ($\psi[j] > l$) then
            $Delete\ \psi[j]$
        end if
    end for
    $l\_max \leftarrow l$
                                                   ▷ $\psi$ is a adapted $Pbox$ of length $l$

    Return $\psi$, $l\_max$
end procedure
```

TABLE IV: Proposed adaptation of the permutation vector for WSN with DPLC

DPLC is used due to its reduction of the transmission overhead and minimizing of the energy consumption especially in WSN. First, a set of packets with different length, where l_i is the length of i^{th} packet payload and l_max is the maximum length of packets existed in one set. Let us note here, in this case, the produced primary $P-box$ must has a length equal to l_max. The cost of this approach requires an additional computation complexity, but it is always linear, and designed to be low.

1) Adaptation of the first approach: The proposed adaptation for the first approach to support the DPLC scheme is described in TABLEIV. Initially, packets of each generation are arranged in an descending order according to their length. Then, a permutation process is performed, starting by the packet that has the maximum length. This packet is used later as the primary P-box with no necessary adaption. Then, next packets are selected in order, and the primary P-box ψ are the output of the permutation of each packet. Noting that, packets having the same length use the same adapted P-box. Hence, the adaptation process is applied one time for this kind of packets.

2) Adaptation for the second approach: The adaptation for the second approach is quite different from the first one, since the second approach is based on the use of different P-boxes. For this reason, the adaptation here is applied after producing each P-box ψ_i, $i = 1,\ 2,\ \ldots,\ h$ and defined as following:

$$\psi\_a_i = Adaptation\_of\_\psi(\psi_i,\ l_i) \tag{6}$$

Noting that, for the second approach, l_max remains fixed, since different P-boxes are employed. Then, the permutation of payload m_i is performed by using ψ_a_i, with a length similar to m_i. In fact, after the adaptation of the second approach, CC has more computational complexity compared to the original approach, but it is still linear and it is always acceptable compared to existing approaches. Additionally, an example of producing of dynamic different $P-box$ after adaptation is shown in Fig.8. Furthermore, this scheme can be used to ensure high level of security using DLPC in WSN.

F. The Proposed Secure Scheme at the receiver side

Upon receiving the packets, different steps are performed by the receiver:

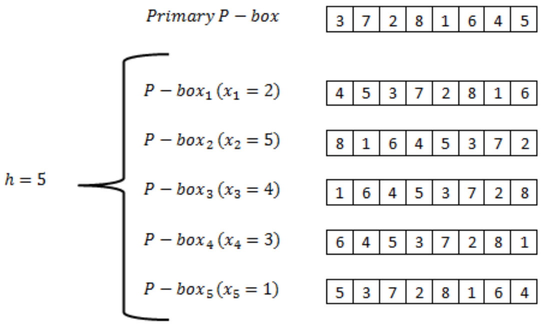


Fig. 7: Example of generation h different $P-box$ for the second approach with $h=5$ and $l=8$

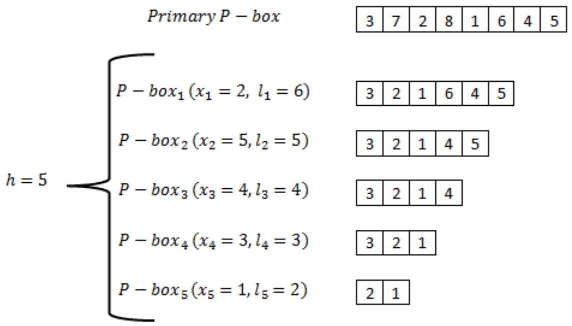

Primary P − box
3 7 2 8 1 6 4 5
h = 5
P − box₁ (x₁ = 2, l₁ = 6)
3 2 1 6 4 5
P − box₂ (x₂ = 5, l₂ = 5)
3 2 1 4 5
P − box₃ (x₃ = 4, l₃ = 4)
3 2 1 4
P − box₄ (x₄ = 3, l₄ = 3)
3 2 1
P − box₅ (x₅ = 1, l₅ = 2)
2 1

Fig. 8: The example of the second proposed approach after adaptation for uses in WSN with DPLC

1) First, the receiver sorts the packet streams according according to their number of generation NG and the sequence number of packets NP.
2) Second, the DK is generated using the same approach, that was investigated at the emitter side.
3) Third, the destination produces the inverse secret permutation vector ψ^{-1} (or for the different ψ_i^{-1} in case of second approach) by using the following transformation:
$$\psi^{-1}[\psi[j]] = j \tag{7}$$

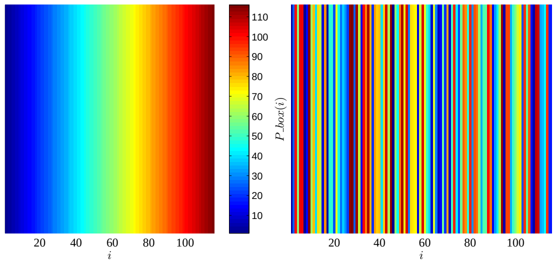
Then, the process of inverse permutation is applied on each encrypted packet contents by using the produced ψ^-1 to recover the original packet content.

IV. Cryptographic Strength and Performance

To demonstrate the efficiency of the proposed approach, security and performance analysis are evaluated in this section using several tests such as: randomness of the proposed permutation layer, key sensitivity and robustness against cryptanalysis attacks.

A. Randomness of the proposed dynamic permutation Layer

The performances of the proposed dynamic permutation scheme are measured in order to demonstrate its safe im-



(a) (b)

Fig. 9: Original and Permuted indexes for a random produce dynamic P-box in a matrix form with $l = 116$

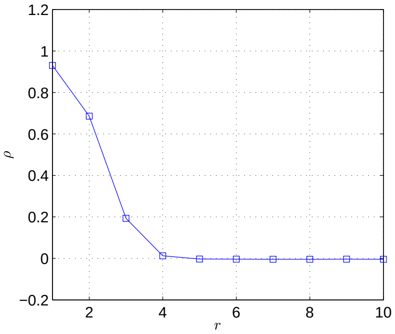


Fig. 10: Variation of the average of ρ of the recurrence of produced P-boxes versus rp for 1000 random dynamic keys.

plementation. In this context, a new metric ”the coefficient correlation ρ” (described in [33]) between the recurrence of permuted vectors $((\psi(t),\ \psi(t+1),\ t = 1,\ 2,\ \ldots,\ l-1\ )$ is tested in order to examine the exact number of iteration rp that needed to obtain a secure permutation. These tests were applied for $nk = 2^{15}$ random dynamic keys. Fig. 10 shows the average of the coefficient correlation between the recurrence of permuted index versus rp for $l_max = 116$ (corresponding to the maximum length of payload in WSN). It is clear that for $rp \geq 4$, the coefficient correlation becomes close to zero (optimal value). For this reason, rp in the proposed scheme is fixed to 4. Additionally, in Fig.12, the average of variation of ρ is shown for the overall dimension of generation h ($h = 1,\ 2, \ldots,\ 32), length packet$l(l=2, 3,..., 116), and $nk = 10000$ between the primary P-box ψ and dynamic ψ_i (produced fromψ as described in the second approach). These results is always close to zero, which indicates that no detectable correlation between the primary and the produced dynamic P-boxes (that produced by performed the left rotation vector on ψ) is existed. Thus, prove the high immunity against eavesdropping attacks, since no useful information can be extracted from the produced dynamic P-boxes.

B. Key Sensitivity

Key Sensitivity refers to a huge change in the ciphertext, responding to a slight change in the keys K. The sensitivity of DK is analyzed for 1000 random dynamic keys, using the percent Hamming distance PH that is calculated between two vectors X and Y of same length l, and described by the following equation:

$$PH = \frac{\sum_{j=1}^{l} Byte2Bin(X_j \oplus Y_j)}{l \times 8} \times 100\%$$

In this case, the sensitivity of DK becomes as bellows:

$$\begin{aligned} KS_w =& \frac{E_{DK_w,\, IV}(M) \oplus E_{DK'_w,\, IV}(M)}{l \times 8} \times 100\% \\ =& \frac{\sum_{j=1}^{l} Byte2bin(C_j^w \oplus C_j^{w'})}{l \times 8} \times 100\% \qquad (8) \end{aligned}$$

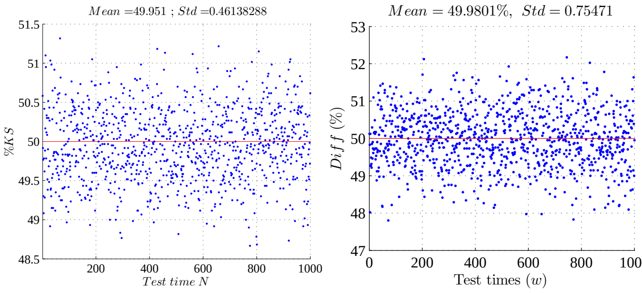
where C^w, $C^{w'}$ are the corresponding cipher packets using DK_w and DK'_w respectively. All the elements of K'_w are equal to those of K_w, except one element, which is the random Least Significant Bit (LSB), that was flipped to show the sensitivity of the scheme with a little change in the key. In Fig. 11-a, the sensitivity of a single LSB modification of the secret key versus 1000 random dynamic keys is shown. It indicates that the proposed cipher has high key sensitivity, since the majority of samples are close to the optimal value in bit level (50%). Additionally, Fig. 11-b shows the percent of hamming distance PH between original and permuted packet. Similarly, it can be seen that the majority of samples are close to the optimal value in bit level (50%). In Fig. 13, the average coefficient correlation between the original and encrypted packets for 10000 different secret permutation layers is shown. These results indicate that no detectable correlation appeared between the original and its corresponding cipher packets, and the coefficient correlation is always close to zero. Therefore, we can consider that the proposed cipher block is strong enough to make the chosen/known plain-text attacks ineffective, while a dynamic key is used for each input packet.

C. Higher Flexibility and lower Complexity and Execution Time

Our proposed scheme has a flexibility with the size of generation h and with the packet length l, and makes the choice of these two parameters dependent on the user requirement. From complexity point of view, The CC of the proposed permutation cipher is $O\ (l)$, and the complexity of the process of generation of P-box is also linear $(O\ (l))$. Noting that, an iteration of un-keyed hash function SHA-512 (with small input block 512 bits) is also required for each input set of packets (h depend of configuration). As results, the proposed approach requires a high level of flexibility and provides the security aspects with a lower complexity.

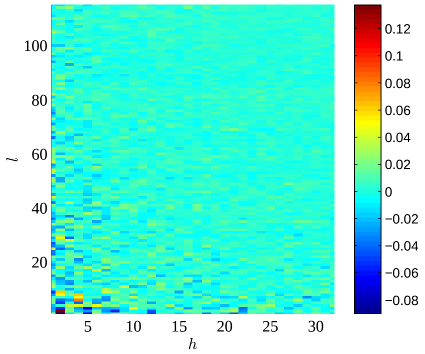
D. Propagation of errors

Additionally, error propagation is an important criterion that is not often considered in the literature, but it is very important for the practical use in any application. Errors occur during



(a) (b)

Fig. 11: The sensibility results for change a random LSB bit of the secret key versus 1000 random keys (a) and its corresponding PH between plain and cipher-packet (b)



(a)

Fig. 12: Variation of the average of ρ between the produced primary P-box and dynamic one versus l and h in a color form for 10000 random dynamic keys.

transmission due to noise and interference produced during the transmission over unreliable channel. But, a strong scheme is that perverse a low propagation of errors. Moreover, a bit error is the substitution of a '0' bit for by '1' bit, or vice versa. The proposed scheme is based on a permutation process that deals with bit error(s). So, errors occurred at a cipher packet, affect the same bit positions of the decrypted packet, and all other positions remains unchangeable. Hence, our proposal is optimal from the error propagation point of view.

V. Cryptanalysis

This discussion is presented in order to demonstrate how powerful the proposed scheme is . First of all, the proposed approach is secure against eavesdropping attacks, due to the use of dynamic property and efficient permutation technique. Moreover, even if we assume that an adversary succeed to recover one generation (this necessities a large computational complexity), all other generations cannot be recovered, since the key is changed dynamically.

Additionally, our proposed approach introduces some delays to the system. This delay depends to the size of h and the length l. Thus, leads to confuse the attacker and protects the system against timing attacks [34].

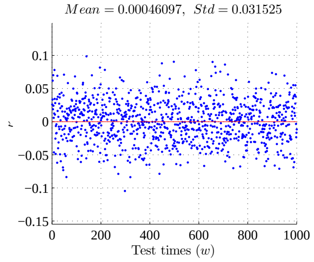


Fig. 13: The variation of the coefficient correlation between the original and encrypted contents packets versus 1000 random dynamic keys respectively, with $l = 116$

In addition, the use of dynamic permutation layer provides a strong resistance to power consumption attacks [35], since different keys are used, which in turn randomize the power consumption.

Furthermore, all the packet contents are permuted via a dynamic secret permutation layer ψ for the first approach, at the source node before any transmission. However, intermediate nodes have no knowledge about the used dynamic key. Hence, they are not able to reconstruct the original packet. Adding to that, the second approach uses different P-boxes which ensures more security, since each permuted packet has its own P-box.

One important issue also is that, the proposed cipher changes the correlation characteristics of the original packets to random packets as in Fig. 13. This is translated to a zero correlation exists between the original and its corresponding cipher packets. Hence, the proposed approach is immune against statistical attacks.

Additionally, the key space of the master key in our scheme is 2^{128}. This is sufficiently large to make the brute-force attack unfeasible. Besides, the sensitivity of the master and dynamic keys are proved since the proposed scheme is based on the cryptographic keyed hash function $SHA-512$.

As results, the proposed approach is secure against the most known forms of attacks such as statistical, differential, chosen/known-plain-text attacks, and brute force attacks.

VI. Conclusion and Perspectives

Security in WSN is a principal requirement for safe end-to-end communication. The existing traditional schemes using cryptographic algorithms that cannot achieve a lower computational complexity and a lower energy consumption whilst ensuring a high security level. For this reason, a new HDCA has been defined and realized to ensure a safe data aggregation while providing less complexity and low energy consumption. To demonstrate the robustness of the proposed scheme, security analysis tests have been analyzed and discussed. Moreover, three approaches are derived from the proposed scheme. Two of them deal with fixed length of packets. And the third one is based on the DPLC scheme. After that, an adaption technique was presented to permit the use of these approaches with

DPLC in the WSN applications. On the other side, simulation results prove the randomness degree of proposed permutation layer, and its key sensitivity as well as its good cryptographic strength against different traditional and physical attacks. These results indicate a significant improvement compared to existing approaches. Indeed, the proposed scheme can be well deployed in WSN, due to its high security and lower computational complexity.

Acknowledgments

This work was partially funded by the French National Research Agency (ANR) as part of the program Digital Engineering and Security (INS-2013), under grant agreement ANR-13-INSE-0006-01.

References

[1] C. Evans-Pughe, "Bzzzz zzz [ZigBee wireless standard]," *IEE Review*, vol. 49, no. 3, pp. 28–31, 2003.

[2] S. Raza, A. Slabbert, T. Voigt, and K. Landernäs, "Security considerations for the wireless hart protocol," in *Proceedings of the 14th IEEE international conference on Emerging technologies & factory automation*, ser. ETFA'09. Piscataway, NJ, USA: IEEE Press, 2009, pp. 242–249.

[3] Y. Huang, "Research of efficient security scheme in wireless network," in *Proceedings of the 9th International Symposium on Linear Drives for Industry Applications, Volume 4*, ser. Lecture Notes in Electrical Engineering, X. Liu and Y. Ye, Eds. Springer Berlin Heidelberg, 2014, vol. 273, pp. 717–724.

[4] T. Karygiannis and L. Owens, "Wireless network security," *NIST special publication*, vol. 800, p. 48, 2002.

[5] A. Perrig, R. Szewczyk, J. D. Tygar, V. Wen, and D. E. Culler, "Spins: security protocols for sensor networks," *Wirel. Netw.*, vol. 8, no. 5, pp. 521–534, Sep. 2002.

[6] C. Karlof, N. Sastry, and D. Wagner, "Tinysec: a link layer security architecture for wireless sensor networks," in *Proceedings of the 2nd international conference on Embedded networked sensor systems*, ser. SenSys '04. New York, NY, USA: ACM, 2004, pp. 162–175.

[7] M. Luk, G. Mezzour, A. Perrig, and V. Gligor, "MiniSec: a secure sensor network communication architecture," in *IPSN '07: Proceedings of the 6th international conference on Information processing in sensor networks*. New York, NY, USA: ACM Press, 2007, pp. 479–488.

[8] L. Batina, N. Mentens, K. Sakiyama, B. Preneel, and I. Verbauwhede, "Low-cost elliptic curve cryptography for wireless sensor networks," in *Security and Privacy in Ad-Hoc and Sensor Networks*. Springer, 2006, pp. 6–17.

[9] H. Wang and Q. Li, "Efficient implementation of public key cryptosystems on mote sensors (short paper)," in *Information and communications security*. Springer, 2006, pp. 519–528.

[10] A. Liu and P. Ning, "Tinyecc: A configurable library for elliptic curve cryptography in wireless sensor networks," in *Information Processing in Sensor Networks, 2008. IPSN'08. International Conference on*. IEEE, 2008, pp. 245–256.

[11] N. Fournel, M. Minier, and S. Ubéda, "Survey and benchmark of stream ciphers for wireless sensor networks," in *Information Security Theory and Practices. Smart Cards, Mobile and Ubiquitous Computing Systems*. Springer, 2007, pp. 202–214.

[12] D. A. McGrew and J. Viega, "The security and performance of the galois/counter mode (gcm) of operation (full version)."

[13] J. Daemen, J. Daemen, J. Daemen, V. Rijmen, and V. Rijmen, "Aes proposal: Rijndael," 1998.

[14] M. Dworkin, M. Dworkin, P. D. Gallagher, and D. N. S. P. f, "Recommendation for block cipher modes of operation: Methods and techniques," 2001.

[15] H. Lee, K. Lee, and Y. Shin, "Aes implementation and performance evaluation on 8-bit microcontrollers," *CoRR*, vol. abs/0911.0482, 2009.

[16] N. Skipjack, "Kea algorithm specifications," 1998.

[17] R. L. Rivest, "The rc5 encryption algorithm," in *Fast Software Encryption*. Springer, 1995, pp. 86–96.

[18] C. Karlof, N. Sastry, and D. Wagner, "Tinysec: a link layer security architecture for wireless sensor networks," in *Proceedings of the 2nd international conference on Embedded networked sensor systems*. ACM, 2004, pp. 162–175.

[19] T. Li, H. Wu, X. Wang, and F. Bao, "Sensec design," *Institue for InfoComm Research, Tech. Rep. TR-I2R-v1*, vol. 1, 2005.

[20] W. Du, J. Deng, Y. S. Han, P. K. Varshney, J. Katz, and A. Khalili, "A pairwise key predistribution scheme for wireless sensor networks," *ACM Transactions on Information and System Security (TISSEC)*, vol. 8, no. 2, pp. 228–258, 2005.

[21] P. Rogaway, M. Bellare, J. Black, and T. Krovetz, "Ocb: A block-cipher mode of operation for efficient authenticated encryption." ACM Press, 2001, pp. 196–205.

[22] H. Noura, S. Martin, and K. A. Agha, "E3sn - efficient security scheme for sensor networks," in *SECRYPT*, 2013, pp. 615–621.

[23] H. Noura, S. Martin, K. Al Agha, and W. Grote, "Key dependent cipher scheme for sensor networks," in *Ad Hoc Networking Workshop (MED-HOC-NET), 2013 12th Annual Mediterranean*, June 2013, pp. 148–154.

[24] H. Dubois-Ferrière, D. Estrin, and M. Vetterli, "Packet combining in sensor networks," in *Proceedings of the 3rd international conference on Embedded networked sensor systems*. ACM, 2005, pp. 102–115.

[25] M. Vutukuru, H. Balakrishnan, and K. Jamieson, "Cross-layer wireless bit rate adaptation," *ACM SIGCOMM Computer Communication Review*, vol. 39, no. 4, pp. 3–14, 2009.

[26] W. Dong, X. Liu, C. Chen, Y. He, G. Chen, Y. Liu, and J. Bu, "Dplc: Dynamic packet length control in wireless sensor networks," in *INFOCOM, 2010 Proceedings IEEE*. IEEE, 2010, pp. 1–9.

[27] R. B. Lee, Z. Shi, and X. Yang, "Cryptography efficient permutation instructions for fast software," *IEEE Micro*, vol. 21, no. 6, pp. 56–69, 2001.

[28] A. J. Menezes, P. C. Van Oorschot, and S. A. Vanstone, "Applied cryptography."

[29] M. J. Campagna, "Security bounds for the nist codebook-based deterministic random bit generator," 2006, matthew.campagna@pb.com 13453 received 1 Nov 2006. [Online]. Available: http://eprint.iacr.org/2006/379

[30] J.-C. Lin, S.-J. Chen, and Y. H. Hu, "Cycle-efficient lfsr implementation on word-based microarchitecture," *Computers, IEEE Transactions on*, vol. 62, no. 4, pp. 832–838, April 2013.

[31] I. Mironov, "(not so) random shuffles of rc4," in *Advances in Cryptology CRYPTO 2002*, ser. Lecture Notes in Computer Science, M. Yung, Ed. Springer Berlin Heidelberg, 2002, vol. 2442, pp. 304–319.

[32] W. Dong, X. Liu, C. Chen, Y. He, G. Chen, Y. Liu, and J. Bu, "Dplc: Dynamic packet length control in wireless sensor networks," in *INFOCOM, 2010 Proceedings IEEE*, March 2010, pp. 1–9.

[33] "Thirteen Ways to Look at the Correlation Coefficient," *The American Statistician*, vol. 42, no. 1, pp. 59–66, 1988.

[34] F. Koeune, J.-J. Quisquater, and J.-j. Quisquater, "A timing attack against rijndael," 1999.

[35] E. Brier, C. Clavier, and F. Olivier, "Optimal statistical power analysis." *IACR Cryptology ePrint Archive*, vol. 2003, p. 152, 2003.