Journal of Theoretical and Applied Information Technology
31st January 2015. Vol.71 No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

ASATE : AN ADAPTIVE SECURE SCHEME FOR EFFECTIVE WIRELESS SENSOR NETWORK IN EMERGENCY SITUATION

[1]RACHID HAJI, [2]HICHAM BEKKARI, [1]ABDERRAHIM HASBI, [1]ABDELILAH MAACH

[1]Network Team and Intelligent Systems Laboratory
Mohammed V University, Mohammadia School of Engineering
Rabat, Morocco
[1] rachaji@gmail.com, hasbi@emi.ac.ma, maach@emi.ac.ma, [2] h.bekkari@gmail.com

ABSTRACT

In emergency situation, wireless sensor networks can be subject to various attacks aimed to mislead information or to paralyze the network. In such context, security is an essential requirement to ensure efficient communication within sensor network. Most of the proposed security protocols for WSNs fix only a part of security issues and are based on authentication or cryptography. In this paper, we propose to enhance framework Ad-M-QOS-DS with a new adaptive secure capability. The new feature brings more confidentiality, data integrity and availability within malicious context. The new security layer ASATE combined three approaches: Authentication based on MAC Filtering, Trust index based on the criticality of events and adaptable Encryption depending on the type of messages spread on the network and the present risk.

Keywords: *Emergency situations; Wireless Sensor Networks; Security; Authentication; Trust Index; Risk; Encryption*

1. INTRODUCTION:

The most important factor characterizing an emergency situation is the lack of information or the difficult access to it. The use of wireless sensor networks (WSN) in this type of applications allows having an almost real-time status of the supervised area by collecting relevant information and thus assisting in the process of rapid response to the disaster. Some studies present the benefits of the use of wireless sensor networks WSN in such situations [1] [2] [3] [4]. A typical WSN consists of several sensors distributed in the area of interest; each sensor consists of three main components: A sensing unit, a wireless communication unit, and a processing and storage unit. All these units are supplied with a battery. The sensors create an Ad-hoc network in a distributed and automatic way to deliver the sensed data to the base station.

In many vital and critical areas such as military, health or anti-terrorism, beside of the guarantee of QoS, the security communication presents also a major key to a successful management and rescue operation during emergency situations with a high risk. However, WSN has several inherent vulnerabilities that increase the security risks. The low-cost and low-power of the WSN devices make them incapable of supporting usual and adequate security mechanisms, making them vulnerable to various types of threats such as DoS attacks that aim essentially to drain their energy and affect the availability to the users [5], thus compromising the reception of supposedly critical data. Consequently, WSN require efficient and effective security mechanisms to be protected from these dangerous threats, while taking into account WSN restraints like limited resources and energy, inaccessibility, the large number of devices (sensors) [6].

In this paper, we propose a new Adaptable Security module based on Authentication, Trust index and Encryption (ASATE) for WSNs that we will implement with our framework Ad-M-QOS-DS [7] in order to ensure communication with confidentiality, data integrity and availability of services in malicious context. Our new security module combined tree approaches:

- Authentication based on MAC filtering.
- Trust index based on the criticality of events, our trust index is centralized at two levels.
- Adaptable encryption depending on the type of messages spread on the network and the present risk.

Journal of Theoretical and Applied Information Technology
31st January 2015. Vol.71 No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

The rest of this paper is organized as follows: in section 2, the related work of security of WSN using authentication, trust index and encryption is presented. Section 3 gives an overview of our framework. Section 4 describes the proposed adaptive security model including its architecture, the adopted approach and the security algorithm. The integration of our proposed security module ASATE with our framework Ad-M-QOS-DS is illustrated in Section 5. Finally, we conclude the paper and present future work in section 6.

2. RELATED WORK

WSN are used in many rescue operations to face emergency cases. Such situations enclose fire, flood, tsunami, earthquake, terrorist attack. The efficiency of rescue activities is linked with communication security and QoS. Indeed, WSN must provide communication with confidentiality, data integrity, and availability of service [5]. So, those networks must benefit from a high level security, especially when implemented on vital domains, such as military or anti-terrorism, where they can be subject to hackers' attacks, aiming for information misleading or network paralysis. Many works deal with this challenge, we will present in this section the related work of three approaches: Authentication, trust index and encryption.

Message authentication is important for many applications in sensor networks; the authentication scheme ensures that the communicating node is the one that it claims to be. Especially for administrative tasks, when a receiver wants to perform a decision-making process, it has to be sure that the data used is originated from the right one. Indeed an adversary can easily inject messages; therefore, the receiver can make the wrong decision. In case of two-party communication, data authentication can be achieved through a purely symmetric mechanism: The sender and the receiver share a secret key to compute a Message Authentication Code (MAC) of all communicated data. When a message with a correct MAC arrives, the receiver knows that it must have been sent by the right sender. A number of authentication schemes for WSNs have been proposed by researchers. In the survey of Guo et al. [8], they classify the authentication mechanism in tree major categories:

- Authentication mechanism based on symmetric cryptography:
  - Authentication mechanism based on KDC
  - Authentication mechanism based on key pre-distribution
- Authentication mechanism based on asymmetric cryptography:
  - Authentication mechanism based on certificate
  - Authentication mechanism based on identity
- Broadcast authentication

Authentication does not enough to prevent insider attacks, so trust approach can be used to increase the security, the reliability, the resilience and the life time of network. Trust model allows detecting malicious and compromised nodes by monitoring the behaviors of WSN.

In the literature, the trust model proposed can be classified as centralized, distributed and hybrid [9], and used to improve data integrity, aggregation and collaboration among sensors nodes and provide reliable communication and routing.

RFSN [10] is the first trust-based model designed and developed exclusively for sensor networks, it use watchdog mechanism to build trust rating.

A Bayesian probabilistic framework model to calculate and continuously update trust values between nodes in wireless sensor networks based on a sensed continuous event (temperature) was constructed [11]. This framework allows excluding malicious and faulty nodes from the network. Thus, the objective of this mechanism is to maintain the security and the reliability of a sensor network. They extend the Beta Reputation System introduced in [12] that deals with binary, discrete data, to the case of continuous sensor data and present a new Gaussian Trust and Reputation System for Sensor Networks (GTRSSN). Based on the trust value maintained by the node for its neighbors, the cooperation occurs between nodes.

In [13] they propose an agent-based trust and reputation management scheme (ATRM) for wireless sensor networks. The objective of their scheme is to manage trust and reputation locally with minimal overhead in terms of extra messages and time delay there is no need for centralized repositories, and the nodes themselves are able to provide their own reputation information whenever requested; therefore, reputation computation and propagation is done without network wide flooding and with no acquisition-latency.

Journal of Theoretical and Applied Information Technology
31st January 2015. Vol.71 No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

A lightweight group based trust management scheme (GTMS) is introduced in [14]. It uses hybrid approach that combines centralized and distributed ones in order to minimize resource consumption. Their group-based trust model works in three levels: at node, cluster-head and the base station levels.

In some contexts, monitoring data and some information collected by the sensors are considered as sensitive, and this information must be protected against traffic analysis and eavesdropping by malicious nodes. A standard approach to protect the confidentiality of such information is cryptography.

However, The use of secret key mechanisms for establishing trust can significantly reduce energy consumption of the sensor node, which is the main advantage of this solution based on HMAC (Hash-based Message Authentication Code) compared to public key algorithms regarding the resource constrained sensor nodes [15]. However, this approach turns out weak faster because if one arrive to compromise a single sensor node, the unique key may be revealed, which will put the entire network at major risk. To overcome this limitation, several researchers propose different schemes that establish pairwise keys rather than a unique global key.

In [16] the authors propose an algorithm for key management in a cluster-based architecture in WSN. The purposes of this scheme are minimizing the computation, communications overhead and storage generated by the key management. They adopt pre-deployed shared symmetric keys with storing only two secret keys in each node. This approach stores the keys as follows:

The Base Station stores all keys shared with nodes and cluster-heads

The cluster-head stores three types of keys

Keys shared with its members;

A key shared with the Base Station;

A key shared with other clusters-head.

Each node stores two keys

A key he shares with his cluster-head;

A key shared with the Base Station (used for revocation of compromised nodes and updating key).

A classification of key management schemes according to the applications requirements was presented in [17]. Because, it is very difficult to design a key management scheme that is optimal for all topologies of sensor networks and their applications. Fig. 1 presents the different schemes under the two major approaches that are asymmetric and symmetric. In addition, some schemes combine both these approaches as [18][19][20].

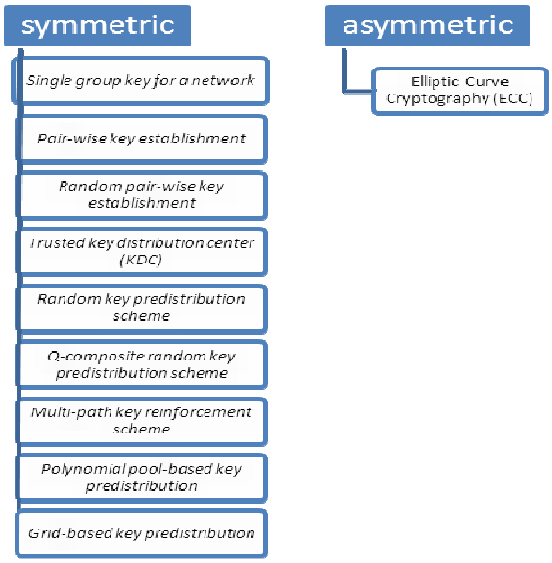

Figure 1: Classification of Encryption Schemes

In this paper, we propose a new adaptable security module to secure the communication within WSNs. Our mean contribution is to combine the tree approaches that are authentication, trust index and encryption and offer a different level of security according to the importance of the events. In addition our mechanism takes into account the QoS requirements.

3. FRAMEWORK AD-M-QOS-DS

Our Framework Adaptive Management of QoS in different situations (Ad-M-QoS-DS) [7] is a wireless infrastructure designed to better use of WSNs in the management of emergency situations. It allows an adaptive QoS management according to the needs specified for each situation of the supervised area. It guarantees a level of QoS using the following parameters: The situation, the degree of importance of information and QoS parameters. Under normal circumstances, the Framework focuses on the efficiency of energy consumption. Upon detection of an event of emergency, the proposed framework adapts its behavior to minimize delay and ensure reliability. And if that requires the intervention of operators, the framework ensures mobility management, collaboration, and security.

Journal of Theoretical and Applied Information Technology
31st January 2015. Vol.71 No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Fig. 2 presents the different modules of our Framework that are necessary for the proper management of rescue operations and cooperation during a disaster. These modules are the classification and prioritization module, the aggregation management module, the adaptive energy management module, the adaptive load management module and mobility management module

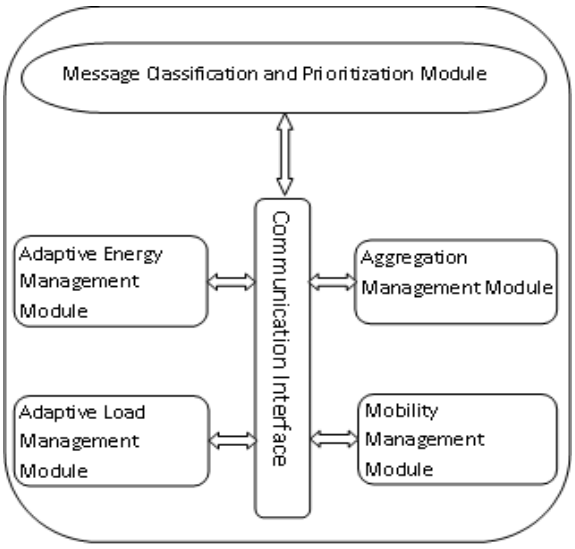

Figure 2: Framework Ad-M-QoS-DS.

The main advantages of our Framework can be summarized by:

- The energy conservation during a normal situation through aggregation, adaptive energy management and adaptive load management modules
- Establishment of a compromise between energy and delay for important data type through aggregation, adaptive energy management and adaptive load management modules.
- Minimizing delay and increase the reliability of critical data type, the fact that in emergency situation the delay and reliability are essential than energy.
- Improved rescue operations by taking into consideration the mobility of operators, and through better collaboration between them in executing the instructions of the committee.

4. SECURING THE FRAMEWORK: AUTHENTICATION, TRUST INDEX AND ENCRYPTION

Generally the information disseminated in the network environment is not critical, except in the domain of health, military and usually in emergency situations where the data is sensitive and requires a certain level of confidentiality. Note that also if the information is available in the environment, anyone can have access to this information. Added to this, the problem of confidentiality in the WSN due to the nature of the wireless medium, that facilitates the interception and remote access to the transmitted data. Therefore, it is legitimate to raise the question of knowing the types of information to be encrypted.

In our approach, the reliability, integrity and availability of data must be our prime concern rather than the confidentiality of events collected by the WSN. For this, we propose an adaptable security module depending on the criticality of messages spread on the network and the present risk (risk free environment or obvious peril due to malicious nodes). Our security module combines three approaches:

- Authentication
- Trust index
- Encryption.

4.1 Architecture Of Network

Since our Framework is in charge of managing the mobility and heterogeneity of sensors nodes regarding resources and type of information collected. In our approach, we adopt a hierarchical architecture such as cluster. For this, we segment the supervision area at a given number of cells and we assume that there is a probability at deployment that allows us to have a diversity of sensors in each cell. Given the heterogeneity of sensors, the role and participation of each node is related to its capacity, for example node with a high capacity computing, storage, and energy can be elected as cluster-head meanwhile those who have normal capacity are responsible for the detection and transmission of events to their cluster-head. Fig. 3 illustrates the architecture.

Journal of Theoretical and Applied Information Technology
31st January 2015. Vol.71 No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

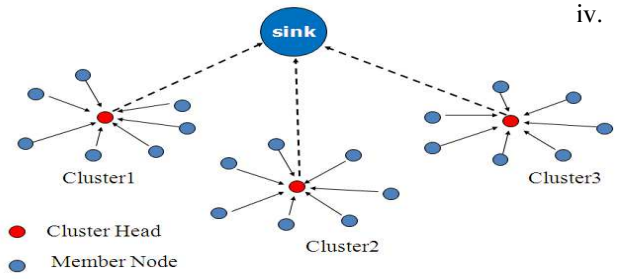

Figure 3: Architecture.

4.2 Authentication

In our framework we will provide authentication via the "MAC filtering" security sub-module. We propose to implement this sub-module at the managers nodes level (cluster-head and base station). Indeed, in the learning and organization phases, the manager node creates a whitelist where it stores all the MAC addresses of the allowed sensors. It also creates an empty blacklist that will be feed upon the detection of a malicious node, see Algorithm 1.

Algorithm 1:

The base station maintains a whitelist containing the MAC addresses of all approved nodes before their deployment.

a. In our hierarchical architecture (3-tiers: sensor node, cluster-head and base station). The security sub-module "MAC filtering" is enabled at cluster-head and at the base station level.
   i. During the clusters formation phase, all communications reach the base station in order to check that all MAC addresses are authenticated.
   ii. If an unauthorized MAC address is detected, the base station adds it to the blacklist and makes a broadcast to block this address in order to eliminate the possibility that the corresponding node is elected as cluster-head or being a member of a cluster.
   iii. After the election of cluster-head, it creates a whitelist for its members.
      1. The validation of this whitelist is made by the base station at the clusters formation phase (as indicated in i. and ii.).
      2. At the cluster level, the authentication of sensors is validated at the cluster-head.
   iv. When adding new sensors, their MAC addresses are recorded in the whitelist at the base station.

1. Before a cluster-head adds a new sensor in the list of its members, it reports the new MAC address to the base station for validation.
   a. If the base station does not validate this new MAC address, it adds it to its blacklist and makes a broadcast to block this sensor, and then the cluster-heads add this sensor in their blacklists.
   b. Otherwise, it is added by cluster-head in their whitelist.

Although authentication protects the network against attacks from outside, for example preventing unauthenticated node to inject packets but it can't solve the problem of compromised or failed nodes. Because, if a compromised node has the secret key of a legitimate node, it can authenticate itself to the network and inject, retrieve information or avoid its transmission. In addition, the sensors can be prone to malfunctions that may prevent them from functioning properly. To address these problems we can use trusted models which have shown their effectiveness in WSNs [10][21][22].

4.3 Trust Index

To further strengthen the reliability of the security approach based on MAC filtering, we propose to combine it with a method based on the trust index. Indeed, it allows for example the detection of a malicious node that impersonates a trusted node by spoofing its MAC address and therefore we choose another way that is more reliable to route data or enhance the security mechanism using encryption algorithms.

In our approach, the mechanism of trust that runs on managers nodes (cluster-head and the base station) is based on the event type. These nodes use the monitoring system "watchdog" to observe the behavior of nodes for different types of events and distribute their confidence indices. Each cluster-head maintains a table of confidence index of its members and the base station conserves a table of confidence index of cluster-heads. In our mechanism, a node has several values of confidence indices according to the results of past actions of each event type.

In this architecture, each node, by using the trust index calculated by the manager node (cluster-head or base station), knows the routing path and the

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

reputation of this path that the sent message take. This reputation of the routing paths is broadcast periodically by the node manager.

As a basic assumption, we assume that the confidence index of nodes is a value between 0 and 1 (0 for the lowest index and 1 for the highest index).

We also assume that the value of reputation routing path is determined by the node with the lowest confidence index on the routing path.

4.3.1 Adopted architecture for trust index

In the wireless sensor network, it is difficult to refer to a central authority for determining the confidence index of a sensor. For this, we propose a trusted system centralized at two levels. The first located within the cluster and managed by the cluster-head and the second is administered by the base station. Thus, the cluster-head handles confidence index for its members and the base station manages confidence index for different cluster-heads.

4.3.2 Type-based calculation of the confidence index

The types of events have already been mentioned in the classification and prioritization module of our Framework Ad-M-QoS-DS [7]. In our context of emergency management these types of events are:

- Normal Event
- Important Event
- Critical Event

In some cases, malicious nodes behave normally during the collection and transmission of data of normal type. As a result, they get to have a high-confidence index enabling them to cooperate with neighboring nodes. However, upon detection of an event of emergency, compromises sensors adopt malicious behavior. Gray-hole attack is a common example [23] which is an improved variant of the black-hole attack [24]. Therefore, neighboring nodes continue to cooperate with these malicious nodes because they have a fairly large confidence index. To counteract this, our index of confidence will be assigned to a node depending on the importance of event. This method has two major advantages:

- It makes difficult to attribute a high-confidence index to a node,
- It makes a node harmless since its confidence index will be falling during a wrong operation concerning an event classified as important or critical.

As for normal events even if they are not communicated, it will affect neither the proper functioning of the network nor compromises its safety compared to the danger that may present as explained above. Hence the importance of using a weighted arithmetic average of the confidence index giving more weight to the important and critical events.

The following formula is used to calculate the index of global confidence index by weighting each type:

$$Ig=w1.Inrl + w2.Iimp + w3.Icrtq \text{ with } w1 + w2 + w3 = 1$$

Ig: Global confidence index

Inrl: confidence index for normal events

Iimp: confidence index for important events

Icrtq: confidence index for critical events

w1, w2 and w3 are the weighting coefficients that can promote an event over other. In our context, we use w1 = 0.2, w2 = 0.3 and w3 = 0.5.

4.3.3 Risk levels definition

In our proposal, we define three levels of risk that a packet may incur during its delivery to its cluster-head and from the cluster-head to the base station. The risk level is strongly related to the confidence index node. We determine these levels by the value of the reputation of the routing path from the transmitting node to its manager node (cluster-head or base station). In this sense, we segment the range of reputation into three parts as follows: [0, a],] a, b] and] b, 1] corresponding to high, medium and low risk respectively with, $0 < a < b \leq 1$.

In our context, we propose a = 0.3 and b = 0.6.

The risk level helps make the decision on what type of data to be secured before their routing or to change the route if the risk level is high and to add the node with low trust index to the blacklist.

4.4 Adaptive Management Of Security Through Encryption

The use of cryptography to secure all communications in sensor networks poses serious problems such as consumption of bandwidth, latency caused by the CPU processing (loss of responsiveness of the network) and essentially the energy costs. Moreover, this implies that each node uses cryptography for each packet sent, even if it doesn't have a special importance nor strategic.

Journal of Theoretical and Applied Information Technology
31st January 2015. Vol.71 No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

This has a negative impact on the QoS level of our Framework.

So to reduce energy costs related to unnecessary encryption, we use a method that consists to define the type of messages to be encrypted based on the incurred risk. No encryption will be applied when the risk of capture of the message is null. This, allows to establish a balance between QoS and security according to severity and criticality of information

Thus, in our approach, the security management will be adaptive and combined with a two level centralized reputation system. The use of encryption will depend on the reputation of the path and the importance of information to be transmitted, which provides a gain of responsiveness and reduction of energy consumption.

4.4.1 Data types to encrypt

Passive monitoring attacks and analysis of control and reconfiguration messages are very dangerous for wireless sensor networks. Because the purpose of these types of attacks is to have a vision of the network architecture by determining the position of critical nodes such as manager nodes (cluster-head, aggregator nodes and the base station) and then attack them, causing a partial or total denial of service.

Then, it becomes essential to encrypt the control and reconfiguration messages. This is to reduce the risk of exposure of the network to the attacks and mask the internal network architecture in a hostile environment.

Therefore, the security events involved in our framework in the context of emergency management will be:

- Control messages,
- Reconfiguration messages,
- Critical events,

These events will be divided into two groups:

- Group A: events that will always be encrypted are:
  - Control messages
  - Reconfiguration messages
- Group B: events which will be encrypted if the level of risk is medium are:
  - Critical events

4.4.2 choosing the type of encryption keys

The use of secret key algorithms is desirable for this type of network as they consume less power than protocols based on public keys. However, the use of a single key makes the network more vulnerable because if only one node is compromised, the key of the entire network will be disclosed, and hence, an attacker can build relationships of trust with the remaining nodes without being detected [15][17].

In our context, we propose to adopt the approach of [16] which is a pre-deployed key protocol. It minimizes processing, communication overhead and storage generated during key management.

Thus, the messages which are limited within the cluster will be encrypted by the key that is shared with the cluster-head, while those who will reach the base station will be encrypted by the key that is shared with this latter. This, in order that the cluster-head and the base station can decrypt the messages intended for them.

4.5 Algorithm

As the reputation system used is centralized at two levels, each node (a cluster member) knows only the level of risk of the route taken to reach its cluster-head. And will therefore be able to determine what type of data requires a certain level of security before sending them to the cluster-head. Similarly, the cluster-head knows the risk level of the road taken to reach the base station through the latter that centralizes the management of the confidence index of the various cluster-heads.

But it may be that the choice used in a cluster is not appropriate to the level of risk involved in routing information from the cluster-head to the base station. Therefore, the security must be adapted as the message cross different areas. It is then possible that the cluster-head encrypts a message, unencrypted by the emitter, before relaying it to the base station. This message will be encrypted by the key that the cluster-head shares with the base station.

So in order to apply the appropriate security level, the source node must be able to determine the risk level and the type group of event that will be sent. In addition, to decrypt the messages received by the manager node, this latter must be able to determine which node encrypts the concerned messages. We can then distinguish three cases.

4.5.1 case 1: risk level is high

In this case, the node manager excludes the node that presents the high level risk and adds its MAC address in the blacklist in order to prevent the

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

communication with this node. Then, the source node chooses another way that presents a low or medium risk level.

4.5.2 Case 2: risk level is medium

In this case, if the message transmitted is belong to the group A or B, the source node encrypts these types of messages. Else, the message will be transmitted without encryption. And in order that the manager node can decrypt the intended message, this latter must know the address of the node sending the message, for this purpose, we use a message header as shown in Tab. 1, which allows us to store the address of this node.

16bits	1bit	1bit	Variable
Source node address	Encryption	Destination	Data

Table 1: Header Packet Structure

For addressing the Tab.1 the first 2 bytes are used to determine address of the sending node of the message, the next bit is used to determine if the message is encrypted or not as illustrated in Tab. 2. And the next bit identifies the recipient as presented in Tab. 3. The three tables below describe the possible values and their meaning.

Encryption bit value	Encryption
0	No encryption
1	Encryption

Table 2: Encryption Coding

Destination bit value	Destination
0	Cluster-head
1	Base Station

Table 3: Destination Coding

So there are three possibilities:

- If the encryption bit is set to 0: no encryption.
- If the encryption bit is set to 1 and if the first field of the address is an ordinary node's address: the message was encrypted by the sending node.
- If the encryption bit is set to 1 and if the first field is the address is a cluster-head's address: the message was encrypted at the cluster-head.

4.5.3 case 3: risk level is low

In this case, the source node encrypts only the messages belong to the group A and transmits all other without any encryption. We use also the same packet header in Tab. 1, used in the second case, in order to allow the manager node to decrypt the intended message.

5. CASE STUDY OF ASATE MODULE

The case study described below is a comparison of two scenarios. One uses a security module with total encryption and the other uses the ASATE module. Tab.4 shows the characteristics of the environment in which we make the comparison. We propose to deploy 64 sensor nodes and assume that this environment generates 1236 events with a probability of occurrence for each type of event. We also propose a number of intruding sensor nodes of around 5% and corrupted ones of around 5%.

Table 4: The Characteristics Of The Case Study Environment

Event number	1236		
Number of nodes	64		
Number of CH	6		
Intruding nodes (5%)	5% with message injection		
Corrupting nodes (5%)	5% with no transmitted message		
Events types	Normal	Important	Critical
Occurrence Probability	0,6	0,3	0,1

The probability of sending packets with different risk levels are shown in Tab.5.

Table 5: Risk Probabilities On Routes For Different Routes

Level	Low	Medium	High
Risk probability for the route between a node and CH	0,55	0,25	0,2
Risk probability for the route between a CH and the BS	0,55	0,25	0,2

Tab.6 shows the result of comparing the two scenarios. In the first scenario that uses a security

Journal of Theoretical and Applied Information Technology
31st January 2015. Vol.71 No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

module with static and total encryption, the fact that all messages, including control ones, were encrypted, has a negative impact on the network's life, delay and bandwidth and energy consumption. By contrast, our ASATE module only encrypts critical messages, when the road has a medium risk level, and control messages. That is to say, the number of encrypted messages is 10% multiplied by 25% which results in 2.5% of the sent messages from the source node to the Cluster Head, add to 7.5% multiplied by 25% which results in 1.87% of the sent messages from the Cluster Head to the Base Station plus control messages.

Moreover, our ASATE module has the advantage to allow adding corrupting and intruding sensor nodes to the blacklist and avoiding high-risk roads by adding sensors that have a confidence index lower than 0.3 to the same list.

scenario with total encryption module			scenario with ASATE module		
Encrypted message(%)	Message injected(%)	Nodes added to blacklist(%)	Encrypted message(%)	Message injected(%)	Nodes added to blacklist(%)
100% + control message	5%	0%	4.37% + control message	0%	5% (intruding nodes) + 5% (corrupting nodes) + nodes with a confidence index lower than 0.3

Table 6: comparison between ASATE and total encryption module

Our approach allows an effective use of the computing power, which reduces energy consumption and therefore extends the lifetime of a network.

6. INTEGRATING THE SECURITY MODULE WITH AD-M-QOS-DS FRAMEWORK

Using WSNs in the management of emergency situations require in addition to QoS assurance, an important level of security. The challenge with such requirements is doubled compared with the principle of providing only the security or guarantee the quality of service; because there is an explicit correlation between the quality of service and security.

In [7] we identified five modules in order to provide a good QoS management in emergency situations. Integrating any module of security with our framework presents some challenges. Indeed, the cryptography approach has a negative effect of bandwidth, delay caused by CPU processing (encryption and decryption) and a high energy cost. In the same sense, both completely centralized and distributed trust index schemes are expensive in terms of energy cost especially for a large scale network due to extra routing overhead and to limitation memory of sensor node to store the database of trust values. For this reason, we take into account these challenges when designing our security module ASATE which is based on hybrid trust index scheme, in order to minimize the routing overhead and the size of the database, combined with an adaptive encryption approach. Indeed, both secure communications and QoS are the most important keys to enhance the rescue operations and save life.

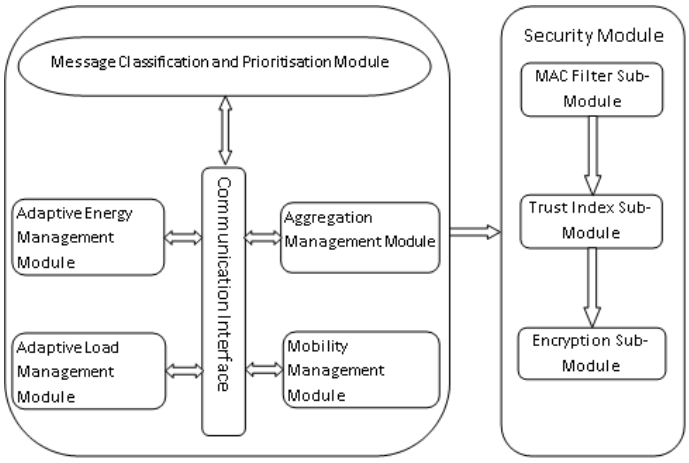

Figure 4: Secure Framework Ad-M-QoS-DS with ASATE.

Fig. 4 illustrate diagram that combines the Ad-M-QOS-DS framework and Security modules to meet the requirement of efficient rescue operations.

The main objective of ASATE module is to guarantee the security and the reliability of the sensor network by encryption and excluding malicious and faulty nodes from the network.

7. CONCLUSION

In this paper, we present our contribution to ensure the security of our Framework G-Ad-QoS-

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

DS. Because, both secure communications and QoS are the most important keys to enhance the rescue operations and save life. We take into account the characteristics of WNS such as the consumption of bandwidth, latency caused by the processing at CPU (loss network responsiveness) and especially the energy cost which could have a negative impact on QoS.

This contribution provides an adaptable security module ASATE according to the importance of circulated messages on the network and the existing risk. Our security module combines three approaches: authentication, trust index and cryptography. We also define the types of data that requires encryption to establish a compromise between QoS and security according to the severity and the criticality of the information.

Our future work consists on improving and optimizing the security module offered and evaluating it by simulations and measurements.

REFRENCES:

[1] N. Dimakis, A. Filippopoulitis, and E. Gelenbe, "*Distributed building evacuation simulator for smart emergency management*," The Computer Journal, 2010, doi: 10.1093/comjnl/bxq012.

[2] A. Filippoupolitis, L. Hey, G. Loukas, E. Gelenbe, and S. Timotheou, "*Emergency response simulation using wireless sensor networks*," in Ambi-Sys '08: Proceedings of the 1st international conference on Ambient media and systems, 2008.

[3] A. Ko and H.Y.K. Lau, "*Robot Assisted Emergency Search and Rescue System With a Wireless Sensor Network*", International Journal of Advanced Science and Technology, Vol.3., Feb., 2009

[4] M. Jafarian and M. Jaseemuddin, "*Routing of Emergency Data in a Wireless Sensor Network for Mines* ", Proceedings in the ICC 2008. IEEE Comm, pp.2813–2818, 2008.

[5] D Krishna Chaitanya, and G Arindam (2010) ''*Analysis of Denial-of-Service attacks on Wireless Sensor Networks Using Simulation*'' Middlesex University, 1-13.

[6] A. D. Wood, and J. A. Stankovic, ''*A Taxonomy for Denial-of-Service Attacks in Wireless Sensor Networks*'', Handbook of Sensor Networks: Compact Wireless and Wired Sensing Systems, CRC Press, 2004 (invited chapter)

[7] R. Haji, A. Hasbi, M. Ghallali, and B. El Ouahidi. ''*Designing an Adaptive QoS-Oriented and Secure Framework for Wireless Sensor Networks in Emergency Situation*,'' Journal of Theoretical and Applied Information Technology. 15 August 2012. Vol. 42 No.1. © 2005 - 2012 JATIT & LLS. All rights reserved. ISSN: 1992-8645.

[8] P Guo, J Wang, J Zhu, Y Cheng ''*Authentication Mechanism on Wireless Sensor Networks: A Survey*'' Onlinepresent.org, proceedings, vol25, 2013

[9] V. Uma Rani, K. Soma Sundaram, '' *Review of Trust Models in Wireless Sensor Networks*'', International Journal of Computer, Information, Systems and Control Engineering Vol:8 No:2, 2014. World Academy of Science, Engineering and Technology.

[10] S. Ganeriwal and M. B. Srivastava, "*Reputation-based Framework for High Integrity Sensor Networks*", ACM Transactions on Sensor Network, Vol. 4, No. 3, Article 15, May 2008.

[11] M. Momani and S. Challa, "*GTRSSN: Gaussian Trust and Reputation System for Sensor Networks*", in International Joint Conferences on Computer, Information, and Systems Sciences, and Engineering (CISSE '07), University of Bridgeport 2007.

[12] A. Jøsang and R. Ismail, "*The Beta Reputation System*," in 15th Bled Electronic Commerce Conference. Bled, Slovenia, 2002.

[13] Boukerche A, Xu L, El-Khatib K. ''*Trust-based security for wireless ad hoc and sensor networks.*'' Computer Communications 2007;30(11–12):2413–27

[14] R. A. Shaikh, H. Jameel, S. Lee, S. Rajput and Y. J. Song, "*Trust Management Problem in Distributed Wireless Sensor Networks*", in The 12th IEEE international conference on Embedded and Real-Time Computing Systems and Applications (RTCSA '06), pp 411-414, 2006.

[15] D.W. Carman, P.S. Kruus and B.J. Matt, ''*Constraints and approaches for distributed sensor network security*'', NAI Labs Technical Report No. 00- 010 (2002).

[16] Jolly G., Kuscu M.C., Kokate P., and Younis M., "*A Low-Energy Key Management Protocol for Wireless Sensor Networks*", Proc. Eighth IEEE International Symposium on Computers and Communication, 2003. (ISCC 2003). vol.1, pp. 335 - 340.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[17] A.-S. K. Pathan, ''*Security of Self-Organizing Networks: MANET, WSN, WMN, VANET.*'', ISBN: 978-1-4398-1919-7, Auerbach Publications, CRC Press, Taylor and Francis Group, USA, 2010.

[18] Huang, Q., Cukier, J., Kobayashi, H., Liu, B., and Zhang, J., ''*Fast authenticated key establishment protocols for self-organizing sensor networks*'', in Proceedings of the 2nd ACM international Conference on Wireless Sensor Networks and Applications (San Diego, CA, USA, September 19–19, 2003). WSNA '03. ACM Press, New York, NY, pp. 141–150, 2003. http://doi.acm.org/10.1145/941350.941371.

[19] Kotzanikolaou, P., Magkos, E., Vergados, D., and Stefanidakis, M., ''*Secure and practical key establishment for distributed sensor networks*'', in Security and Communication Networks,Wiley InterScience, NJ, USA, 2009. http://dx.doi.org/10.1002/sec.102.

[20] Shaikh, R. A., Lee, S., Khan, M. A. U., and Song,Y. J., ''*LSec: Lightweight security protocol for distributed wireless sensor network*'', in 11th IFIP International Conference on Personal Wireless Communications, LNCS 4217, (pp. 367–377), Albacete, Spain: Springer-Verlag, 2006.

[21] A. Srinivasan, J. Teitelbaum and J. Wu, "*DRBTS: Distributed Reputation-based Beacon Trust System*", in The 2nd IEEE International Symposium on Dependable, Autonomic and Secure Computing (DASC '06), 2006.

[22] Zahariadis T, Leligou H, Trakadas P, Voliotis S. ''*Trust management in wireless sensor Networks*'', European Transaction on Telecommunications Vol. 21, (4), 2010, pp: 386--395.

[23] Chris Karlof and David Wagner. ''*Secure routing in wireless sensor networks: attacks and countermeasures*''. Ad Hoc Networks, 1(2-3):293–315, 2003.

[24] N. Ahmed, S. S. Kanhere, et S. Jha, ''*The holes problem in wireless sensor networks: a survey*'' SIGMOBILE Mob. Comput. Commun. Rev., vol. 9, no 2, p. 4–18, 2005.