Journal of Theoretical and Applied Information Technology
15 August 2012. Vol. 42 No.1

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

DESIGNING AN ADAPTIVE QOS-ORIENTED AND SECURE FRAMEWORK FOR WIRELESS SENSOR NETWORKS IN EMERGENCY SITUATION

[1]RACHID HAJI, [2]MOHAMED GHALLALI, [1]ABDERRAHIM HASBI, [2]BOUABID EL OUAHIDI

[1]Network Team and Intelligent Systems Laboratory

Mohammed V University, Mohammadia School of Engineering

Rabat, Morocco

[2]Data Mining and Network Laboratory

Mohammed V University, Faculty of Sciences

Rabat, Morocco

[1] rachaji@gmail.com ; hasbi@emi.ac.ma

[2] ghallali@finances.gov.ma ; ouahidi@fsr.ac.ma

ABSTRACT

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. In such cases, the information availability, reliability, security and delay of its delivery are critical to the success of rescue operations. In this paper we design a new Framework Ad-M-QoS-DS (Adaptive Management of QoS in different situations) that permits an adaptive management according to the QoS requirements of each situation in the supervised area by grouping multiple modules and parameters. Next, we have proposed a Sensor Security Module (SSM) for our Framework to dispute sensor security challenges and describe the role of its components. At the end of the paper, we implement the proposed Module within the Base Station (BS).

Keywords: *Emergency situations; Wireless Sensor Networks; QoS; Sensor security; Energy; Mobility*

1. INTRODUCTION:

An emergency situation can be caused either by a natural event or man-made and can occur in various ways such as fire, flood, tsunami, earthquake, terrorist attack (a nuclear attack, attack by toxic gas), etc. Such emergencies cause a dangerous and hostile environment characterized by lack of information or difficult access to it. 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.

The use of WSN is becoming more important in several domains including emergency management. Communications in such situations must be reliable and have low latency taking into account the mobility and the efficiency of energy consumption. The mechanisms and QoS models proposed for traditional networks and ad-hoc networks are not suitable for wireless sensor networks given their unique characteristics: The (limited) resources constraints (energy, memory, processing capacity, etc.), many-to-one and multi-hop communication, … [5]. For these reasons, several works were conducted on the study of QoS management in WSN [6][7][8]. However, most of these works deal with QoS in a given situation and focus on one or two parameters such as energy, delay or reliability. Reference [9] presents an approach of data routing based on priority; it provides a Framework for an adaptive routing protocol that defines two paths to transmit data according to their priority. Reference

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

[10] uses an architecture similar to that of a cluster with differentiation of the roles of nodes to minimize energy consumption while communicating in real time and ensure a defined level of QoS.

In this paper, we propose a framework for Adaptive Management of QoS in different situations (Ad-M-QoS-DS) that 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.

The rest of this paper is organized as follows: in section 2, the related work of QoS and security of WSN is presented. Section 3 describes the proposed framework in two subsections by presenting its workflow and discussing its different components. Security modules are proposed and implemented in section 4. Finally, we conclude the paper and present future work in section 5.

2. RELATED WORK:

A. QoS in WSN:

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 QoS. Indeed, communication must be reliable and have low latency. It should take into account the mobility and the optimization of energy consumption. Many works deal with this challenge, [11] present an assured corridor mechanism (ACM assured corridor mechanism) in order to minimize delays and ensure the reliability of transmission under critical conditions. The ACM is implemented regardless of the type of routing protocol and MAC protocol. It tries to create a secured tunnel between the source node that detects the event and the base station by sleeping nodes surrounding the tunnel to avoid collisions and keeping the nodes within the tunnel in standby state to eliminate the transition time from one state to another. [12] Presents an algorithm called PEQ (Periodic, Event-Driven and Query-Based Protocol) that provides fault tolerance and a minimum time (low latency). PEQ is a routing algorithm, which is realized in three steps. The first step comprises the construction of the hop tree. The sink starts the process of building the hop tree, which will be used as a configuration and subscription message propagation mechanism to the sensor network. The second step involves the propagation of subscriptions to the sensor network. Finally, the last step is responsible for delivering events from the sensors to the sink, by using the fastest and less costly route, in terms of energy savings. [13] Presents a platform for mission-critical management which integrates WSNs, unmanned aerial vehicles (UAVs), and actuators into a disaster response setting. The authors focus in the paper on dynamic networking under mobility conditions. For this purpose, they propose a new reliable cost-based data-centric routing algorithm (RCDR) to deal with the dynamics of WSNs. The RCDR algorithm proposes a global gradient paradigm. In order to set up a global gradient in the entire network, the sink sends out a data query when it wants to collect data from the network. To deal with the constraint of mobility and to minimize the effect of reflooding which takes a lot of energy in the network, the authors propose two schemes to efficiently resume the disrupted global gradient by local interactions between sensors: the sensor movement adjustment scheme and sink movement compensation scheme. Reference [9] presents a Framework for adaptive routing protocol which utilizes an approach of data routing based on priority; the Framework defines two paths to transmit data according to their priority. it presents an enhanced version of Ad hoc On-Demand Distance Vector Routing (AODV) in order to discover and maintain the shortest path and therefore well performs delay, in the other hand, it utilizes an ant-based protocol to construct an energy-efficiency path in order to minimize the energy consumption.

B. Security in WSN:

The WSN present much inherent vulnerability that increases the security risks. The low-cost and low-power of the WSN devices make them incapable of supporting usual and adequate security tools to prevent them from undergoing several types of threats, especially DOS attacks, that aim essentially for increasing their energy consumption, to block their availability to the users [14], compromising this way the reception of supposedly critical data, or even drain them of their already low power supply, sometimes irreplaceable. Therefore, WSN demand efficient and effective security mechanisms to be protected from this hazardous threat, while taking under consideration WSN restraints like limited resources and energy,

Journal of Theoretical and Applied Information Technology
15 August 2012. Vol. 42 No.1

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

inaccessibility, the large number of devices (sensors) [15]. On the other side, we mustn't neglect also the limitless resources that can be used by the attackers to exert more effective, concentrated, and successful DOS attacks, and the more WSN networks evolve, they become more pervasive and accessible, allowing these threats to become also more outstanding, and improved[15].

3. DESIGNING A NEW FRAMEWORK FOR ADAPTIVE QOS AD-M-QOS-DS:

In this section, we will present the workflow of our framework, describe in detail its main components and illustrate a scenario of intercommunication between the different components of Framework.

A. WORKFLOW of Ad-M-QoS-DS:

Rescue operators are assumed to be equipped with sophisticated sensors and can communicate directly with the base station. Upon detection of an event, sensors transmit the information on multi-hop to the base station which is responsible for transmitting them to the Coordination Committee. The latter analyzes the information received. If the event is safe, the data will be stored in a database and if the event presents a danger the Committee takes appropriate decisions and informs the operators on the appropriate actions. Fig. 1 illustrates the workflow of our Framework.

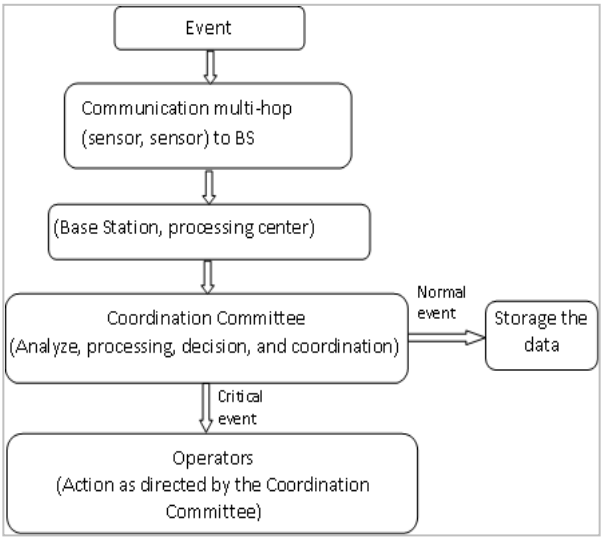


Figure 1: WorkFlow of the Framework.

B. Components of the Ad-M-QoS-DS FrameWork:

In this section, Fig. 2 presents the different modules of our Framework that are necessary for the proper management of rescue operations and cooperation during a disaster.

Message Classification and Prioritization Module: In monitoring environment application of eventual emergency and in the emergency situation, we should supervise different events and control their level risk. To do this, we propose the message classification and prioritization module that acts as an arbiter between the different types of messages. It classifies messages according to the nature of events: temperature, pressure, gas, beating of the heart [5]. This module also defines three levels of priority for each class [16]: normal, important and critical (see Tab. 1). According to this matrix, the Framework adjusts its behavior to ensure the level of QoS required for each event. We will implement this module in the application layer it will add in the header of packet the information about the type of event and its priority level. Indeed, the framework prioritize packet with high criticality. It adopts a FIFO approach for packets with the same level of priority. This information will be helpful in routing layer in order to meet the required level of QoS.

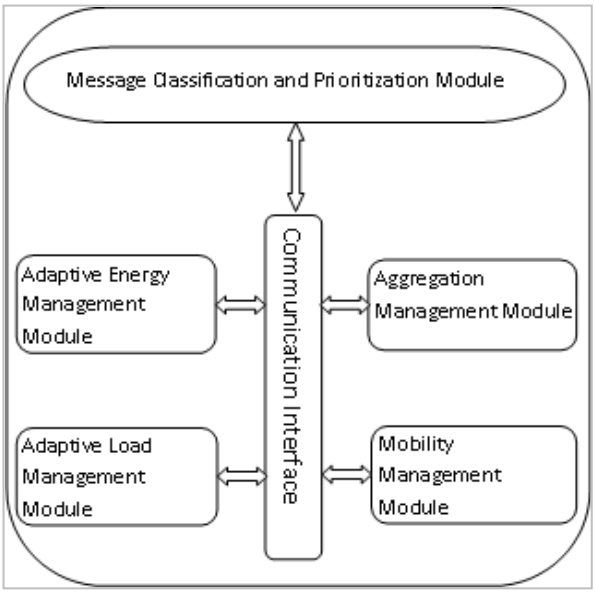


Figure 2: Framework Ad-M-QoS-DS.

Table 1: Classification and priority matrix.

	Temperature	*Pressure*	*Gas*	*Heart beat*
Normal	TN	PN	GN	BCN
Important	TI	PI	GI	BCI
Critical	TC	PC	GC	BCC

Journal of Theoretical and Applied Information Technology
15 August 2012. Vol. 42 No.1

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

TN, TI, TC : temperature thresholds.
PN, PI, PC : pressure thresholds.
GN, GI, GC : gas thresholds.
BCN, BCI, BCC : heart beat thresholds.

Aggregation Management Module: In different scenarios of applications of WSN, many sensors can detect the same event at the same area and all of them try to send this information to the sink [Figure. 3], this case generates many traffic in the network, thereby the bandwidth and energy will be much solicited. But the WSN are characterized by their resources constraints and given that the communication cost in terms of energy is greater than the processing cost [Figure. 4] so the proposed framework should implement an aggregation technique in order to reserve energy and bandwidth [17]. The aggregation process has a positive impact on energy and bandwidth but it has a negative impact on delay and reliability [18] [19]. The aggregation management module determines according to the matrix Tab. 1 defined in the previous module and QoS level required, which type of message will be the subject of the aggregation process and with what degree. For example in a normal situation when a sensor detects an event, this module allows the framework to apply the adopted aggregation technique for this type of packets, and in case of an important situation, the framework applies the aggregation process for this type of event but with a different degree from the first one (e.g., the number of packets to aggregate, the period of waiting packets...) but in the emergency situation the packets of this event will label it as non-aggregate data and will follow the shortest path and given the duplicated packets the information will be more reliable.

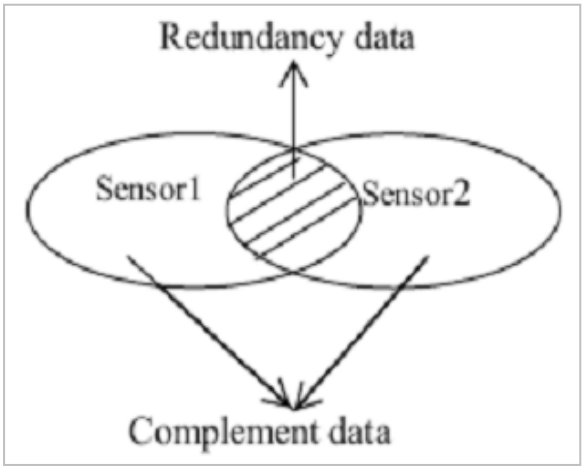
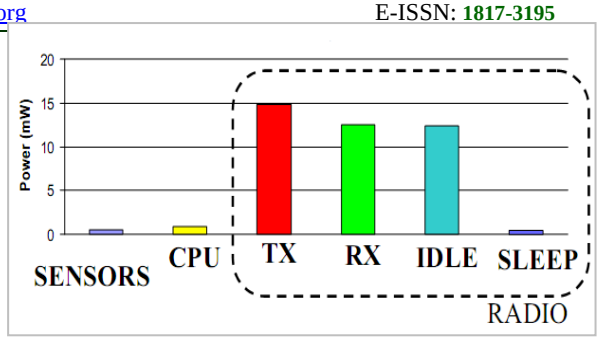


Figure 3: Sensors region overlapping.



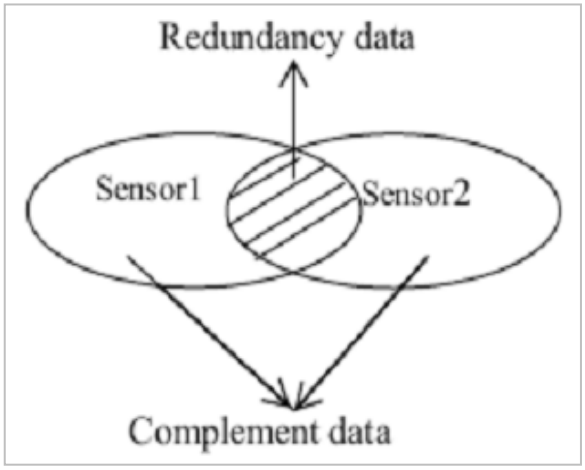


Figure.4: Power consumption of node subsystems [20]

Adaptive Energy Management Module: This module focuses on power management throughout the lifetime of the network. It guarantees the coverage of the monitored area and increases the lifetime of the network. There are several works that studied energy management but most of these works were limited to a specific situation [21] [22] [23]. This module of the proposed Framework has the advantage of supporting power management in different situations (Normal, important, and critical situations). This module can implement the technical threshold of energy for participation in the communication and transfer of information [24]. Our contribution is to make the threshold adaptive .i.e., the threshold of participation will be changed in our proposed mechanism according to the situation and the requested level of QoS. This module will benefit from aggregation module which has a positive impact on energy.

Adaptive Load Management Module: Generally the traffic in WSN passes through a large number of nodes to a small subset of nodes called base stations. This constraint leads to an overload of the most requested nodes near the base station (BS) and

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

consequently an interruption of flow to the BS [25] [26]. Hence the need to integrate this module in our framework. The mechanism of the adaptive load management that we provide allows balancing the load between all adjacent nodes to the base station to avoid any interruption of flow. With this module the Framework decides to drop the packets of a neighbor or to transmit them according to the following criteria: The matrix defined in the first module, the QoS level required, and the ability of the node in terms of energy and transmission.

Mobility Management Module: In case of a disaster, when nodes may fail and links may become unavailable, new sensors can be added to the network (Rescue operators equipped with sensors, new sensor deployment, etc). This leads to a very dynamic topology. All these constraints push us to integrate in our Framework a mobility management module to ensure the coverage and the optimization of energy consumption [13] [27]. This module should deal with the challenges imposed by the mobility of nodes in WSN, including the challenges associated with data aggregation in sensor network and the challenges of the design of routing protocols.

C. Framework components intra-communication:

In this section we present how our framework Ad-M-QoS-DS will perform their actions. In the first time when a sensor detects an event the first module in framework takes action by classifying and prioritizing the event by adding two prioritization bits in the packet (as we mentioned above the framework adopts, in his first version, the FIFO approach for different type of events having the same criticality). In the output of this module, packets will be differentiated according to their priority: normal, important or critical.

This differentiation of packets allows the aggregation module to choose what mechanism will be used to perform in-network data aggregation and take into consideration the latency-constrained data. In this module we propose to use tree-based aggregation approaches rather than gossip-based aggregation because the first approach have better performance and energy-saving characteristics [28]. When the priority of packet is normal, we propose to use an aggregation scheme that strives to save sensor's energy without considering delay of data such as the protocol proposed by [29], the authors compare this protocol through simulation with ESPAN (energy-aware spanning tree algorithm) and LPT for data aggregation (Lifetime-Preserving Tree) and show that has better performance in terms of energy saving and number of failed nodes which increases the network lifetime. When the priority of packet is important, in this case the aggregation scheme that will be used should be delay-constraint. Thus we propose to use the algorithm presented in [30], the algorithm perform through simulation a balance between energy consumption and timeliness level. When the priority of packet is critical, it won't be subject to any aggregation mechanism and will follow the shortest path and given the duplicated packets the information will be more reliable.

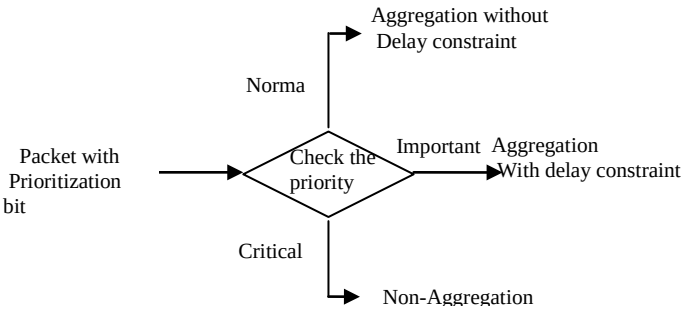


Figure 5: Diagram of Aggregation module.

The energy module keeps an open eye on the energy level of each node along the network lifetime; it defines three thresholds of participation in processes of communication depending on the degree of priority of packets. The energy and aggregation modules guarantee for our framework a good rationalization of energy consumption and therefore the maximal possible energy saving.

The adaptive load management module will be activated in some nodes especially in the neighbors of base station or sink to prevent the interruption of flows. This module communicates implicitly with the classification and prioritization module by exploiting the priority of the packets and communicates also with the energy module in order to compare the residual energy with the various thresholds defined by the later. This module allows the framework to make the decision to delete or forward the packets according to several parameters: the priority bits of the packet, the residual energy of node and the thresholds defined by the energy module.

After those steps, WSN must also provide communication with confidentiality, data integrity, and availability of service [31]. Thereby, those networks must benefit from a high level security, especially when implemented on vital domains,

Journal of Theoretical and Applied Information Technology
15 August 2012. Vol. 42 No.1

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

such as military or anti-terrorism, where they can be subject to hackers' attacks, aiming for information misleading or network paralysis, namely denial of service (DoS) attacks, considered one of the most effective against WSN as indicated in [32] [33] [34]. However, due to power and performance constraints, those networks can't afford to use conventional security protocols and mechanisms. Therefore, we will implement a security module adapted to those limitations, and effective enough to counter most threats targeting the network.

4. SECURITY OF FRAMEWORK AD-M-QOS-DS:

In this step, we need a comprehensive and central module for our framework [35] which meets the following aims:

- Applying the Security Policy with low resources (energy, CPU, Memory),
- Awareness of sensor ,
- Applying the best practices on sensor security,
- Establish a system of control on several levels: (layer2, layer3, data and application level),
- Allowing an automatic update of security patches,
- Having a warning system in real time,
- Testing the sensor security through a periodic audit or a vulnerability scan.

To meet these requirements based on the security supplied by BS, we present the Sensor Security Module (SSM) for our framework Ad-M-QoS-DS.

A. Designing a Sensor Security Module (SSM):

For better security against the risk of DOS attacks, and to meet the challenges previously mentioned, we will propose a new security module that we called: Sensor Security Module (SSM).

This module (SSM) consists of four sub-modules; it will be displayed as following:

- Strategy & Policies:

This module will generate the set of Sensor security policies and implement security policies to be applied in the Base Station (for all sensors). By following the standards and best practices, this module aims to reduce risk of Deny of Service attacks.

- Sensor Security & Integrity Control:

This module is the core of this proposed module. It is presented in the following diagram in four parts.

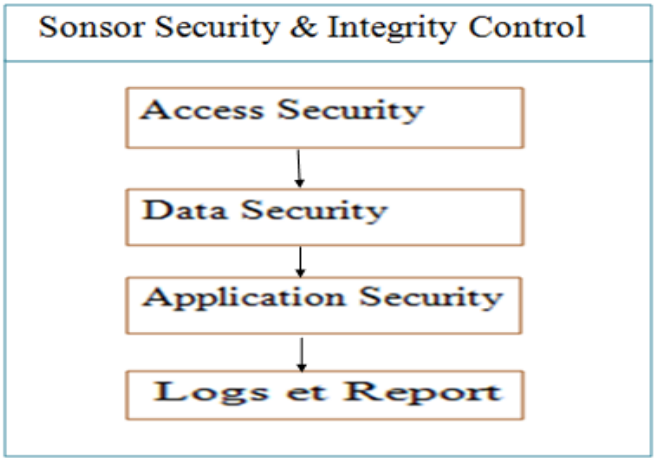


Figure 6. Central Module of SSM.

Access Security:

This module deals with the security applied during the access step, using level 2 filter (MAC address filter for sensors) and level 3 filter (IP Access-List) for allowing access for trust sensor only.

Data Security:

This function can be provided in the Base Station; it enables encryption of critical data during the transfer (Figure. 8), plus a backup / restore for critical data of sensor.

Application Security:

This module is the most interesting (Figure 9); it can detect and eliminate, in real time, the spread of untrusted data for all sensors. This can be done at this level with an application firewall in order to filter all traffic entering or leaving the sensor base station.

In addition, authentication and authorization systems allow limited access to the Sensor device via a strong password. It also allows an automatic disconnection in case of non-use (Timeout) in order to block the DOS attacks.

The vulnerabilities scan is used in this module to allow access to legitimate data only. Non legitimate

Journal of Theoretical and Applied Information Technology
15 August 2012. Vol. 42 No.1

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

access will be dropped in this module, and an Alert will be sent to the Alert System (Figure 9).

Log & Report:

The function of the traceability of all activities between sensors to know the safety level of each sensor devices. This operation is performed through the private and reserved area of Base station gateway.

This feature will allow the gateway to better know the nature and frequency of sensors malwares by region and by period.

- Security Audit:

Based on a security audit report generated periodically, the BS performs a quick scan of each sensor during the phase of low activity. The audit module is supported by a vulnerability test requested manually by security manager in the BS.

- Alert System:

This is the last module of the proposed SSM. The Base Station will notify the security administrator of the risks associated with the existence of attacks.

In this module, the manager of the base station will be informed, in real-time, about the security status of each sensor.

An SMS or an e-mail will be sent directly by the Base Station when any security problem occurs.

Finally, we propose the overall pattern of SSM which brings together the four modules mentioned above.

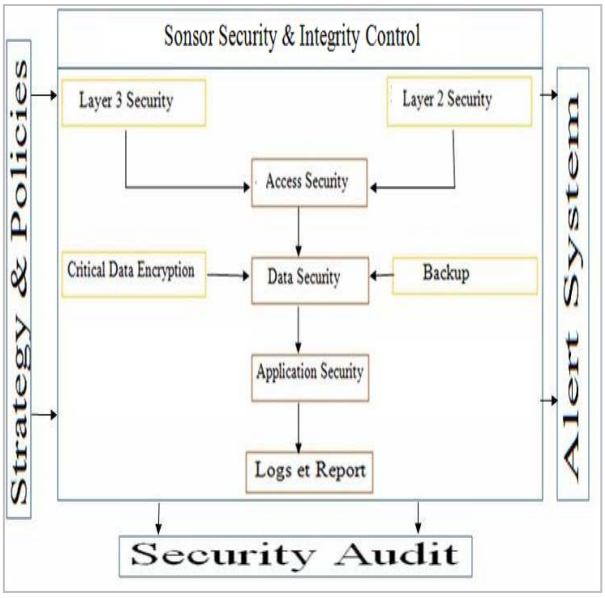


Figure 7.A proposed SSM.

B. Sensor Security Module implementing:

To ensure the safety of the Sensor device, we propose a security solution installed completely within the local network of base station Gateway.

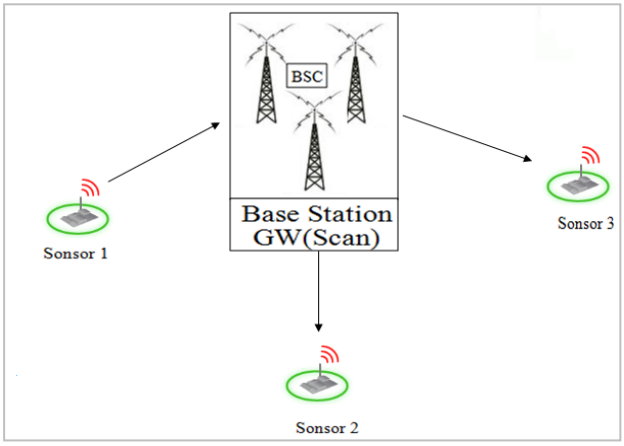


Figure 8.A central gateway for sonsor communication [20].

All those data can be scanned and disinfected inside the gateway, using its security module: firewall and Intrusion Prevention system (IPS) [36].

A black listed Sensors device was rejected before this applicative scan on the basis of its MAC address or its IP address in the Access Security Module (Figure 6).

For a better efficiency, this solution can be generated between two redundant Base Stations in order to limit the security risk, and to insure a High Availability (HA) solution.

The security gateway will contain all the necessary security elements (redundant Firewalls, Sensor Intrusion Detection / Prevention System, Vulnerabilities Test..) to block the spread of malicious programs and to stop the DOS attacks.

The following diagram describes the global the features of the SSM once implemented at the Base station gateway.

Journal of Theoretical and Applied Information Technology
15 August 2012. Vol. 42 No.1

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

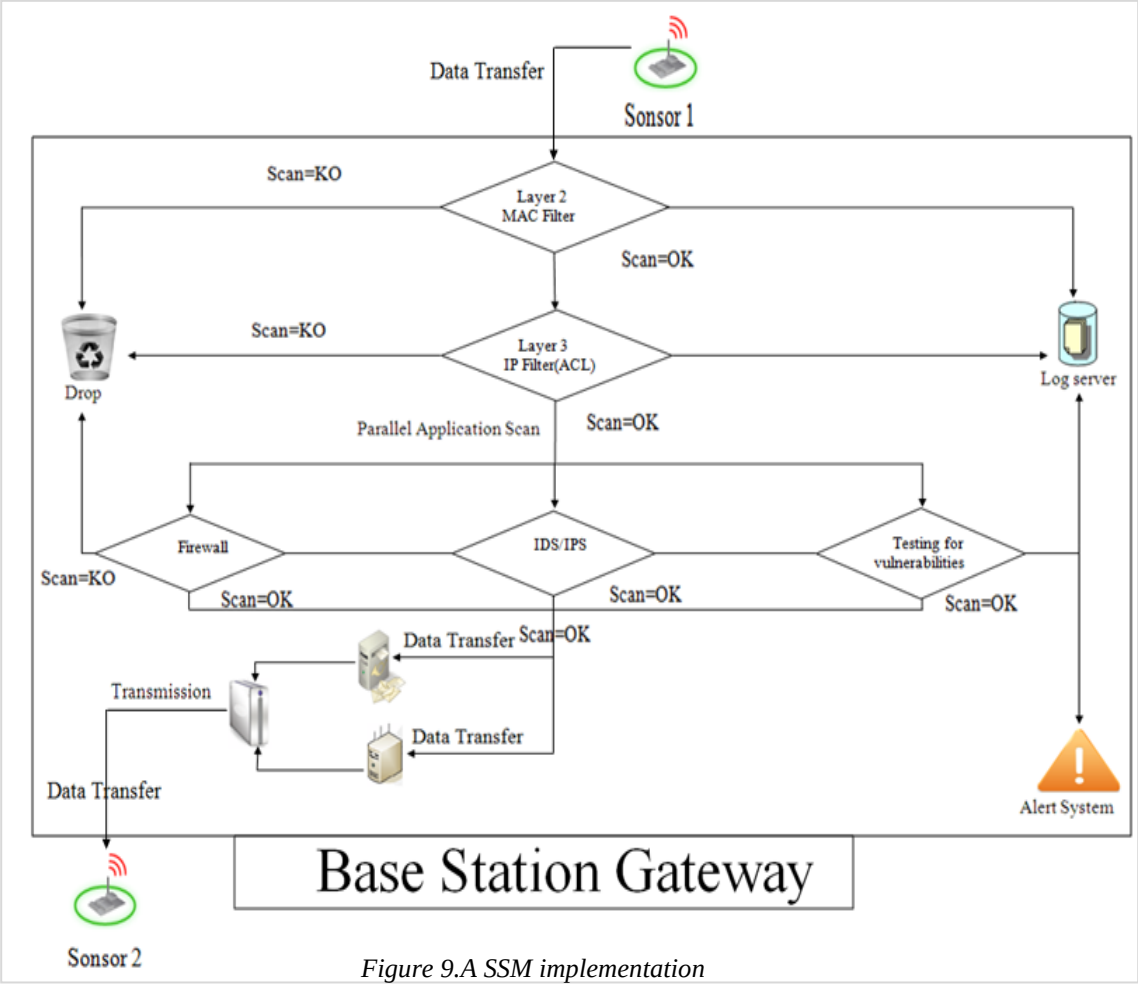


Figure 9.A SSM implementation

When a seonsor1 sends data, the gateway performs three tests (Figure 9):

1. Layer 2 scan: if the MAC address of the sonsor1 is allowed by this level, the frame moves to step 2. Otherwise, the frame will be dropped and a log message will be sent to log server for traceability and reporting.

2. Layer 3 Scan: in this ACL Scan, only the granted IP address passed for the next step.

3. Parallel Applicative scan: to reduce the scan time, a parallel scan will be done by firewall scan, antimalware detection, DOS attack scan, authentication of sensor. In each attack detected, a warning system is notified.

After successfully completing these three levels of scans, the data will be accepted for delivery to the server inside the Base station.

The use of this central solution based on Base Station security services gives a self and an optimal protection for the sensor devices. No security program will be installed in these Sensor devices: the full scan is done by the Base Station.

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

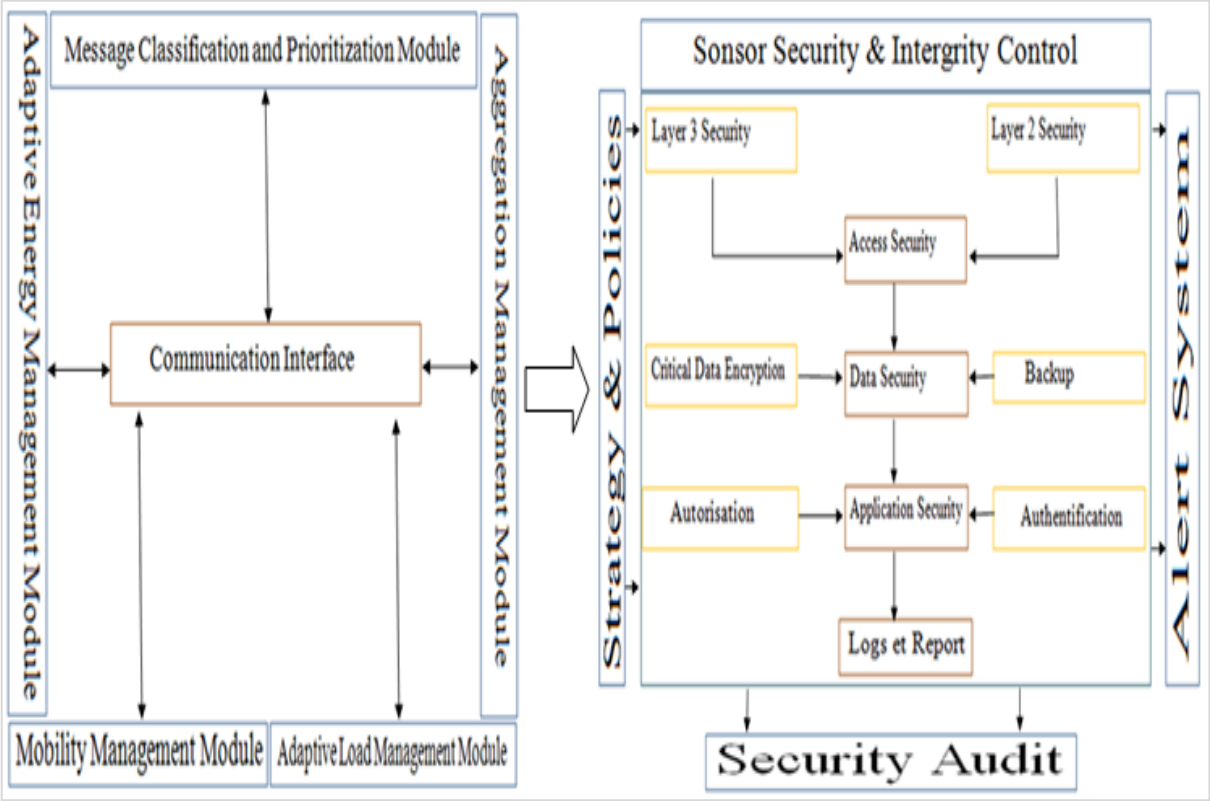


Figure 10: Secure Framework Ad-M-QoS-DS.

This diagram combines the QoS and Security modules to meet the requirement of efficient rescue operations. As we mentioned above the security enhance the energy consumption by blocking DoS attack and the In emergency cases both secure communications and QoS are the most important keys to enhance the rescue operations and save life (Figure 10).

5. CONCLUSION:

In this paper, we proposed a new framework for better use of WSNs in the management of emergencies. Indeed, we described the workflow of our Framework in both normal and emergency situations; then we explained the different modules that allow the Framework to meet the needs in terms of QoS and improve it in order for the rescue operation to succeed.

A new SSM was proposed and implemented in the Base Station to provider and enveloping a full scan against all DOS attacks.

For a maximum security of WSN: we plan to explore this further in our future work, thorough a unique solution for sensor device vulnerabilities scanning and testing.

The vulnerability test offered by the Base Station after the Sensor agent security request will be the subject of a future work in which we are aiming to prepare a complete diagram with redundant firewalls, intrusion detection, vulnerability test, to test and measure the degree of infections and their impact on the resources consumption upon the scan process.

Our future work consists, also, on improving and optimizing the QoS modules offered and evaluating them 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

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

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. Chen and P.K. Varshney , "*QoS Support in Wireless Sensor Networks: A Survey*," Proc. Int'l Conf. Wireless Networks (ICWN 04), CSREA Press, 2004, pp. 227-233.

[6] Y.J. Li; C.S. Chen; Y.-Q. Song; Z. Wang, "*Real-time QoS support in wireless sensor networks: a survey* ", In Proc of 7th IFAC Int Conf on Fieldbuses & Networks in Industrial & Embedded Systems (FeT'07), Toulouse, France, Nov. 2007.

[7] T. Kawai, N. Wakamiya, and M. Murata, "*ACM : A transmission mechanism for urgent sensor information*," in Proceedings of IPCCC 2007, New Orleans, Louisiana, USA, April 2007, pp. 562–569.

[8] A. Boukerche, R. W. N. Pazzi, and R. B. Araujo, "*A fast and reliable protocol for Wireless sensor networks in critical conditions monitoring applications*," In Proc. Of ACM Int'l Symp. On Modeling, Analysis and Simulation of Wireless and Mobile Systems (MSWiM), 2004.

[9] S. Sharma and D. Kumar,"*An approach to optimize adaptive Routing Framework to provide QOS in Wireless Sensor Networks*',International Journal of wireless Networks and Communication,Volume 1,Number 1,2009. pp;55-69

[10] E. Toscano, O. Mirabella, L. Lo Bello, "*An Energy-Efficient Real-Time Communication Framework for Wireless Sensor Networks"*, the 6th International Workshop on Real-Time Networks (RTN'07) in conjunction with the 19th Euromicro International Conference on Real-Time Systems (ECRTS'07), Pisa, June 2007.

[11] T. Kawai, N. Wakamiya, and M. Murata. ACM: A transmission mechanism for urgent sensor information. In Proceedings of IEEE IPCCC 2007, pages 562–569, New Orleans, Louisiana, USA, April 2007.

[12] A. Boukerche, R. W. N. Pazzi, R. B. Araujo, A fast and reliable protocol for wireless sensor networks in critical conditions monitoring applications, MSWiM'04: Proceedings of the 7th ACM International Symposiumon Modeling, Analysis and Simulation of Wireless and Mobile Systems, ACM Press, New York, NY, USA, 2004, pp. 157–164.

[13] A.T. Erman, L. Hoesel, P. Havinga, "*Enabling Mobility in Heterogeneous Wireless Sensor Networks Cooperating with UAVs for Mission-Critical Management*", IEEE Wireless Communications, vol. 15, is. 6, p. 38-46, 2008.

[14] Analysis of Denial-of-Service attacks on Wireless Sensor Networks Using Simulation by Doddapaneni.krishna Chaitanya, 2Ghosh.Arindam.

[15] A Taxonomy for Denial-of-Service Attacks inWireless Sensor Networks by Anthony D. Wood and John A. Stankovic

[16] B. Deb, S. Bhatnagar, and B. Nath. ReInForM: Reliable information forwarding using multiple paths in sensor networks. In Proceedings of LCN 2003, pages 406–415, Bonn, Germany, Oct. 2003.

[17] C. Intanagonwiwat, D. Estrin, R. Govindan, and J. Heidemann, "*Impact of network density on data aggregation in wireless sensor networks*," in Proc. Int. Conf. Distributed Computing Systems , Vienna, Austria, July 2002.

[18] B. Krishnamachari, D. Estrin, and S. Wicker, "*The impact of data aggregation in wireless sensor networks*," In Proc. Intl. Workshop of Distributed Event Based Systems, July 2002.

[19] E. Fasolo, M. Rossi, J. Widmer, M. Zorzi, "*In-network aggregation techniques for wireless sensor networks: a survey*", IEEE Wireless Communications, Volume: 14, Issue: 2, Pages: 70-87, April 2007.

[20] D. Estrin, A. Sayeed, and M. Srivastava, Mobicom Tutorial "*Wireless Sensor Networks"*, Mobicom 2002.

[21] H. O. Tan and I. Korpeoglu, "*Power Efficient* Data gathering and aggregation in wireless sensor networks," ACM SIGMOD Record, vol.32, no.4, pp.66–71, Dec. 2003.

[22] X. Fan, S. Li, Z. Li, J. Li, "*Sensors dynamic energy management in WSN*," In Scientific Research Publishing, Inc. ISSN: 1945-3078, Volume: 2, Issue: 9, Sept 2010.

[23] K. Akkaya, M. Younis, "*Energy and QoS aware routing in wireless sensor networks*," Cluster Computing, Volume 8, Numbers 2-3, 179-188, DOI: 10.1007/s10586-005-6183-7, in press.

[24] A. Hafid, F. Chender, T.J. Kwon, "*Energy Aware Passive Clustering in Wireless Mobile Networks*," IEEE IWCMC, 2008.

[25] K. Thanigaivelu and K. Murugan, "*To Alleviate Congestion Using Hybrid Sink for Delay Sensitive Applications in Wireless Sensor Networks*," Communications in Computer and Information Science, 2010, Volume 90, Part 2, 431-438, DOI: 10.1007/978-3-642-14493-6_44.

[26] M. Mamun-Or-Rashid and C.S. Hong, "*Dynamic Contention Window based Congestion Control and Fair Event Detection in Wireless Sensor Network*", In the Proceedings of 31st Korea information Processing Society (KIPS),Korea, pp. 1288-1290, May 2007.

[27] M. Lee and S. Lee, "*Data dissemination for wireless sensor networks*," In Proceedings of the 10th IEEE International Symposium on Object and Component-Oriented Real-Time Distributed Computing, (ISORC 07), Santorini Island, Greek, pp. 172-180, May, 2007.

[28] Laukik Chitnis, Alin Dobra, Sanjay Ranka. Analyzing the multiple aggregation trees technique for fault tolerance in sensor networks. In proceedings of \emph{International Conference on

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

Information Systems, Technology and Management} (ICISTM 2007), New Delhi, India, March 2007. pg. 269-279.

[29] Z. Eskandari, M. H. Yaghmaee, and A. H. Mohajerzadeh, "*Energy efficient spanning tree for data aggregation in wireless sensor networks*," SN'08 Workshop at ICC- CN, 2008.

[30] K. Akkaya, M. Younis, and M. Youssef. "*Efficient Aggregation of Delay constrained Data in Wireless Sensor Networks*". The 3rd ACS/IEEE International Conference on Computer Systems and Applications, pages 904 – 909, 2005.

[31] Analysis of Denial-of-Service attacks on Wireless Sensor Networks Using Simulation by Doddapaneni.krishnaChaitanya, and Ghosh.Arindam,Middlesex University

[32] Five Basic Types of Insider DoS Attacks of Code Dissemination in Wireless Sensor Networks by Yu ZHANG, Xing She ZHOU, Yi Ming JI, Yee Wei LAW, Marimuthu PALANISWAMI

[33] Main Types of Attacks in Wireless Sensor Networks by Teodor-grigorelupu

[34] Denial of Service in Sensor Networks by Anthony D.WoodJohn A.Stankovic

[35] Mohamed Ghallali, "*Designing A New Framework In Order To Limit The Spread Of Malware In Mobile Phone*", IJECST | Int. J.EnCoTe, 2012, v0101, 01-08 ISSN : 2277 - 9337 March – April 2012.

[36] Mohamed Ghallali, "*Mobile phones security: the spread of malware via MMS and Bluetooth, prevention methods*. MoMM 2011: 256-259, Proceedings of the 9th International Conference on Advances in Mobile Computing and Multimedia.