Noname manuscript No.
(will be inserted by the editor)

Energy-Efficient Secured Data Reduction Technique using Image Difference Function in Wireless Video Sensor Networks

Christian Salim* · **Abdallah Makhoul** ·
Raphaël Couturier

the date of receipt and acceptance should be inserted later

Abstract Wireless sensor networks (WSN) have become the rising stars of technology. Every object in this world tends to be sensorly developped, monitored and controlled. Monitoring an area of interest for security reasons for military applications, catastrophic natural events, ... gives each captured frame a huge importance to be able to achieve this surveillance system. Thus, Wireless Video Sensor Networks (WVSN) represents the leading technology to implement this kind of surveillance systems. A WVSN consists of three different layers: The video-sensor node, the coordinator and the sink. A video sureveillance system can have hundreds or thousands of video-sensor nodes. Hence, several challenges exist in such a densely deployed system. The leading challenge is for sure the energy consumption problem for capturing, processing and transmitting several images on the network, but it is not the only challenge. Data transmitted on the network from several sensor nodes to a coordinator must be secured. Thus, the emergence of the security challenge in WVSN. In this paper, on the sensor-node level, for data reduction, a new algorithm has been proposed. This algorithm adapts the frame rate and reduce the number of images sent from the sensor node to the coordinator. This algorithm is compared to our most recent algorithm in [1]. For the security challenge, the

C. Salim
Femto-st institute, Univ. Bourgogne Franche-Comté, Belfort, France
E-mail: christian.salim@univ-fcomte.fr
* Corresponding Author

A. Makhoul
Femto-st institute, Univ. Bourgogne Franche-Comté, Belfort, France
E-mail: abdallah.makhoul@univ-fcomte.fr

R. Couturier
Femto-st institute, Univ. Bourgogne Franche-Comté, Belfort, France
E-mail: raphael.couturier@univ-fcomte.fr

one-round algorithm from [2] is adapted to our approach and scenario. This approach is validated by experimentation using Cpp for OpenCV on Raspberry Pi 3 and by comparing it to other previous, existing approaches.

Keywords Wireless Video Sensor Networks · Security · Data Reduction · Energy Consumption · Image Difference.

1 Introduction

Numerous changes have impacted the surveillance field in the past decade. Nowadays, to monitor an area of interest and areas where people's interactions are quite difficult, WVSNs are here to serve as a quasi-intelligent system to monitor and detect any abnormality in a specific zone.

The system in wireless video sensor networks WVSN combines the event driven and periodic approaches. The wireless video sensor networks are composed of 3 layers: The Wireless Sensor Node level, The Coordinator level and the Sink. Despite their very limited energy resources, the wireless video sensor nodes are responsible for monitoring a well known area of interest. Thus, they are limited to their FOV (field of view), they only monitor the area by filming it according to their FOV. The sensors send the filmed sections to the coordinator. This process is energy consuming due to the huge number of frames captured and sent by the sensor nodes to the coordinator. WVSN operates periodically if the sensor nodes do not detect any intrusion in the monitored area of interest [1]. Fig 1 shows the architecture of WVSN, where the network can be divided into several areas composed of a certain number of sensor nodes connected to a coordinator, and different coordinators from different areas are connected to the sink.

In this paper, our main challenge is to reduce the energy consumption on the sensor node level especially the energy consumption related to the sensing and transmission processes. Hence, the data security challenge has been taken into account. Our algorithms are implemented on the sensor node, which means that the time execution is very important to be able to have live monitoring.

In the first place, an approach has been proposed to reduce the energy consumption related to the sensing and transmission on the sensor node level using data reduction techniques. The proposed algorithm STAFRA (sensing and transmission adaptive frame rate algorithm) reduce the number of frames sensed and sent by each sensor node.
For the transmission process, a frame is sent to the coordinator only if it represents a difference while comparing it with the last frame sent to the coordinator and it is called a critical frame as in [1]. In this paper, the comparison is done using the norm L2 relative error function while using a predefined threshold. In this case the number of frames sent to the coordinator will be reduced and as

consequence the energy consumption related to transmission is reduced. But this reduction can increase furthermore by reducing the size of those images as follows: if both frames are different, the sensor node decides to send only the different part of the new image to the coordinator (the difference image). This part of the image is to be joined with the last sent image on the coordinator to rebuild the new frame.
On the sensing level, the frame rate is adapted depending on the number of critical frames transmitted from the sensor node to the coordinator in each period. The number of frames sensed by the sensor will be reduced, which leads to a direct reduction of the energy consumption for the sensing process on the sensor node level.

Hence security issues are emerging nowadays in WVSN depending on the type of application. In this approach, a security algorithm is adopted from [2] to secure the data transmitted from the sensor node to the coordinator. The One-round algorithm [2] is efficient considering the low execution time needed to encrypt a frame.

As the results show at the end of this paper, after implementing both algorithms on Rpi3, the time execution ensures that both algorithms can run together on a sensor node for more than 10 images per second. Those results ensure the live monitoring while reducing the energy consumption and encrypting all the sent data.

Our paper is divided into 6 sections, section II introduces the state of the art in this specific domain while section III briefly explains the proposed method. Data Reduction technique is explained in detail in section IV. In section V, the security contribution is discussed to conclude the proposed method. Section VI presents some simulations and experimentations results to validate our approach. At the end, section VII concludes our paper with some future work.

2 Related work

Different techniques have been proposed in the litterature to reduce energy consumption in Wireless Sensor Networks: Data Redundancy techniques [4–10], Data aggregation [8], Backround subtraction [11], Geometrical criteria [12–14], Physical and Network layers approaches [15,16] and Scheduling [4, 17–20]. Data redundancy has been considered in several research work for energy reduction. A GPS module introduction to control the cameras and detect which camera is to be actuated depending on the sensor's position is presented in Akkaya et al. [7]. The overlapping approach has been studied by in Priyadarshini et al. [5] where their work eliminates redundacies by turning off some cameras and activating the optimal number of cameras according to the overlapping FOV's of different cameras. An in-network data aggregation technique at the coordinator level is proposed in [8]. This proposition by Makhoul et al. identifies similar data generated by the nearly duplicate nodes. In order to save energy, some sensors are turned off.

In order to reduce the energy consumption on the sensor node level, Akkaya et al. in [11] adopted the background subtraction (BS) and compression techniques as common data reduction schemes.

Scheduling techniques are one of the most used methods in many previous works [4,17–20]. The authors in [4] divided the region into several clusters using a clustering methodology. In each cluster, to avoid data redundancy for all overlapping cameras, a scheduling approach has been adopted in their method. Authors In [17] divided the region according to the different risk levels of the sensor nodes to form several areas of interest. Each area has its own adaptive scheduling model. This model changes the capture speed of the node based on its risk level and environment.

Several studies tried to solve this issue by proposing physical and network layers solutions [15,16]. In [15] a CMOS image sensor was proposed to generate two outputs, in order to differentiate between the normal image with a normal frame rate of 30 fps and the images of moving objects with an adaptable frame rate of 960 fps and over. They reconstuct the image from both outputs. This construction shows the details in stationary objects and the suppressed motion in moving objects. Frame rate is higher in the hottest region where it matters the most to detect and track any event.

In [12–14], some geometrical criterias are taken into consideration. In [12] the cover set concept and the behavior functions modeled by quadratic Bezier curves are used to help a node to find its redundancy level and to adapt the frame capture speed of video node which is related to its assigned criticality depending on its position on the network and its redundancy level. In this approach the nodes on the borders detect the intrusion in the first place, that is why a higher criticality is assigned to those node in comparison with interior nodes with lower criticality. A scheduling algorithm is proposed to control the activity of sensor nodes according to the redundancy level and criticality of each node.

Some other works prefer to do all the processing on a cloud server or multiple cloud servers [21], [22]. In those approaches the security topic is also taken into consideration and the processing is very efficient since it is done on cloud servers. Those algorithms are foreground extraction algorithms on data that are encrypted by the coordinator of the video surveillance network and sent to the cloud server to do the processing.

Unfortunately, these studies in WMSN make all the analysis on the coordinator level or on cloud servers, disregarding what can be done on the video-sensor level concerning the reduction in terms of energy and bandwidth consumption starting from the very first layer.

This paper also focuses on the security challenge. Hence, a lot of previous encryption standards and algorithms are present in the literature: The asymmetric Encryption algorithms such as Elgamal [23] and Diffie-Hellman [24]. This kind of encryption is known to guarantee that the person who is receiving the public key is the person who was supposed to receive it, and so it is safe to let him/her receive the encrypted information. The symmetric encryption such as: Data Encryption Standard (DES)[25,26], in those works the authors proposed algorithms to enhance the quality of the images based on a chaotic map where the DES block cipher is installed to increase the key space. As mentioned in [27], the huge amount of multimedia data transceived by all the modern applications can not be supported by the DES implementation. Thus, in [28] an AES algorithm is defined to encrypt images after performing some changes on the key generation or other components. In [27] the authors modified the AES algorithm proposed in [28] in order to improve the performance in securing images. The AES encryption technique has also its disadvantages: it requires a high number of rounds which is not feasible or efficient for tiny limited sensor nodes. Thus, the one round algorithm technique proposed in [2] and adopted in our work is a simple algorithm that requires less execution time than AES and less rounds.

In this paper, a method that detects the critical frames and send them to the coordinator is proposed. The frame rate of the video-sensors is adapted. Our approach for the sensing and transmission part on the sensor node level is inspired from [1] and [29]. In [1], the authors studied how to send only the critical vital signs to the coordinator by introducing LED algorithm. In [29], the authors proposed the ASA algorithm which consists of changing the sampling rate after several consecutive numbers of critical values in consecutive periods. Then, to add security to the data sent to the coordinator, the one-round algorithm has been adopted from [2]. In the next section, the architecture of WVSN is briefly discussed. The proposed approach is explained in the following sections.

3 Architecture

WVSN as mentioned before, is divided into three main layers: The wireless video sensor nodes, the coordinator and the sink as shown in figure 1. Each sensor node captures the required data, in the wireless video sensor network, the frames in a video sequence is the data sensed by the sensor node. Then the sensor node transmits the data to the coordinator responsible for the area of interest. The coordinator gathers all the data from all the sensors in its area and sends it to the sink so that the team which is in charge of this field analyze it.

In a simple WSN, no algorithms are set on any level. Thus, the huge number of frames captured by several sensors in each area of interest increases the energy consumption on every sensor node especially that they have limited energy resources. By sending 15 frames per second, for a tiny sensor, this process can damage its battery quickly.

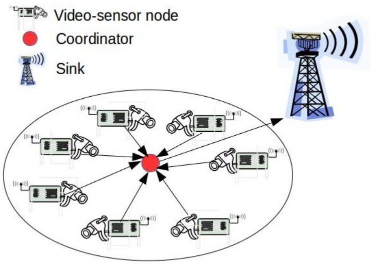

Fig. 1 Architecture of WVSN

In this paper, the idea of reducing the energy consumption on the sensor-node level and the overall network is developped in its two phases: the sensing phase and the transmission phase. Then the security model for the transmitted images from the sensor-nodes to the coordinator is discussed.

4 Data Reduction and Energy Consumption

In WSN, sensor-nodes operate periodically, and send a huge number of packets to the coordinator. This scenario causes the presence of the energy consumption challenge which is the most important challenge in WSN in general. More specifically this challenge is present in WVSN because images are multimedia data of greater size than simple numerical data and the video-sensor nodes have limited energy ressources.

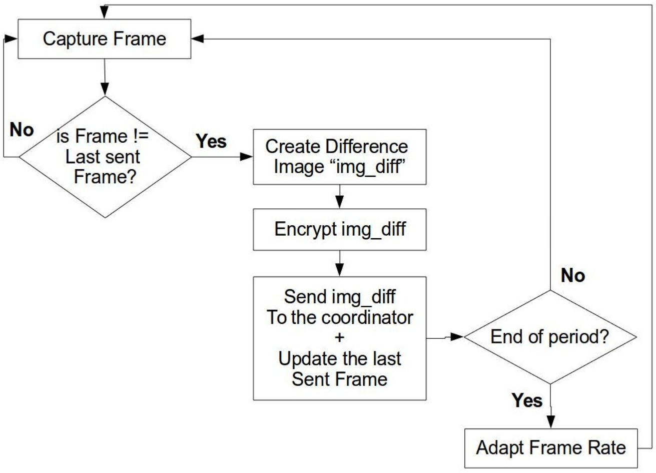
Capture Frame
No
is Frame != Last sent Frame?
Yes
Create Difference Image "img_diff"
Encrypt img_diff
Send img_diff To the coordinator + Update the last Sent Frame
No
End of period?
Yes
Adapt Frame Rate

Fig. 2 Sensor node behavior

Data reduction is one of the methods to overcome this challenge. In this approach, data reduction is adopted for the sensing phase and the transmission phase on the sensor-node level. This process has a functionality to reduce the huge number of raw images sensed from the sensors, and the number of images sent by the sensors to the coordinator. The diagram in Figure 2 summarizes the behavior of our approach on the sensor node level including the security aspect.

4.1 Sensing and Transmission Phases

On the video-sensor node level, an daptation of the $MASRA$ algorithm proposed in [1] has been suggested. This adaptation replaces the color-edge similarity method to compare two consecutive frames in $MASRA$ with a norm simple euclidean distance similarity method to reduce the energy consumption related to transmission using the norm L2 relative error function in C++ in OpenCV. To apply this function, each image is transformed to a matrix. The frame rate adaptation technique is used to reduce the number of sensed frames on the sensing level. As shown in STAFRA (sensing and transmission adaptive frame rate algorithm) algorithm 1, the role of the similarity pattern is to detect any difference in two consecutive images sensed by the sensor-node by using a norm similarity function. If the difference between those images does not surpass a certain threshold of similarity sim, the sensor-node creates a new image called img_diff of the same size that represents the difference between both images. To be able to create this img_diff, the absolute images difference function $absdiff(MATA, MATB)$ is adopted. This function is a simple operation that takes the two matrix of the compared images as parameters. It computes the absolute value of the difference for each pixel, for each channel. A difference image is generated throughout this function as shown in Figures 3,4,5 where figure 5 is the difference image of the first two frames. As we can see, the shadow of the moving person and the person are the only differences taken into account. The size of this new image is smaller than a full image, since it only includes the difference and not a complete image. The sent image is called critical frame in the remainder of this paper because it means that an event is happening in the area of interest.

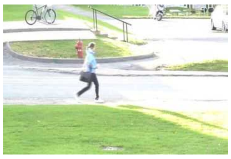
Fig. 3 The First Frame

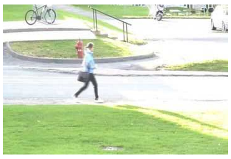
Fig. 4 The Second Frame

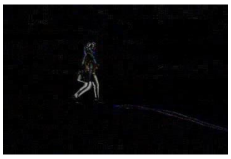
Fig. 5 The Difference Frame

Hence, in our approach the number of critical frames in each period affects the frame rate of the sensor-node for the next period. If in a given period i, the number of critical frames cr_{nb_i} exceeds one of the two predefined threshold th_{up} or th_{down} the frame rate changes according to the number of critical frames in this period. Both thresholds as shown in algorithm 1 are generated based on a parameter d that represents the minimum detectable change (In MASRA algorithm it was set to be adapted after several periods of change and not after 1 period). In this case, the frame rate of the next period $i+1$ is calculated as mentioned below:

$$FR = 2 \times nb_{cr_i} \tag{1}$$

Algorithm 1 Sensing and Transmission Adaptive Frame Rate Algorithm *STAFRA*

```
Store the first period's critical values in $nb_{cr}$
Set $FR = 2 \times nb_{cr}$
Set $d$ the parameter that represents the minimum detectable change
Set $th_{up} = nb_{cr} \times (1 + d/2)$
Set $th_{down} = nb_{cr} \times (1 - d/2)$
Set $sim$ the maximum similarity needed to send the next frame
Set $norm\_sim$ distance similarity between two frames
while $Energy > 0$ do
    for each period $i$ do
        Take first frame $kf_0$
        Send first frame $kf_0$
        Take frame $kf_i$ at $R_t$ Rate
        Compare $kf_i$ to the latest sent frame
        Generate $norm\_sim$ as the dist similarity between the two frames.
        if $norm\_sim < sim$ then
            Generate frame the $img\_diff$ between the 2 frames
            Run One-round algorithm for $img\_diff$
            Send encrypted $img\_diff$ to the coordinator
            $nb_{cr_i}$++
        end if
        $i$++
    end for
    $nb_{cr_i}$=number of critical frames in this period
    if $nb_{cr_i} > th_{up}$ OR $nb_{cr_i} < th_{down}$ then
        Set $nb_{cr} = nb_{cr_i}$
        Set $FR = 2 \times nb_{cr}$
        Set $th_{up} = nb_{cr} \times (1 + d/2)$
        Set $th_{down} = nb_{cr} \times (1 - d/2)$
    end if
end while
```

The frame rate in the STAFRA Algorithm varies according to the criticality of the events happening in the area of interest. If no critical frames are detected in a period, the sensor node senses the first frame of every period and sends it to the coordinator as the only frame of the actual period. The period in our approach is equal to 1 second, and the initial maximal frame rate is 30 frames per second. In a non critical scenario the sensor node only captures the first frame of every period and sends it to the coordinator, neglecting the other 29 frames. Thus, this method can reduce the number of frames captured by every sensor node, and also the number of frames sent to the coordinator. This data reduction helps to reduce the energy consumption on the sensor node level by a significant percentage presented in our experiments.

5 Data Security

Securing the images sent in a WVSN for surveillance can not be negligible. In the proposed scenario, a simple efficient and quick algorithm is needed to do the encryption. One-round algorithm is a simple cipher scheme [2], it is based on simple operations (XOR). In this algorithm, the keys are dynamically produced, based on a dynamic key that changes according to the session or the input image. As several scientists affirm that confusion and diffusion must be preserved in any encryption algorithm, the one-round algorithm guarantees the confusion and diffusion since 2 substitution boxes are used. One of the most encouraging advantages of this algorithm is that it can be adapted to simple limited devices such as Raspberry Pi, or sensors in wireless video sensor networks. In the following the encryption algorithm is described.

5.1 Encryption Algorithm

After reducing the number and size of the data sent from the sensor nodes to the coordinator, securing the data is one of the needs in WVSNs. Thus, an energy efficient encryption algorithm must be implemented on the sensor node level. The one-round algorithm is symmetric and is based on a secret key SK shared between the sender and the receiver. As stated in [2], this key is employed with a *Nonce* to produce a dynamic key. This dynamic key is split to obtain four sub-keys that will be used to build the primitives of the encryption/decryption processes. This cipher is based on only one round since a dynamic key with a large size is used. In the encryption process, an input image of size $C \times R \times P$ is divided into α sub-matrices x_1 , x_2 , . . . , x_α having a square size equal to $h \times h$ bytes each. If the number of bytes of an image is not a multiple of h^2 , a padding operation is performed to adjust the size of the last sub-matrix (x_α). In addition, h can be equal to 4, 8, 16 or 32. On the other hand, the sub-matrices number α is obtained as follows:

$$\alpha = \frac{R \times C \times P}{h^2} \tag{2}$$

In this paper, the size of the blocks is set to 4 to have better security noting that it was 8 in [2]. As we stated earlier h can be equal to 4, 8, 16 or 32, so the One-round algorithm is flexible and depends on the needs of the application. If h is equal to 4 than we have the most demanding scenario in terms of execution time and energy consumption but we will get the best security level. After several experiments we were able to perform STAFRA and One-round algorithms together on more than 15 frames per second if h is equal to 4. In this case, the algorithms run quickly while guaranteeing data reduction and a good level of security. The sub-matrix selection, function f, function g, the switch operation as well as an illustration of the encryption and decryption algorithms are all used as mentioned and explained in [2].

As mentioned before, this algorithm presents a good security result with very low execution times. Algorithm 2, for encryption purposes is implemented on the sensor node's level and algorithm 3 for decryption is implemented on the coordinator's level. This work focuses more on the sensor node level behavior because it is the level where the energy consumption is the most critical. Thus, in the experimentations and simulations, the energy consumption on the sensor node level is studied based on the complexity and the time of execution of each algorithm. That is why, the decryption algorithm can be said to be disregarded in the experimentations.

Algorithm 2 One Round Encryption Algorithm.

```
START One_Round_Encryption($X$)
for $i = 1$ to $\alpha$ do
    $x_i = X[i]$
    $y_i = X[\pi[i]]$
    $cx_i = S_2(S_1(x_i) \oplus RM_1 \oplus y_i)$
    $cy_i = S_1(S_2(y_i) \oplus RM_1 \oplus RM_2)$
    $X[i] = cx_i$
    $X[\pi[i]] = cy_i$
end for
END One_Round_Encryption($X$)
```

Algorithm 3 One round decryption Algorithm

```
START One_Round_Decryption($X$)
for $i = 1$ to $\alpha$ do
    $cx_i = X[i]$
    $cy_i = X[\pi[i]]$
    $y_i = S_2^{-1}(S_1^{-1}(cy_i) \oplus RM_1 \oplus RM_2)$
    $X[i] = S_1^{-1}(S_2^{-1}(cx_i) \oplus RM_1 \oplus y_i)$
    $X[\pi[i]] = y_i$
end for
END One_Round_Decryption($X$)
```

6 Experimental Results

In this section we present the simulations used to validate our technique. This part is divided into two subsections:

- Data Reduction and Energy Consumption.
- Data Security for Transmission.

In the first part, the experimentations check the data reduction based for the sensing phase on the sensor node level by adapting the frame rate according to the technique mentioned above. Then, it checks the data reduction in terms of size of the data for the transmission phase, by sending only the difference between the images. And at the end it computes the total reduction of energy consumption if the STAFRA algorithm is adopted while comparing it to the MASRA algorithm proposed in [1]
In the latter, as in [2], a one-round algorithm is tested first on big images (800 KB images) to check the validity of the approach. Then it is tested on the sent images from the sensor-node (Raspberry Pi) to the coordinator/server (laptop). Those sensed and transmitted images are of 320 x 240 pixels on RGB and compressed to jpeg images as per STAFRA algorithm before starting the security algorithm process.

For this purpose, both algorithms presented in this paper have been tested using Cpp for OpenCV on Raspberry Pi 3. A nano camera is installed on the Raspberry Pi to monitor the area of interest. The Raspberry Pi serves as the sensor node in our network, it is wirelessly connected to an octa core i7 16 GB RAM laptop that has the coordinator's functionalities. The network in this paper is a client server network (The Raspberry Pi as a client and the laptop is the server where the images are stored). This network is described in figure 6, where the sensor-node is wirelessly connected to the coordinator.

In the experimentations, the initial and maximum frame rate is set to 10 frames per second for the sensor-node. The minimum FR (frame rate) in this work is 2 frames per period. A period is equal to 2 seconds which means 20 frames exist in every period. If no critical event is happening in the area of interest, the frame rate is set to its minimum, sensing 2 frames per period. The frame rate varies according to the number of critical frames (sent frames) in every period. The sensor-node sends the first frame of each period to the coordinator. All the other sensed frames in the same period are compared to this frame (or the last sent frame). If those compared frames are not similar, the new frame is sent to the coordinator. In this method, the different part of this new frame is sent and not the full image. Note that every sent frame is encrypted using one-round algorithm [2]. Both algorithms are run for 60 seconds (30 periods).

6.1 Data Reduction and Energy Consumption

The reduction of the energy consumption on the sensor node level can be done via several techniques, one of these techniques is data reduction on the

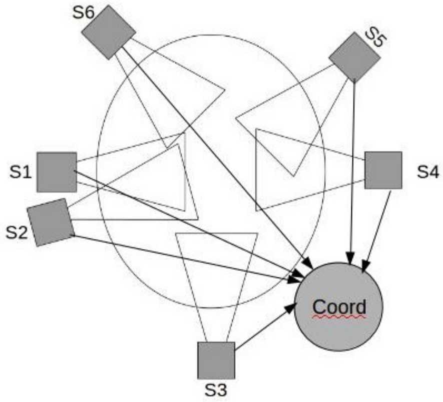

Fig. 6 Experimental Network

sensing phase and on the transmission phase. Each sensor-node in a WVSN operates periodically and sends all the data sensed to the coordinator. The key to reducing the frames transmitted from the sensor to the coordinator is to send only the different frames sensed by the sensor node in each period.

6.1.1 Critical Frames

The critical frames are the frames that are different from the first frame in each period. To be able to specify those frames, the L2 norm similarity in $STAFRA$ algorithm compares the consecutive sensed images. The first sent image in the period is called the "background image" to which all the other images are compared to. The images that are sent to the coordinator are only the images that are different from this background image. In this approach, the algorithm sends the different parts of the image comparing with the background image using the absolute difference function. Instead of sending a raw image of $320 \times 240 \times 3$ which means 230 KB, this method compresses the image into a jpeg image of 6 KB to be sent to the coordinator, and 4 KB if only the difference is sent. Tables 1 and 2 shows a comparison between sending a raw image and a jpeg image depending on the execution time of every operation on the sensor node. In Table 1: "sim" is the execution time of the similarity process, "compress" is the execution time for compression, "difference" represents the execution time to create the difference image and "send" is the time needed to transmit the image to the coordinator.

Table 1 Execution Time Comparison per Event

Type	Size	Sim	Compress	Difference	Send
Raw	230 KB	1 ms	0	0	1000 ms
JPEG	6 KB	0.7 ms	0.02 ms	0	26 ms
JPEG +DIFF	4 KB	0.7 ms	0.02 ms	4 ms	17 ms

Table 2 Total Execution Time Comparison

Img Type	Total Execution Time
Raw	1001 ms
JPEG	27 ms
JPEG +DIFF	22 ms

6.1.2 Frame Rate Adaptation

Different scenarios have been taken into consideration in the experimentations. The frame rate varies according to the number of sent data in the last period.

For the sensing phase, the frame rate adaptation serves to reduce the number of frames sensed per period depending on the number of critical frames sent in the previous period.

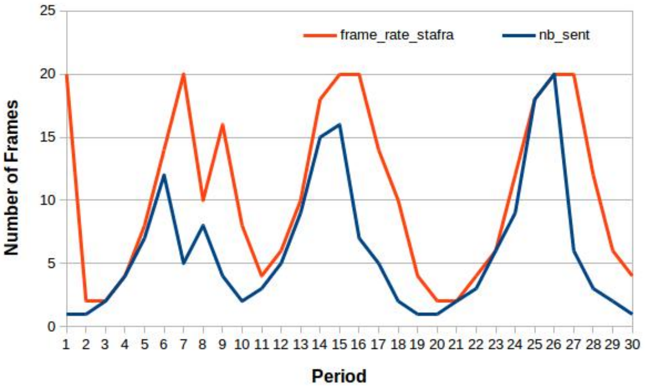

Fig. 7 Frame Rate Adaptation

Figure 7 shows the adaptation of the frame rate on the sensing phase depending on the criticality of the event in the monitored area. This adaptation causes the reduction of the number of frames sensed by the sensor-node as shown in table 3. A data reduction of 50% is reached by adapting the Frane Rate, and another 25% are added when applying the critical frames method.

Table 3 Frame Rate Adaptation Data Reduction over 60 seconds

ALL	Sensed Frames	Critical Frames
600	300	170

6.1.3 Comparison

This approach is compared to several other methods on the sensor node level regarding the execution time and the frame rate adaptation. For the execution time and accuracy of the similarity, this method is compared to the $MASRA$ algorithm in [1] where the colour and edge similarities were both present to detect the difference between images. The difference between $STAFRA$ and $MASRA$ algorithms for the frame rate adaptation has an influence on the number of critical frames sent per period as shown in Figures 8 and 9.

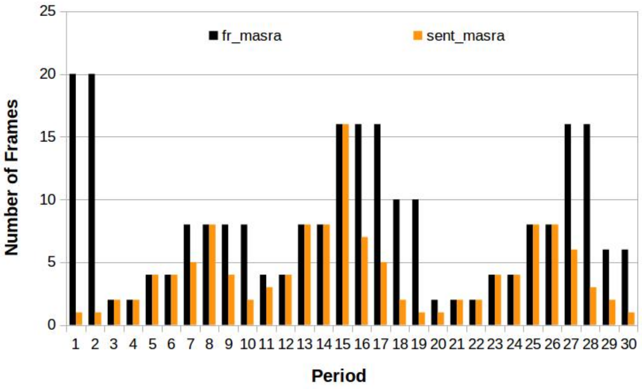

Fig. 8 MASRA Frame Rate Adaptation and Number of Sent Frames

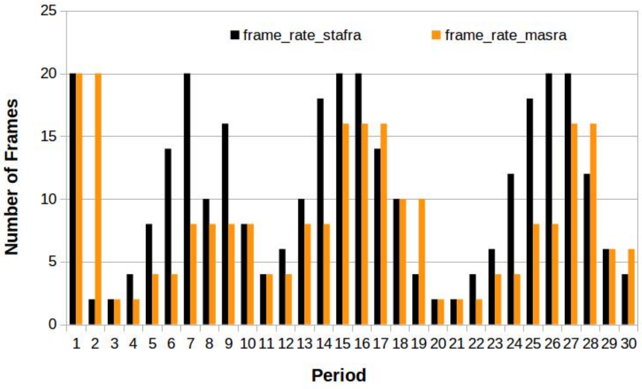

Fig. 9 Frame Rate Adaptation Comparison

The frame rate adaptation in the $MASRA$ algorithm changes after at least two periods of intrusion detection. For this reason, some needed frames can not be captured because the frame rate is not adapted on time. It should be added that the frame rate decreases once the intrusion leaves the area.

Those two figures show the superiority of the $STAFRA$ algorithm to change the frame rate earlier than $MASRA$. Thus, $STAFRA$ has less errors while detecting and tracking the intrusion, and it resets the sensor-node to its idle mode with a FR= minimum frame rate earlier than $MASRA$. This process captures less frames and save energy while increasing the quality of the surveillance.

A comparison of the execution time for several approaches on the sensor node level. This comparison takes into consideration the similarity, the compression, the transmission as shown in tables 4 and 5 where all the execution times are in ms. Edge similarity, color-edge similarity and Norm similarity are compared in those tables. Note that images sent using the MASRA algorithm are RAW images, but the compression of those images into jpeg images is also taken into consideration. In Table 4: "sim" is the execution time of the similarity process, "compr" is the execution time for compression, "Diff" represents the execution time to create the difference image and "send" is the time needed to transmit the image to the coordinator.

Table 4 Execution Time Comparison per Method per Function

Method	Type	Size	Sim	Compr	Diff	Send
Color-Edge	Raw	230 KB	5	0	0	1000
Edge	Raw	230 KB	3	0	0	1000
Norm	Raw	230 KB	1	0	0	1000
Color-Edge	JPEG	6 KB	4.2	0	0	26
Edge	JPEG	6 KB	2.7	0	0	26
Norm	JPEG	6 KB	0.7	0	0	26
Norm	JPEG+DIFF	4 KB	0.7	0	0.3	17

Table 5 Total Execution Time Comparison

Method	Img Type	Total Execution Time
Color-Edge	Raw	1005 ms
Edge	Raw	1003 ms
Norm	Raw	1001 ms
Color-Edge	JPEG	30 ms
Edge	JPEG	29 ms
Norm	JPEG	26 ms
Norm	JPEG+DIFF	18 ms

Tables 4 and 5 show the superiority of $STAFRA$ algorithm and the norm similarity method over $MASRA$ algorithm using the edge or the color-edge similarities. The execution time proves a gain of at least 30% when implementing *STAFRA* algorithm.

6.2 Data Security for Transmission

As discussed in the paper, securizing the data transmitted on the network is one of the important issues in WMSN. To secure the frames on the sensor node level, the one round algorithm is implemented. In the table below, the difference of the execution time of this algorithm is presented with different image types.

Table 6 One Round Algorithm Execution Time

Method	Img Type	Execution Time
One_round	Raw	500 ms
One_round	JPEG	15 ms
One_round	JPEG+DIFF	10 ms

As shown above in table 6, the execution time for the One-Round algorithm for the difference image sent from the sensor node to the coordinator, costs 10 ms. By adding the 18 ms needed for all the functions mentioned in the section above, 28 ms are needed to compute and send the image from the sensor node to the coordinator. Refering to table 5, this execution time remains better than execution times of other approaches without applying the security algorithm to enhance the security on the network.

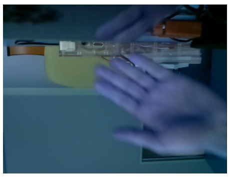

Fig. 10 The Original Frame

Fig. 11 The Encrypted Frame

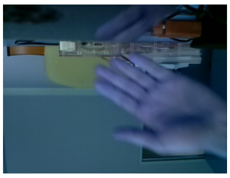

Fig. 12 The Decrypted Frame

Figures 10,11,12 show the validity of the security algorithm and how the frame can be retreived on the coordinator using the decryption algorithm.

7 Conclusion

In this paper, a new data reduction adaptive frame rate algorithm *STAFRA* is presented to adapt the frame rate of each sensor node according to the event happening in the area of interest. This adaptation leads to reduce the number of sensed frames on the sensor node level. Thus, it reduces the energy consumption needed for the sensing process. The data reduction algorithm adds a comparison between frames with the last frame sent, if both images are similar, the second one is not sent to the coordinator. In case the second image is different, the difference between the two images is sent to the coordinator and not the whole image. The difference image is 30% smaller than the original image. This functionality reduces the energy consumption for the transmission process on the sensor node level by reducing the number and the size of the images sent to the coordinator.

As for the security manner, our algorithm ensures the security of the sent data from the sensor node to the coordinator, while maintaining a low execution time and low energy consumption on the sensor node level. For future work, an algorithm on the coordinator level must be done to rebuild each new image. It needs to combine the last sent image with the difference image.

Acknowledgement

This work has been supported by the EIPHI Graduate School (contract "ANR-17-EURE-0002").

References

1. C. Salim, A. Makhoul, R. Darazi, and R. Couturier. Combining frame rate adaptation and similarity detection for video sensor nodes in wireless multimedia sensor networks. *IWCMC*, pages 327 – 332, 2016.
2. Hassan Noura, Ali Chehab, Lama Sleem, Mohamad Noura, Raphaël Couturier, and Mohammad M. Mansour. One round cipher algorithm for multimedia iot devices. *Multimedia Tools and Applications*, Jan 2018.
3. Stanislava Soro and Wendi Heinzelman. A survey of visual sensor networks. *Advances in Multimedia*, 2009:21, 2009.
4. Mohammad Alaei and Jose M. Barcelo-Ordinas. A method for clustering and cooperation in wireless multimedia sensor networks. *Sensors*, 10(1):3145–3169, 2010.
5. Debapriya Soumyesh Das Sushree Bibhuprada B. Priyadarshini, Biswa Mohan Acharya. Redundant data elimination and optimum camera actuation in wireless multimedia sensor network (wmsn). *IJERT*, 2(6), 2013.
6. Wusheng Luo, Qin Lu, and Qin Xiao. Distributed collaborative camera actuation scheme based on sensing-region management forwirelessmultimedia sensor networks. *Distributed Sensor Networks*, 12(0):1–14, 2012.
7. Andrew Newell and Kemal Akkaya. Distributed collaborative camera actuation for redundant data elimination in wireless multimedia sensor networks. *Ad Hoc Networks*, 45(4):514–527, 2011.
8. Jacques M. Bahi, Abdallah Makhoul, and Maguy Medlej. An optimized in-network aggregation scheme for data collection in periodic sensor networks. *ADHOC-NOW*, 11(0):153–166, 2014.
9. Abdallah Makhoul, Hassan Harb, and David Laiymani. Residual energy-based adaptive data collection approach for periodic sensor networks. *Ad Hoc Networks*, 35:149–160, 2015.

10. Abdallah Makhoul, David Laiymani, Hassan Harb, and Jacques M. Bahi. An adaptive scheme for data collection and aggregation in periodic sensor networks. *IJSNet*, 18(1/2):62–74, 2015.
11. Pinar Sarisaray-Boluk and Kemal Akkaya. Performance comparison of data reduction techniques for wireless multimedia sensor network applications. *Hindawi Publishing Corporation*, 15(0):1–15, 2015.
12. Ali Benzerbadj and Bouabdellah Kechar. Redundancy and criticality based scheduling in wireless video sensor networks for monitoring critical areas. *Procedia Computer Science*, 21(0):234–241, 2013.
13. Salima Benbernou, Abdallah Makhoul, Mohand-Said Hacid, and Ahmed Mostefaoui. A spatio-temporal adaptation model for multimedia presentations. *ISM*, pages 143–150, 2005.
14. Jacques M. Bahi, Abdallah Makhoul, and Maguy Medlej. A two tiers data aggregation scheme for periodic sensor networks. *Ad Hoc and Sensor Wireless Networks*, 21(1/2):77–100, 2014.
15. Jaehyuk Choi, Sang-Wook Han, Seong-Jin Kim, Sun-Il Chang, and Euisik Yoon. A spatial-temporal multiresolution cmos image sensor with adaptive frame rates for tracking the moving objects in region-of-interest and suppressing motion blur. *IEEE JOURNAL OF SOLID-STATE CIRCUITS*, 42(12):1–12, 2007.
16. Richard Stewart, Keith Trahan, David Chesavage, Sean Casey, Michael Rome, and Chris Kokinakes. Surveillance system and method with adaptive frame rate. *Patent Application Publication*, 21(0):234–241, 2003.
17. CongDuc Pham, Abdallah Makhoul, and Rachid Saadi. Risk-based adaptive scheduling in randomly deployed video sensor networks for critical surveillance applications. *J. Network and Computer Applications*, 34(2):783–795, 2011.
18. Mohammad Alaei and Jose M. Barcelo-Ordinas. A method for clustering and cooperation in wireless multimedia sensor networks. *Patent Application Publication*, 10(0):3145–3169, 2010.
19. Zhenquan Qin, Lei Wang, Can Ma, Jiaqi Xu, and Bingxian Lu. An overlapping clustering approach for routing in wireless sensor networks. *International Journal of Distributed Sensor Networks*, 2013(0):1–11, 2013.
20. Yingwei Yao and Georgios B. Giannakis. Energy-efficient scheduling for wireless sensor networks. *IEEE TRANSACTIONS ON COMMUNICATIONS*, 53(8):1–10, 2005.
21. Xin Jin, Kui Guo, Chenggen Song, Xiaodong Li, Geng Zhao, Jing Luo, Yuzhen Li, Yingya Chen, Yan Liu, and Huaichao Wang. Private video foreground extraction through chaotic mapping based encryption in the cloud. In Qi Tian, Nicu Sebe, Guo-Jun Qi, Benoit Huet, Richang Hong, and Xueliang Liu, editors, *MultiMedia Modeling*, pages 562–573, Cham, 2016. Springer International Publishing.
22. X. Jin, Y. Wu, X. Li, Y. Li, G. Zhao, and K. Guo. Ppvibe: Privacy preserving background extractor via secret sharing in multiple cloud servers. In *2016 8th International Conference on Wireless Communications Signal Processing (WCSP)*, pages 1–5, Oct 2016.
23. T. Elgamal. A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Transactions on Information Theory*, 31(4):469–472, Jul 1985.
24. W. Diffie and M. Hellman. New directions in cryptography. *IEEE Trans. Inf. Theor.*, 22(6):644–654, September 2006.
25. Qian Gong-bin, Jiang Qing-feng, and Qiu Shui-sheng. A new image encryption scheme based on des algorithm and chua's circuit. In *2009 IEEE International Workshop on Imaging Systems and Techniques*, pages 168–172, May 2009.
26. Ludger Hemme. A differential fault attack against early rounds of (triple-)des. In Marc Joye and Jean-Jacques Quisquater, editors, *Cryptographic Hardware and Embedded Systems - CHES 2004*, pages 254–267. Springer Berlin Heidelberg, 2004.
27. Medien Zeghid, Mohsen Machhout, Lazhar Khriji, Adel Baganne, and Rached Tourki. A modified aes based algorithm for image encryption. *International Journal of Advanced Trends in Computer Science and Engineering*, 21, 01 2008.
28. J. Daemen and V. Rijmen. Aes - the advanced encryption standard. *The Design of Rijndael*, 1(1):1–238, 2002.

29. C. Alippi, G. Anastasi, M. Francesco, and M. Roveri. An adaptive sampling algorithm for effective energy management in wireless sensor networks with energy-hungry sensors. *IEEE TRANSACTIONS ON INSTRUMENTATION AND MEASUREMENT*, 59(2), 2010.