Energy-efficient Adaptive Encryption for Wireless Visual Sensor Networks

Danilo de Oliveira Gonçalves[1], **Daniel G. Costa**[1]

[1]PGCA-UEFS, State University of Feira de Santana, Brazil

daniloxm@gmail.com, danielgcosta@uefs.br

Abstract. *Wireless sensor networks are usually composed of small sensor nodes with low processing power, limited memory and restricted energy supply. Among them, camera-enabled sensors can be used to gather visual data, but some relevant processing and transmission challenges are raised. In general, sensor networks have many vulnerabilities that can be exploited by attackers, demanding defense measures. However, traditional security mechanisms may impose high computing and communication overhead, which may compromise network performance specially when visual data is sensed from monitored fields. In this context, this paper proposes a new paradigm to ensure energy-efficient security for wireless visual sensor networks, defining an adaptive encryption approach. Doing so, confidentiality, authenticity and integrity are assured adaptively and according to application requirements, saving resources of networks while providing acceptable levels of protection for retrieved data.*

1. Introduction

Wireless Sensor Networks (WSN) are an emerging low-cost technology designed to retrieve information from several types of environments. Those networks are composed of hundreds, even thousands, of small devices with sensing, processing and communication capabilities [Yick et al. 2008]. Usually, WSN are only able to collect scalar data such as temperature, pressure or humidity. However, there is another type of sensor network that employs camera-enabled sensors to also retrieve video streams and still images [Costa and Guedes 2011], potentially enriching monitoring and control applications. Such Wireless Visual Sensor Networks (WVSN) retrieve much more information from the environment when compared to scalar sensor networks, imposing many designing and operation challenges.

WSN are inherently vulnerable to various types of security threats due to their distributed nature and the way they are employed, especially in remote areas [Yick et al. 2008]. In addition, wireless communications are subject to failures and security attacks. Depending on applications requirements, security aspects may be very important to ensure proper network operation, correct energy expenditure and the preservation of secrets. Therefore, security may be a very important issue in WSN design, but due to resource constraints in sensor nodes, traditional security mechanisms with high computing and communication overhead become too degrading for WSN [Sen 2009]. In short, security in WSN is a challenging task and resource limitations are even more stringent when networks retrieve multimedia data.

Generally speaking, wireless sensor networks are intrinsically vulnerable to internal and external attacks [Yick et al. 2008]. We then propose an innovative approach to provide security to wireless visual sensor networks with small additional overhead. A new security paradigm is proposed herein, referred as Adaptive Encryption, which is centered at minimizing the use of network resources to provide security.

The proposed adaptive encryption paradigm arises as a generic security approach that is premised on the adaptation of security mechanisms according to application monitoring requirements. This paradigm is centered at the definition of Confidential Areas (CA), which define an area of influence and an expected level of confidentiality. Actually, a wireless visual sensor network may be monitoring areas of interest with different demands for confidentiality. The network then employs a specific encryption mechanism that optimally provides protection of sensed data. For example, a wireless visual sensor network monitoring a factory may view areas with different relevances for an application, as the parking area, the engines rooms, entrance halls and the manager office. Each of these areas may have different confidentiality requirements concerning critical data that have to be protected from external attackers. In other words, using this model, it is not necessary to apply security mechanisms for the network as a whole, if the application requirements indicate that only a few sensor nodes in specific areas should have their data secured.

The proposed approach aims to minimize the use of network resources that are required to provide security, mainly energy consumption, when compared to mechanisms that provide the same protection for the entire network. As most wireless sensor networks have limitations in communication, processing, memory, storage and energy, the proposed model can be valid to aggregate different security levels without degrading network performance. Besides Confidential Areas, we also define procedures to create those areas and a specialized protocol. Moreover, we define different security schemes for validation of the proposed approach.

The remainder of the paper is organized as follows. The second section presents some related works. Section 3 presents the key definitions of the proposed approach. Section 4 defines the procedures to configure confidential areas. Initial results are presented in Section 5, followed by conclusions and references.

2. Related works

Many applications for wireless visual sensor networks may require minimum levels of security to assure confidentiality, authenticity and integrity for images captured by a network. However, traditional security mechanisms are not adapted to such networks. Thus, there is a need for optimizations and new paradigms to efficiently provide security in WVSN.

Attacks will typically be centered in exploiting vulnerabilities in some communication layer, eavesdropping transmitted data, altering confidential data or prejudicing the network operation with artificial malicious information [Gonçalves and Costa 2015]. Security threats may be of different types and may have different impacts on wireless sensor networks [Wang et al. 2013, Winkler and Rinner 2014, Chen et al. 2009]. This complex scenario push us to incorporate some defense mechanisms, which should comply with particularities and limitations of employed sensor nodes.

Cryptography is the basic defense mechanism in wireless sensor networks. It may be employed to provide authenticity, confidentiality and integrity for sensed data.

Actually, all communications can be intercepted by malicious nodes, demanding some protection. However, cryptography may be too resource-demanding, potentially degrading the limited resources of sensor networks. In this context, selective encryption comes as an optimized method that provides a reasonable level of secure data transmission with reduced overhead [Lecuire et al. 2007, Costa and Guedes 2011]. In short, this principle exploits characteristics of media coding algorithms to provide secrecy while reducing computational complexity [Grangetto et al. 2006].

In selective encryption, the basic idea is to encode only a set of blocks of sensed images. The work in [Nikolakopoulos and Fanakis 2009] proposes an adaptive compression mechanism to adapt transmission rate according to current network conditions. In the same way, the work in [Nikolakopoulos et al. 2010] proposes the use of Quadtree decomposition to support adaptive image compression and efficient congestion control. Raw images are decomposed using a Quadtree algorithm, and authors propose that higher compression should be adopted when fewer information should be transmitted, in a dynamic and adaptive way. The work in [Wang et al. 2010] proposes a selective encryption mechanism for video streams encoded using MPEG-4 codec. The relevance of video frames for the reconstruction process at the destination is exploited, where only high-relevant parts are encrypted.

In a similar context, data aggregation combines and summarizes data packets from several sensor nodes, which may be then encrypted [Ozdemir and Xiao 2009]. As source nodes may be compromised, authentication mechanisms may be also required before aggregation. A malicious node may provide false data packets that may reduce quality of aggregated data [Simplicio et al. 2013]. The work in [Gao et al. 2014] exploits the similarity that may be present in multimedia data, compressing sensed data for transmission. In a different way, the work in [Elsabi and Ozdemir 2012] combines data aggregation with watermarking, considering aggregation of scalar and image data.

All these security approaches influenced our work, but we proposed a different innovative solution for security protection. The definition of confidential areas, which can be dynamically created over monitored fields, is proposed in this paper to guide optimized cryptography, potentially bringing significant results for WVSN. And so cryptography context is not defined for specific transmission flows, as it happens when selective encryption is employed. Actually, the proposed approach defines a global perception of confidentiality that is valid for the entire network. To the best of our knowledge, no work has proposed such approach before.

3. Proposed approach

The idea behind the proposed approach of adaptive encryption is to provide security for wireless visual sensor networks without severely degrading the limited resources of sensor nodes. In order to achieve these objectives, the adaptive encryption model is centered at the concept of *Confidential Area* (CA). In addition, we propose herein other concepts related to confidential areas, as *Confidentiality Levels* and *Security Schemes*. These three concepts together will govern the operation of the proposed adaptive encryption model.

Sensing applications may require different confidentiality levels for certain parts of any monitored area. Thus, using the proposed paradigm, a sensor network is divided into smaller areas, where these areas may have different security levels that can be reflected in specific security mechanisms. Doing so, we can provide strong security only to areas with high security requirements, leaving the remaining areas with weaker security protection.

3.1. Confidential areas

The Confidential Area (CA) is a concept that defines a delimited geometrical area that is associated to a particular confidentiality level. Each confidentiality level is then mapped to a security scheme, which defines how data collected by sensor nodes will be protected. In other words, sensors included into a confidential area will be subject to a security pattern defined by applications. A typical WSN can have more than one CA, each one with particular levels of confidentiality. The application requirements concerning security demands for retrieved data and the characteristics of the monitored field will guide the definitions of confidential areas in sensor networks.

Therefore, the concept of CA defines that each delimited area has a particular confidentiality level, but how to provide security for collected data inside each area varies according to the adopted security scheme. Actually, although it is defined as a confidential area, the use of cryptography algorithms will naturally provide also authenticity and integrity for transmitted data. The use of the term ”confidentiality” was to emphasize the critical nature of some of retrieved data.

We defined a set of characteristics for Confidential Areas in wireless visual sensor networks, as follows:

- The creation of CAs and the inclusion of sensor nodes into them is performed centrally, at the sink side;
- Confidential areas do not overlap. That is, there is no intersection among different confidential areas, neither between areas with the same confidentiality levels;
- It may change over time. The borders of any CA may be adjusted, or the confidentiality level may be updated;
- A CA will always be a convex 2D quadrilateral. In this way, a CA is defined by a fivefold: CA(N,P,Q,R,S), where N is its confidentiality level and P, Q, R e S are ordered pairs of vertices of the quadrilateral.
- Some location service must be employed to support the proposed approach, which may be based on reference points, relative positions or GPS (Global Positioning System) coordinates [Pescaru and Curiac 2014];
- The definitions of all CAs in a WVSN are strictly indicated by application requirements, which is an abstract concept. The same physical network may have different CAs, according to the defined monitoring tasks;
- The concept of confidential areas is not used to prioritize data traffic generated within a CA. However, confidential data may also require QoS guarantees;

3.2. Confidentiality levels

The concept of Confidentiality Level (CL) is used to numerically represent a need for confidentiality for data originated from the corresponding CA. We define four different values for CL, as follows:

- **Level 0:** Area without encryption or any security mechanism, being the lowest level. This level is not associated to any CA, since it exists only to configure nodes that are not inside any CA. The notation is CA$_{N=0}$;

- **Level 1:** CA with low security. In those areas, sensor nodes require light security, with ”low” protection being applied. The notation is CA$_{N=1}$;
- **Level 2:** CA with moderate security requirements. Security at this level is slightly higher than the previous level, but with features that ensure some resource savings. Its notation is CA$_{N=2}$;
- **Level 3:** CA with maximum security. At this level, all collected data is protected at the highest level, even with high use of sensors’ resources. The notation is CA$_{N=3}$.

Often, there may be the need for more than one CA with the same value for CL. An example is the use of this model in an intrusion detection system, where the doors of a building can be monitored by sensor nodes inside multiple CA$_{N=3}$. In this case, there will be several CAs with level 3 on entering and exiting doors of the building.

3.3. Security schemes

The security schemes define which mechanism, aspect or security measure will be applied to each CA depending on their confidentiality levels. Such schemes may define, for example, encryption algorithms, key sizes, key management approaches or other mechanisms associated to data protection.

A wireless visual sensor network may define any type of security scheme, according to its monitoring requirements, but usually an unique scheme will be employed for the entire network at a time. We created some reference schemes to be used in generic networks, presented as follows, but generally any security scheme may be defined.

- **Scheme 1 - Coding**:
  - Level 0: Unencrypted;
  - Level 1: Selective image encryption (DWT at two levels);
  - Level 2: Selective image encryption (DWT at one level);
  - Level 3: Full image encryption.
- **Scheme 2 - Encryption key size**:
  - Level 0: Unencrypted;
  - Level 1: 128-bit key;
  - Level 2: 192-bit key;
  - Level 3: 256-bit key.
- **Scheme 3 - Collected data type**:
  - Level 0: Unencrypted;
  - Level 1: Encryption of only scalar data;
  - Level 2: Encryption of scalar data and still images;
  - Level 3: Encryption of scalar data, still images and video streams.

Therefore, a security scheme will define which action will be taken when applying the proposed adaptive encryption model. In addition, it is worth mentioning that data collected inside a CA level 1 still has some confidentiality, even with reduced protection. Actually, the concept of security scheme makes it clearer that the general idea of the proposed approach is to degrade less network resources when compared to security approaches that protect the network as a whole.

4. Network deployment and configuration

One key issue of the proposed approach is how to associate deployed sensor nodes to defined confidential areas. As CAs are defined by applications, nodes must know which CA they belong to.

In wireless visual sensor networks, camera-enabled sensors monitor an area based on a direction of viewing, defined by their Field of View (FoV) [Costa and Guedes 2011]. Hence, the same sensor may view areas ”belonging” to different CAs. Actually, there are different configurations for sensor nodes in relation to a confidential area, concerning the overlapping of the sensor's FoV and the defined CA.

We define that only for the configuration where a sensor node and its field of view are both outside of a considered CA, that sensor node is assumed as not belonging to that confidential area. In all other cases the sensor node belongs to the considered CA.

Figure 1 presents the Field of View of camera-enabled sensors. For simplification, we assume the FoV as an isosceles triangle, defined by a sensing radius (R), a viewing angle (θ) and an orientation (α).

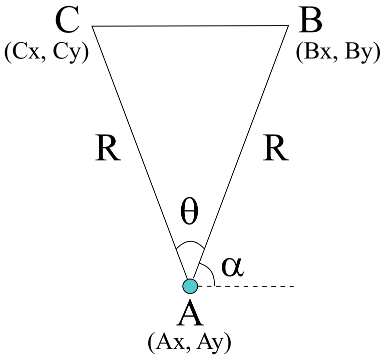


Figure 1. Field of View (FoV) of a visual sensor node [Costa et al. 2014].

4.1. Geometric model

We propose a geometric model to regulate the association of any sensor node to confidential areas. In this geometric model, each vertex is analyzed at a time. If at least one vertex of the FoV is within a CA (Figure 2(a)), the sensor node as a whole will be considered included in that CA, assuming its preset policies and security schemes. In order to perform the desired computing for each vertex, we employ linear geometry, as graphically expressed in Figures 2(b) and 2(c).

Assuming a quadrilateral PQRS which defines a CA and one vertex V, as shown in Figure 2(b), the following triangles will be created: VPQ, VQR, VRS, VPS. The formulation in (1) is employed to compute the areas of these triangles, comparing the result to the computed area of the CA.

$$\begin{aligned} &X = \Delta_{VPQ} + \Delta_{VQR} + \Delta_{VRS} + \Delta_{VPS} \\ &If\; X = \Delta_{PQRS}\;\; (Vertex\; within\; the\; CA) \\ &If\; X > \Delta_{PQRS}\;\; (Vertex\; out\; of\; the\; CA) \end{aligned} \tag{1}$$

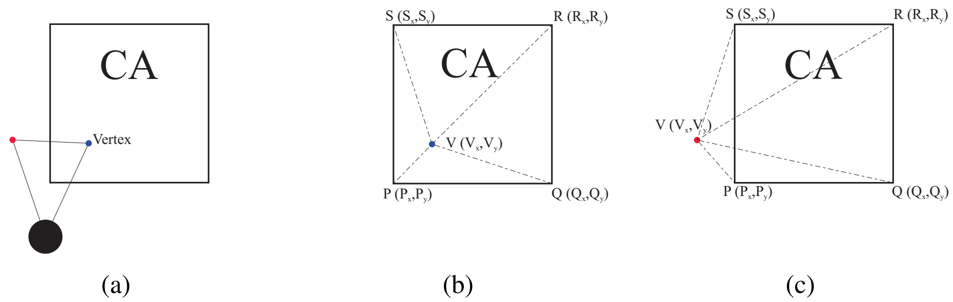


Figure 2. Viewing a CA (a) Sensor node with one of the vertices within the CA; (b) Example of an included vertex; (c) Example of a not included vertex.

The areas of the created triangles will be computed as expressed in (2).

$$\begin{aligned}
\Delta_{VPQ} &= \frac{V_x.(P_y - Q_y) + P_x.(Q_y - V_y) + Q_x.(V_y - P_y)}{2} \\
\Delta_{VQR} &= \frac{V_x.(Q_y - R_y) + Q_x.(R_y - V_y) + R_x.(V_y - Q_y)}{2} \\
\Delta_{VRS} &= \frac{V_x.(Q_y - S_y) + R_x.(S_y - V_y) + S_x.(V_y - R_y)}{2} \\
\Delta_{VPS} &= \frac{V_x.(P_y - S_y) + P_x.(S_y - V_y) + S_x.(V_y - P_y)}{2}
\end{aligned} \tag{2}$$

Besides the computing of vertices positions, there are other scenarios that must to be treated. If a vertex is on top of one side of the CA or upon the prolonged line of one side of the CA, only three triangles can be created. This way, even when one of the areas of the four triangles is zero, if the sum of the other three areas is equal to the area of the CA, it means that the vertex is located over one side of the CA. If the sum of the three other areas of the triangles is greater than the area of the CA, it means that the vertex is on the prolonged line of one side of the CA and thus out of the CA.

Another situation is if one of the vertices of the triangle formed by the sensor node and its FoV is coincident with one of the vertices of the quadrilateral that delimits the CA. In this case, a coincidence test must to be performed. If the test is successful, the vertex is assumed as belonging to the considered CA.

A final remark is when the sensor's FoV covers two or more different CAs. In this case, the proposed approach associates the sensor to the CA with highest confidentiality level, in order to not compromise the application requirements.

4.2. Association protocol

The procedures previously described are required to associate sensor nodes to confidential areas. Actually, such computing is performed in a centralized way, at the sink side. Thus, there should be adopted some mechanism to inform sensor nodes that they belong to a particular confidential area, and hence they must follow a particular security scheme. Moreover, as it is an adaptive approach, changes in parameters of CA must be reflected into the network. For these cases, we propose the application-level Confidential Area Association Protocol (CAAP).

Initially, sensor nodes are pre-configured with the security scheme to be adopted by the sensing application. Each sensor node should already know what to do with sensed data when it is associated to a CA. Moreover, when the network starts operation, every sensor node is automatically associated to the confidential area with level 0.

The CAAP protocol has its operation centered at three different types of messages. A request/identification message of sensor node (CA-Request), a configuration message (CA-Configure) and an acknowledgment message (CA-ACK). CA-Request is a message that is only sent by the sink toward a sensor node. This message requests information about the sensor node, such as CA current level and location. In an ideal scenario where sensors do not change position, this message may become unnecessary if the sink node is configured with information of all sensor nodes. However, as position of sensor nodes may change along the time, the sink should send a CA-Request message requesting information of the sensor nodes. After receiving a CA-Request, the sensor node answers this message sending back a CA-ACK message for acknowledgment purposes. This CA-ACK message also reports the requested information, which is usually the current location and confidentiality level. The CA-Configure message is a return message, sent only by the sink node toward a sensor node and providing configuration after computing the corresponding CA. Finally, another CA-ACK message is also used for the acknowledgment of the CA-Configure message, finishing the communication cycle.

CAAP is intended to be an energy-efficient reliable application-layer protocol. As wireless transmissions are very susceptible to transmission errors and packet losses, this protocol provides retransmissions as an error recovery mechanism. As described previously, the CA-ACK message is sent only by a sensor node as a response and acknowledgment to other messages. Actually, the CA-ACK message is not confirmed by its receptor, i.e., it is used for the acknowledgment of two other messages, but who sends a CA-ACK does not receive any acknowledgment of receipt. This is due to energy constraints of sensor nodes.

The protocol operation is controlled by two counters: t_m and t_{ack}. The counter t_m sets the time that the sink node should wait for the receiving of a CA-ACK message. On the other hand, the counter t_{ack} sets the time required to ensure that a CA-ACK message was received by the sink node. Thereby, t_{ack} is used by sensor nodes to control whether it should assume or not that a transmitted CA-ACK message sent by it was correctly received by the destination. In such way, if no CA-ACK message is received by the sink before t_m, the corresponding message should be retransmitted. Actually, a retransmission will be required in the following cases:

- If a CA-request or CA-Configure message is lost (dropped or corrupted) during transmission;
- If a CA-ACK message is lost;
- If a CA-ACK message is received after t_m.

In order to ensure some scalability to the proposed protocol, t_m should double if a CA-request or CA-Configure message needs to be retransmitted. The maximum number of retransmissions of the same message was settled in 4, in order to avoid many retransmission attempts when routes are congested or inactive. Thus, for *r* as an attempt of retransmission, *r* = 1, ..., 4, and the end-to-end time for transmission, processing and acknowledgment defined as t_r, we can define t_m as $t_m = 2^{(r-1)}.t_r$. The value for t_m is reset to the reference value t_r after each successful transmission.

It is expected that $t_{ack} < t_m$, even in cases of retransmission when t_m increases. Concerning counter t_{ack}, after sending a CA-ACK message, the transmitting sensor node waits for t_{ack} with the following constraints:

- If a CA-request or CA-Configure message is received before t_{ack}, it is assumed that the CA-ACK was lost;
- If a CA-request or CA-Configure message is receive after t_{ack}, it must be assumed that the CA-ACK was received correctly and that it is a new message.

Figure 3 illustrates an example of CAAP operation.

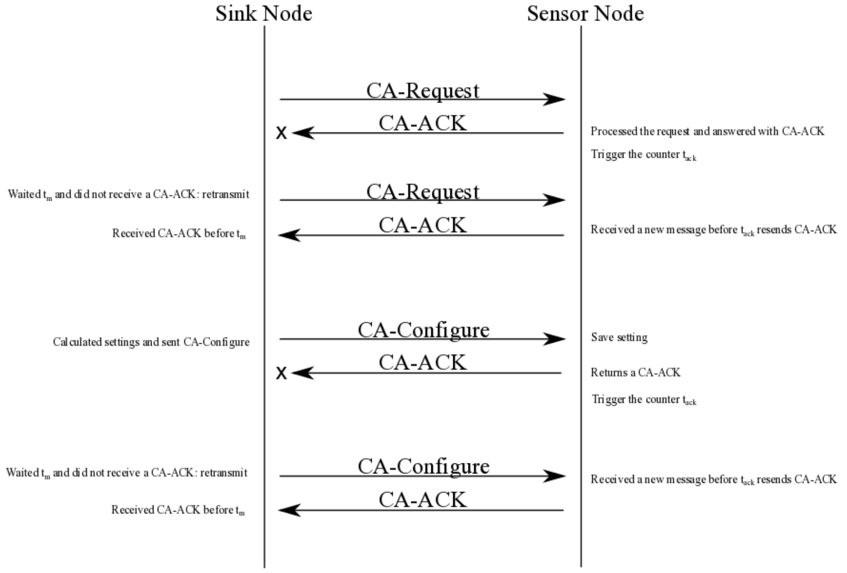

Sink Node
Sensor Node
CA-Request
CA-ACK
Processed the request and answered with CA-ACK
Trigger the counter t_{ack}
Waited t_m and did not receive a CA-ACK: retransmit
CA-Request
Received CA-ACK before t_m
CA-ACK
Received a new message before t_{ack} resends CA-ACK
Calculated settings and sent CA-Configure
CA-Configure
Save setting
CA-ACK
Returns a CA-ACK
Trigger the counter t_{ack}
Waited t_m and did not receive a CA-ACK: retransmit
CA-Configure
Received a new message before t_{ack} resends CA-ACK
Received CA-ACK before t_m
CA-ACK

Figure 3. Operation example of CAAP protocol with CA-ACK losses.

5. Numerical results

In order to validate the proposed approach and attest the expected benefits, a series of mathematical verifications were performed. Some verification scenarios were defined, where AES (Advanced Encryption Standard) [Wang et al. 2011] was employed as the reference algorithm (although other algorithms could be employed with no prejudice to the performed verifications). We defined two security schemes: Scheme 1, based on DWT (Discrete Wavelet Transform) image coding, and Scheme 2, based on different AES key sizes, as previously defined.

Figure 4 presents a diagram for the first security scheme. Sensor nodes located at CA$_{N=3}$ will encrypt all data of every retrieved image, which are transmitted with no coding. Sensor nodes located at CA$_{N=2}$ will apply DWT just once, encrypting only sub-layer $LL_{(1)}$. Finally, sensor nodes located at CA$_{N=1}$ will perform encoding in two DWT levels, encrypting only the sub-layer $LL_{(2)}$. The remaining visual sensors will not encrypt sensed images.

Regarding Scheme 2, Figure 5 presents its generic diagram.

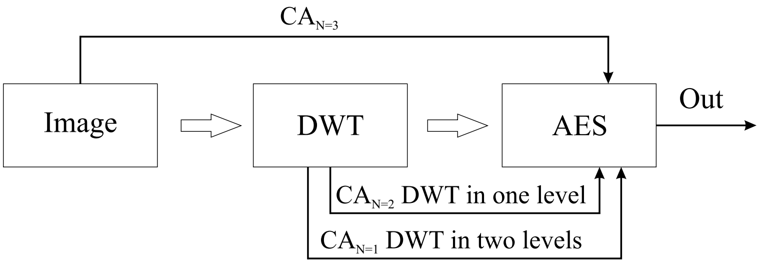


Figure 4. Diagram for Scheme 1.

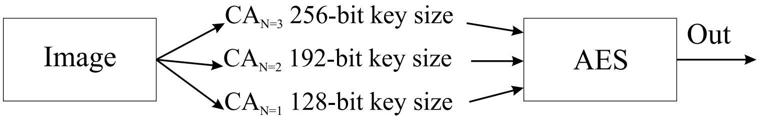


Image
$CA_{N=3}$ 256-bit key size
$CA_{N=2}$ 192-bit key size
$CA_{N=1}$ 128-bit key size
AES
Out

Figure 5. Diagram for Scheme 2.

The main objective of the proposed approach is to save energy when compared with security mechanisms where every sensed data is protected. For that, energy consumption when applying AES encryption in source nodes had to be assessed. Energy consumption was assessed based on definitions in [Potlapally et al. 2006] and parameters as sensed data and key size. The formulation in (3) defines the consumed energy for the performed encryption.

$$EnergyCost_{(Si)} = EKey_{(Si)} + (EByte_{(Si)} * Size_{(Data)}) \tag{3}$$

In equation (3), $EKey_{(Si)}$ represents the energy costs to expand the symmetric key for algorithm Si. The energy consumed per byte in encryption/decryption using the algorithm Si is given by $EByte_{(Si)}$, and $Size_{(Data)}$ is the total data size to be encrypted by the algorithm Si. Using this equation it is possible to estimate energy consumption for any symmetric encryption algorithm.

The values for $EKey_{(Si)}$ and $EByte_{(Si)}$ are described in [Potlapally et al. 2006], for algorithm AES, as presented in Table 1.

Table 1. Energy cost of AES variants [Potlapally et al. 2006].

Key Size (bits)	$EKey_{(AES)}$ (μJ)	$EByte_{(AES)}$ in ECB mode (μJ/B)	$EByte_{(AES)}$ in CBC mode (μJ/B)	$EByte_{(AES)}$ in CFB mode (μJ/B)	$EByte_{(AES)}$ in OFB mode (μJ/B)
128	7.83	1.21	1.62	1.91	1.62
192	7.87	1.42	2.08	2.30	1.83
256	9.92	1.64	2.29	2.31	2.05

We defined some verification scenarios to be considered when assessing energy consumption, as expressed in Table 2.

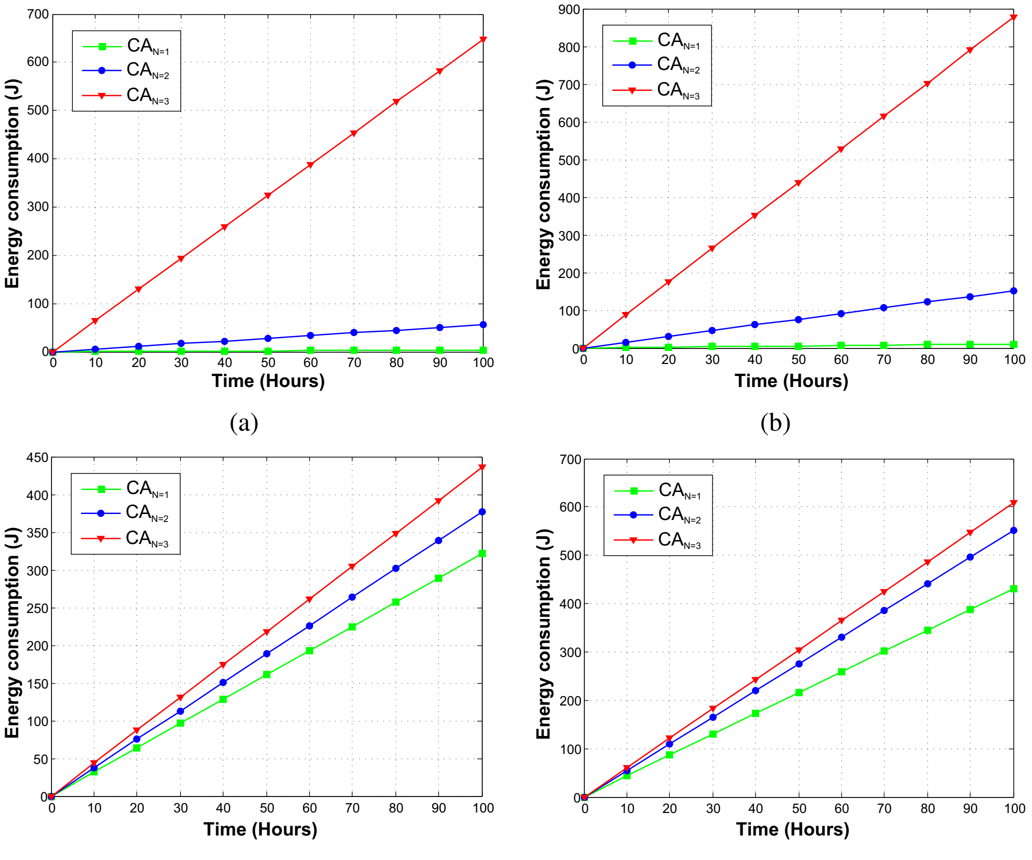
All performed verifications considered 100 hours of transmissions where all deployed visual sensors periodically transmit images. Moreover, we assumed that each

Table 2. Initial verification scenarios.

Scenario	Security scheme	Image resolution	Key size	CA$_{N=1}$	CA$_{N=2}$	CA$_{N=3}$	Algorithm
1	1	128 x 128 x 8	128 bits	125	125	125	AES / ECB
2	1	256 x 256 x 4	256 bits	125	125	125	AES / ECB
3	2	128 x 128 x 4	vary	90	90	90	AES / ECB
4	2	128 x 128 x 4	vary	90	90	90	AES / CBC

source node collects, encrypts and transmits only one image snapshot per second. Concerning the encryption algorithm, we considered AES in ECB (Electronic Code Book) or CBC (Cipher Block Chaining) modes.

Figure 6 presents the total consumed energy for image encryption in all deployed source nodes, for Scenarios 1, 2, 3 and 4.



(a)

(b)

(c)

(d)

Figure 6. Energy (J) (a) Scenario 1; (b) Scenario 2; (c) Scenario 3; (d) Scenario 4.

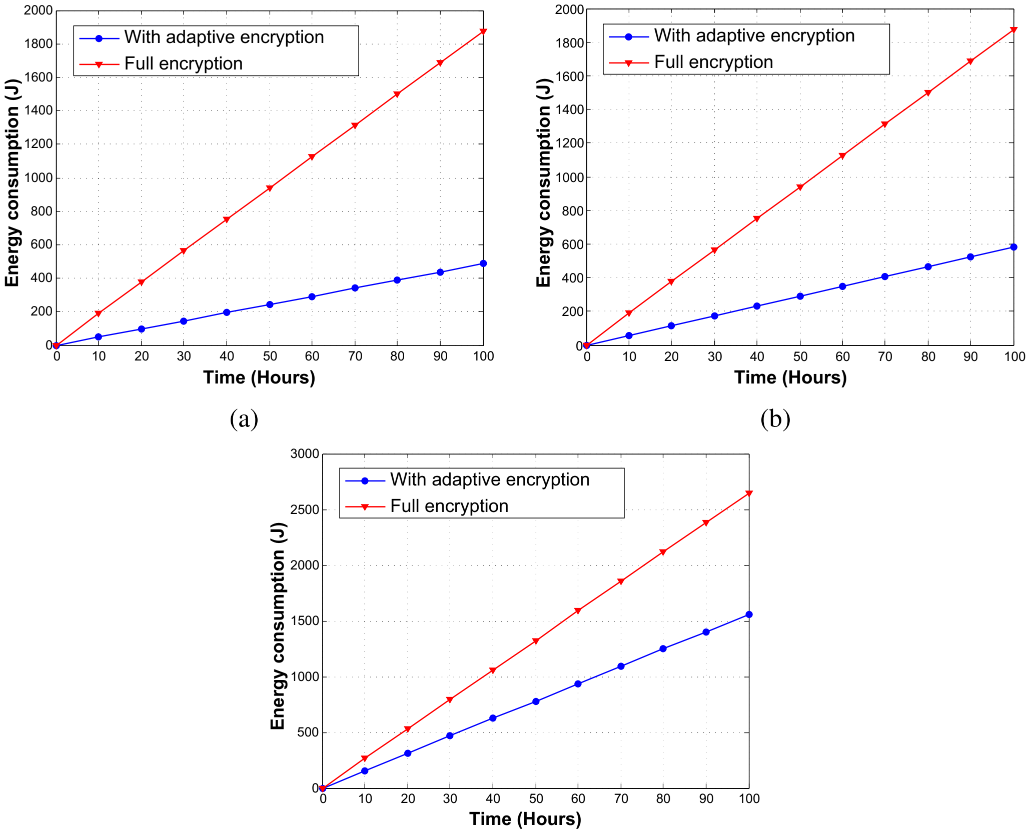
As can be seen in Figure 6, energy consumption depends on the adopted security scheme, which directly depends on definitions of confidential areas. In other words, the identification of CAs is central for energy preservation in WVSN, since neither all visual source nodes and viewed areas will have the same security requirements. As expected, energy consumption was higher for confidential areas with higher confidentiality levels.

The second stage of verifications was concerned with energy consumption for an entire wireless visual sensor network, when the proposed approach is employed. Table 3 presents the configurations for Scenarios 5, 6 and 7, that will be considered for these verifications. For these three scenarios, a total of 270 visual source nodes were deployed, where some of them are associated to $\text{CA}_{N=0}$.

Table 3. Additional verification scenarios.

Scenario	Security scheme	Image resolution	Key size	$\text{CA}_{N=1}$	$\text{CA}_{N=2}$	$\text{CA}_{N=3}$	Algorithm
5	1	128 x 128 x 8	128 bits	46	32	67	AES / CBC
6	1	128 x 128 x 8	128 bits	41	56	79	AES / CBC
7	2	128 x 128 x 4	vary	41	56	79	AES / CBC

The presented results in Figure 7 shows the consumed energy for a network ensuring full protection for all sensor nodes (as if all nodes where in a $\text{CA}_{N=3}$) and the energy for a network employing the proposed approach. Actually, the energy consumed for CAAP operation is too low compared to the overall data transmissions, with CAAP messages typically sizing less than 20 bytes.



(a)

(b)

(c)

Figure 7. Energy consumption (a) Scenario 5; (b) Scenario 6; (c) Scenario 7.

One can see in Figure 7 that energy consumption in a sensor network without the proposed solution is higher than the consumed energy for the same network when employing the adaptive encryption mechanism. And although it may seem that the ”traditional” security mechanism is safer, the proposed approach provided high security protection to all critical data.

As a final remark, CAAP may impact the overall latency for assignment of sensor nodes to CAs. Actually, the initial assignment during network startup is not necessarily a concern, but additional CAAP communications will incur in some delay for nodes assignment and use of the proper security scheme. In fact, latency in wireless sensor networks depends on many characteristics, as duty cycling configuration, MAC operation, bit rate, routing protocol, among others. Nevertheless, for any additional delay, and considering that CAAP comprises few messages, the time until new security schemes will be applied due to new CA configurations will be too short comparing to the network lifetime. And such additional delay will not cause a security breach.

After initial verification, we may expect that the proposed solution will bring significant results to wireless visual sensor networks. Actually, fewer energy consumption is achieved while assuring strong protection to sensed data with high confidential requirements.

6. Conclusions

As applications may have different security requirements for monitored areas, this paper proposes an innovative approach that can save energy while assuring acceptable levels of security protection. We defined the concepts and procedures for the adoption of this approach, which was initially designed for wireless visual sensor networks.

This work is not concluded yet. As future works, the proposed approach will be validated in real sensor networks, employing RaspBerry PI sensor motes to implement Secure Schemes and CAAP. Doing so, we plan to validate processing and memory costs of the proposed approach. Moreover, we also want to integrate it with QoS and QoE-based optimizations, achieving secured and prioritized wireless visual sensor networks.

Acknowledgment

The authors would like to acknowledge the support of the Brazilian research agency CNPq (grant number 441459/2014-5), that partially funded this work.

References

Chen, X., Makki, K., Yen, K., and Pissinou, N. (2009). Sensor network security: a survey. *IEEE Communications Surveys & Tutorials*, 11(2):52–73.

Costa, D. G. and Guedes, L. A. (2011). A survey on multimedia-based cross-layer optimization in visual sensor networks. *Sensors*, 11(5):5439–5468.

Costa, D. G., Silva, I., Guedes, L. A., Portugal, P., and Vasques, F. (2014). Selecting redundant nodes when addressing availability in wireless visual sensor networks. In *Industrial Informatics (INDIN), 2014 12th IEEE International Conference on*, pages 130–135. IEEE.

Elsabi, E. and Ozdemir, S. (2012). Secure data aggregation in wireless multimedia sensor networks via watermarking. In *Proceedings of the International Conference on Application of Information and Communication Technologies*, pages 1–6.

Gao, R., Wen, Y., Zhao, H., and Meng, Y. (2014). Secure data aggregation in wireless multimedia sensor networks based on similarity matching. *International Journal of Distributed Sensor Networks*, 2014:Article ID 494853, 6 pages.

Gonçalves, D. and Costa, D. G. (2015). A survey of image security in wireless sensor networks. *Journal of Imaging*, 1(1):4–30.

Grangetto, M., Magli, E., and Olmo, G. (2006). Multimedia selective encryption by means of randomized arithmetic coding. *Multimedia, IEEE Transactions on*, 8(5):905–917.

Lecuire, V., Duran-Faundez, C., and Krommenacker, N. (2007). Energy-efficient transmission of wavelet-based images in wireless sensor networks. *Journal on Image and Video Processing*, 2007:1–15.

Nikolakopoulos, G. and Fanakis, N. (2009). A reconfigurable transmission scheme for lossy image transmission over congested wireless sensor networks. In *Proceedings of the International Congress on Image and Signal Processing*.

Nikolakopoulos, G., Kandris, D., and Tzes, A. (2010). Adaptive compression of slowly varying images transmitted over wireless sensor networks. *Sensors*, 10(8):7170–7191.

Ozdemir, S. and Xiao, Y. (2009). Secure data aggregation in wireless sensor networks: A comprehensive overview. *Computer Networks*, 53(12):2022–2037.

Pescaru, D. and Curiac, D.-I. (2014). Anchor node localization for wireless sensor networks using video and compass information fusion. *Sensors*, 14(3):4211–4224.

Potlapally, N. R., Ravi, S., Raghunathan, A., and Jha, N. K. (2006). A study of the energy consumption characteristics of cryptographic algorithms and security protocols. *Mobile Computing, IEEE Transactions on*, 5(2):128–143.

Sen, J. (2009). A survey on wireless sensor network security. *International Journal of Communication Networks & Information Security*, 1(2):59–82.

Simplicio, M. A., Oliveira, B. T., Margi, C. B., Barreto, P. S. L. M., Carvalho, T. C. M. B., and NÃslund, M. (2013). Survey and comparison of message authentication solutions on wireless sensor networks. *Ad Hoc Networks*, 11:1221–1236.

Wang, Q.-X., Xu, T., and zhou Wu, P. (2011). Application research of the aes encryption algorithm on the engine anti-theft system. In *Proceedings of IEEE International Conference on Vehicular Electronics and Safety*, pages 25–29.

Wang, W., Hempel, M., Peng, D., Wang, H., Sharif, H., and Chen, H.-H. (2010). On energy efficient encryption for video streaming in wireless sensor networks. *IEEE Transactions on Multimedia*, 12(5):417–426.

Wang, Y., Attebury, G., and Ramamurthy, B. (2013). Security issues in wireless sensor networks: a survey. *International Journal of Future Generation Communication and Networking*, 6(5):97–116.

Winkler, T. and Rinner, B. (2014). Security and privacy protection in visual sensor networks: A survey. *ACM Computing Surveys*, 47(1):97–116.

Yick, J., Mukherjee, B., and Ghosal, D. (2008). Wireless sensor network survey. *Computer networks*, 52(12):2292–2330.