Wireless Sensor Network Layer Solution for Security Management

Kais Mekki, Ahmed Zouinkhi, Mohamed Naceur Abdelkrim

13th International conference on Sciences and Techniques
of Automatic control & computer engineering
December 17-19, 2012, Monastir, Tunisia

Wireless Sensor Network Layer Solution for Security Management

Kais Mekki, Ahmed Zouinkhi, Mohamed Naceur Abdelkrim

Research Unit MACS (Modeling, Analysis and Control of Systems), National Engineering School of Gabes, 6029 Gabes, Tunisia.
Mekki.Kais@gmail.com
Ahmed.Zouinkhi@enig.rnu.tn
Naceur.Abdelkrim@enig.rnu.tn

Abstract. *Wireless sensor networks have profound effects on many application fields like security management which need an immediate, fast and energy efficient route. In this paper, we define a QoS based network layer for security management of chemical products warehouse which can be classified as real-time and mission critical application. This application generate alert packets caused by unusual events which need a short end to end delay and low packet loss rate constraints. After each node compute his hop count and build his neighbors table in the initialization phase, packets can be routed to the sink. We use Random Re-Routing protocol which dynamically transfers routine data packets to secondary paths in the network, while offering a fast track path with better QoS for the packets carrying unusual events data. We add an energy threshold for the routing protocol to control the energy consumption and we adapt the network topology changes by rerun the initialization phase when chemical units were added or removed from the warehouse. Analysis shows that the network layer is energy efficient and can meet the QoS constraints of unusual events packets.*

Keywords. *WSN, Security, Routing protocols, Quality of Service, Simulation.*

1. Introduction

In the sector of the chemical industry, the priority is granted to the protection and the safety of goods and people. It is for that besides that one seeks without cease to develop increasingly reliable means ensuring safety at the level storage and handling of the dangerous chemicals, from where the integration of the Wireless Sensor Networks (WSN) in the systems design of security.

Currently, many security systems depend on safety measurements eventually exposing people lives to unpredictable environments as for examples storage and transport activities of dangerous chemical substances.

This subject attracted the interest of several research projects as the research center for automatic control (CRAN) at Lorraine University in France [1]. The project presented in [1] [2] develops a security management application of chemical products warehouse by wireless sensor network. The purpose of this application is to monitor chemical storage because such storage management product may cause great danger if safeguards are not respected. This application generates security alerts. An alert is transferred by a high priority packet across the wireless network to achieve the sink. Hence, this real-time application requires strict constraints on both delay and packet loss rate in order to report the alert data to the sink node within certain time limits without loss. These performance metrics (delay and packet loss rate) are usually referred to as Quality of Service (QoS) requirements [3]. Therefore, enabling real-time application in wireless sensor networks requires energy and QoS awareness in network layer of the protocol stack in order to have efficient utilization of the network resources and effective access to sensors readings.

Thus, QoS routing is an important topic in sensor networks research, and it has been the focus of the research community of WSN. Many QoS based routing protocols specifically designed for WSN have been proposed, for example, SPEED [4], MM-SPEED [5], RPAR [6], THVR [7], FELGossiping [8], M-HTR[9], RRR [10], EQSR [11] and MARP [12]. For our application, we had chosen Random Re-Routing (RRR) protocol.

In this paper, we realize energy efficient and QoS based network layer which uses RRR routing protocol for security management of chemical products warehouse, and we evaluate his adaptation to the application functionality with extensive simulations.

The rest of the paper is organized as follows. In the next section, we describe the security management application of chemical products warehouse. In section 3, we present the network layer and, in section 4, we analyze the performance of the proposed solution. Finally, we conclude the paper in section 5.

2. Security Management Application

Accidents in the chemical industry are becoming frequent due to the absence of adequate security measures especially in the chemical warehousing field. This topic has attracted the interest of several research projects [1].

The application of our work has been done to meet the needs of this field, its goal is to monitor dangerous chemical products warehouse. This application was able to turn the chemical units in communicating entities by wireless sensor nodes to collect information from its environment as shown in figure 1.

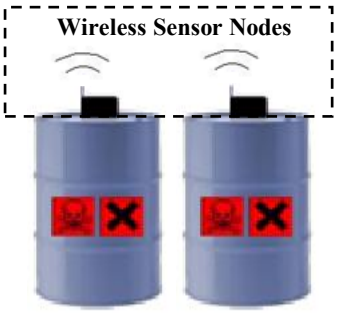

Fig. 1. Communicating entity for dangerous chemical products.

The sensors glued to chemical units must periodically send information (routine data) about the status of products (temperature, pressure, etc). If there is an abrupt change from an environmental or internal state of chemical products, the application at the sensors must report this alert (unusual event) to the control center via the sink node by high priority packet as shown in figure 2.

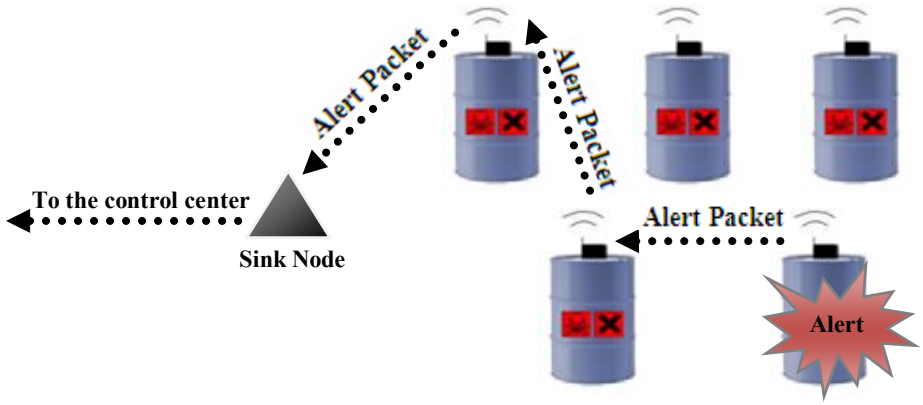

Fig. 2. Routing of unusual event packet.

The sensors must use energy efficient and QoS based network layer which gives a short delay and low packet loss rate for unusual events packets.

3. Network Layer Solution

3.1. Network Initialization Phase

The network initialization phase [8] starts after the sensor nodes are randomly distributed in the controlled area. In the beginning, the sink broadcasts a HELLO message to its neighbors. The HELLO message contains: the hop count (HC) and the sender address (SA). The hop count is used to setup the gradient to the sink which means it shows the node distance to the base station, and the sender address is used to build the neighbor table of each node. After broadcasting the HELLO message, all 1-hop neighbors will receive this message and each one will execute the following steps:

- **If it doesn't have a gradient:**
  - Gets its hop count by saving HC in its memory.
  - Saves SA and the hop count of the sender node in its neighbor table. The hop count of the sender is equal to HC-1.
  - Increases HC by 1. The old HC is then replaced in the HELLO message with the new one and the node will continue to broadcast this message to farther nodes. As shown in figure 3, at each stage the hop count will be incremented by 1.
- **If it has a gradient:**
  - Gets SA and the hop count of the sender node. If SA exists in neighbor table, the corresponding hop count will be replaced with the new one. Else, information will be saved in the neighbor table.
  - Compares its gradient to the HC and will replace its hop count with the message's HC if the latter is smaller, and will add 1 to the HC prior to broadcasting it. However, if its gradient is smaller than or equal to the HC, it will discard the message. As a result, the gradient will keep the best route.

Finally, the process will continue until all nodes receive the HELLO message. At that time, the network initialization phase will be completed. Now each node knows its distance to the sink node and its entire neighbors and their gradient through neighbor table. Nodes can starts routing packets to the base station through a routing protocol.

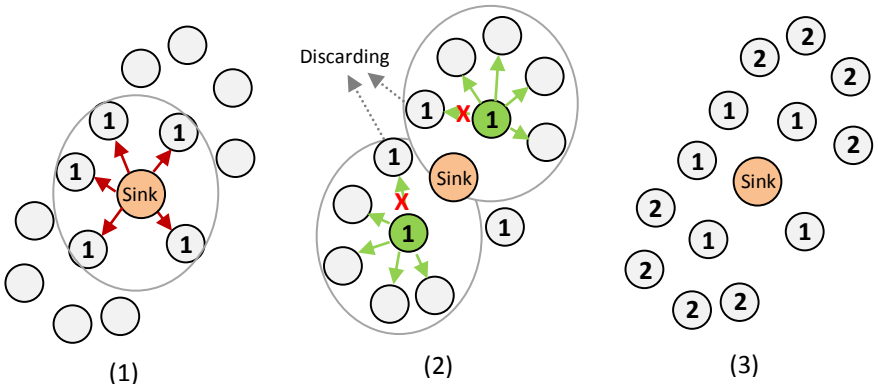

Fig. 3. Network Initialization Phase.

3.2. Routing Protocol

We had chosen Random Re-Routing (RRR) protocol which is evaluated in [13] and compared with other QoS based routing protocols. Simulation results in [13] showed that RRR can achieve very low end to end delay and low packet loss rate, and we have to study this protocol for supporting our security management application and his network layer.

RRR [10] is a distributed and adaptive routing algorithm which can detect the occurrence of unusual events (alert) and provide better QoS for packets that carry alert information. The WSN is composed of sensor nodes which may have both sensing and forwarding roles. RRR is implemented in each of the sensor and forwarding nodes. It distinguishes packets of routine data and unusual events, packets from unusual events are routed along preferred paths, while the routine data are randomly shunted to slower and possibly longer secondary paths.

In RRR, the sensor nodes will change their routing policy adaptively according to the current traffic level. When the overall total traffic level is low, the preferred paths will be shared by all packets. However, when the total traffic exceeds a given threshold, the preferred paths will be reserved for forwarding only the unusual events data packets and secondary paths will be used for the routine data packets. This mechanism provides significantly better QoS to unusual events packet.

In more detail, each node monitors the rate at which it receives unusual events packets, and if this rate does not exceed a threshold θu, then the node forwards all packets it receives along their preferred path towards their destinations as shown in figure 4. The preferred path will be the path with the minimum number of hops (the shortest one). In this case, RRR uses the same path for both types of packets which can consume a lot of transit nodes energy especially if it continues for long time. To

control this, we add an energy threshold to RRR protocol. If the energy consumed by transit node exceeds the threshold (e.g. energy consumption exceeds 85% of the initial energy), then the node is only involved in unusual events packets routing as shown in figure 5. If a node (source or transit) senses that the rate at which it forwards unusual packets exceeds the threshold θu, then it will forward all unusual events packets along the preferred path to their destination, while all routine data packets will be directed along a randomized route which leave the shortest paths to the high priority traffic (unusual events packets) as shown in figure 6.

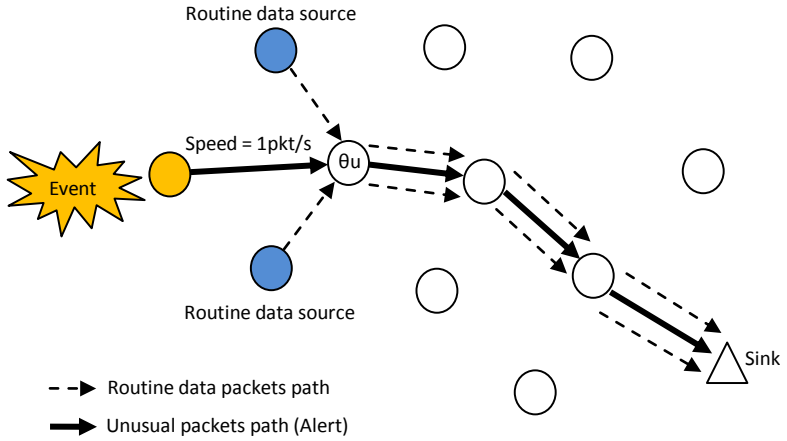

Fig. 4. RRR behavior in not congested traffic for θu=3pkt/s and speed (alert packets)=1pkt/s.

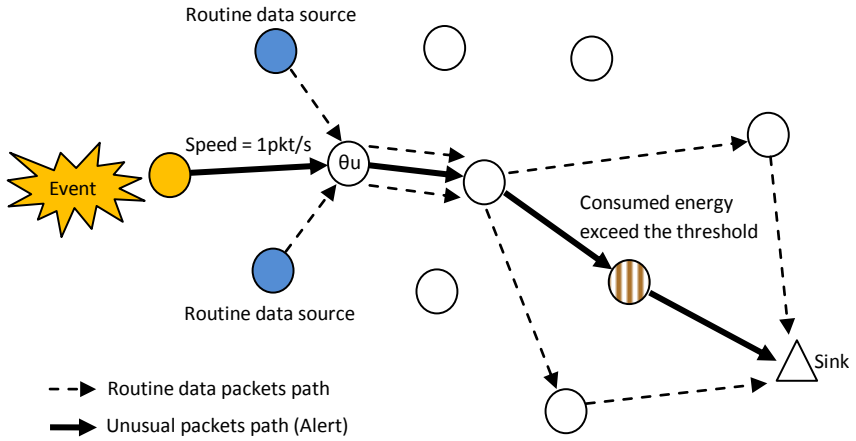

Fig. 5. RRR behavior if the consumed energy of node exceeds the energy threshold.

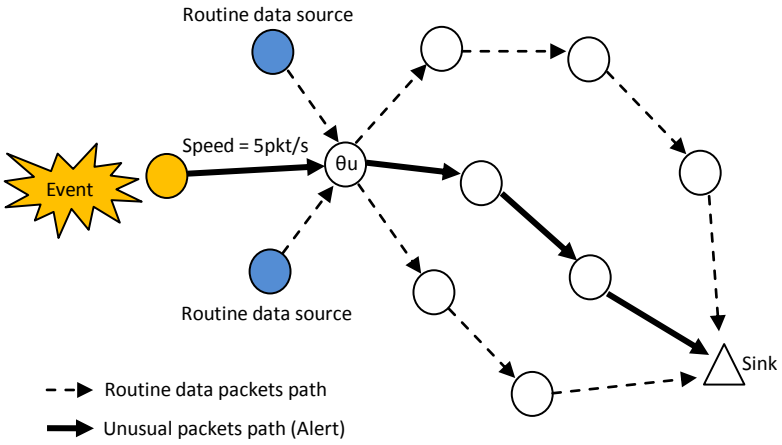

Fig. 6. RRR behavior in congested traffic for θu=3pkt/s and speed (alert packets)=5pkt/s.

3.3. Adding/Removing Chemical Units

If a set of chemical units are added or removed from the warehouse, a node glued to one of these chemical units broadcasts respectively a joining or leaving message to all nodes that are in its transmission range [14]. A node that receives this message, routes it to the sink. Then, the sink begins running the initialization phase to rebuild the hop count and neighbor tables of all network nodes, hence adapting the network topology to change in the number of nodes.

4. Analysis

In this section, we evaluate the packet average delay, the packet loss rate and the energy consumption of the network layer under different sensor nodes densities. Furthermore, we use Castalia simulator [15] to implement the network layer. Currently, many wireless sensor network simulators are available as NS2 and SENSE but Castalia provides realistic wireless channel and radio models, and realistic node behavior especially relating to access of the radio [16] [17].

The simulated networks consist of 100, 200, 300 and 400 nodes respectively with a single sink. The node positions are all uniformly distributed at random within a 300m x 300m square (m=meters). The communication range is 30 meters, the sink is located at the center of the square and the RRR threshold θu is 3pkt/s. The simulation parameters that we have chosen have been selected so as to be compatible with other studies of WSN [10] [12] [18].

We simulate the network under two state of traffic:

- Not congested traffic: the routine data packet rate is 0.2 pkt/s for each node, while the unusual event traffic rate is 1 pkt/s at 2 nodes. In this case, the unusual event traffic rate at the intermediate nodes doesn't exceed θu.
- Congested traffic: the routine data packet rate is 1 pkt/s for each node, while the unusual event traffic rate is 5 pkt/s at 4 nodes. The network load becomes higher now as there are more sources of unusual event with higher rate, so the unusual event traffic rate at the intermediate nodes exceeds θu.

We simulate these two routing schemes under different node densities between 100 and 400 nodes.

4.1. Delay

Figures 7 and 8 shows the packet average end to end delay for each type of packet and for four levels of network density (100, 200, 300 and 400 nodes).

Figure 7 shows that the network layer is able to meet the time constraints for alert packets (unusual event) in congested traffic, the alert packet delay is very short even with the increasing of the network density. In congested traffic, the unusual event traffic rate at the intermediate nodes exceed the threshold θu and then the unusual event packets are routed along the shortest path whereas the routine data packets are forwarded via random alternative paths. So as shown in figure 7, the unusual event data achieve lower packet delay than the routine data.

Figure 8 shows the packet average delay in not congested traffic. As expected, the routine data packet delay is very close to the unusual event packet delay because the network handles both unusual event and routine data by the shortest path.

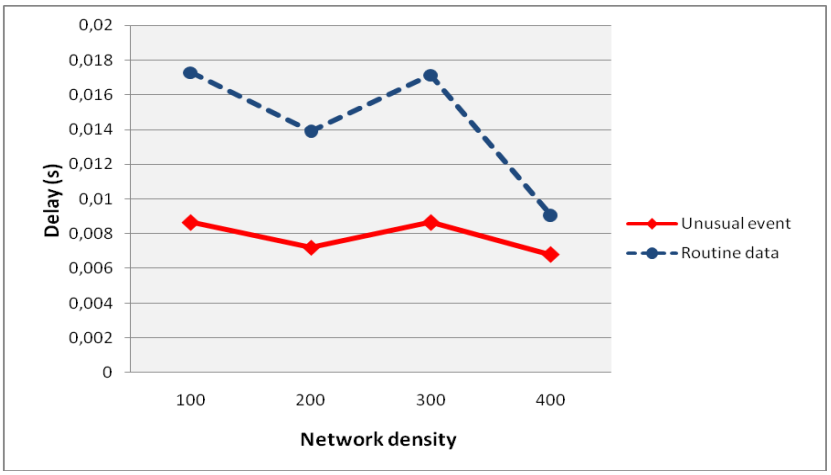

Fig. 7. Delay performance in congested traffic.

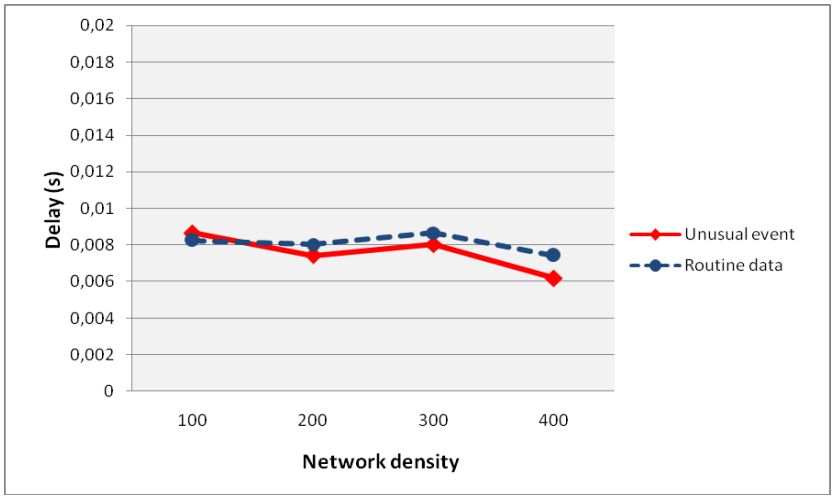

Fig. 8. Delay performance in not congested traffic.

4.2. Packet Loss Rate

Figures 9 and 10 shows that the network layer guarantees a very low packet loss rate for the alert packets in the two classes of traffic.

In congested traffic, the routine data packets have a medium packet loss rate as shown in figure 9 because they pass through random alternative paths that have a low quality of service and may be congested by routine data packets from other sources. The analysis of trace files showed that the majority of packets are lost due to:

- Overloading of nodes causing saturation of the queues.
- Interference because we have many transfers, so there is more concurrent access to the radio channel.

Reasoning according to the density of the network, figures 9 and 10 shows that the network layer was able to maintain a constant and low packet loss rate for alert packets even when the density of the network increases. For routine data packets, the number of successfully received packets increases because the node will have more choices of the next hop when the number of neighbor nodes increases.

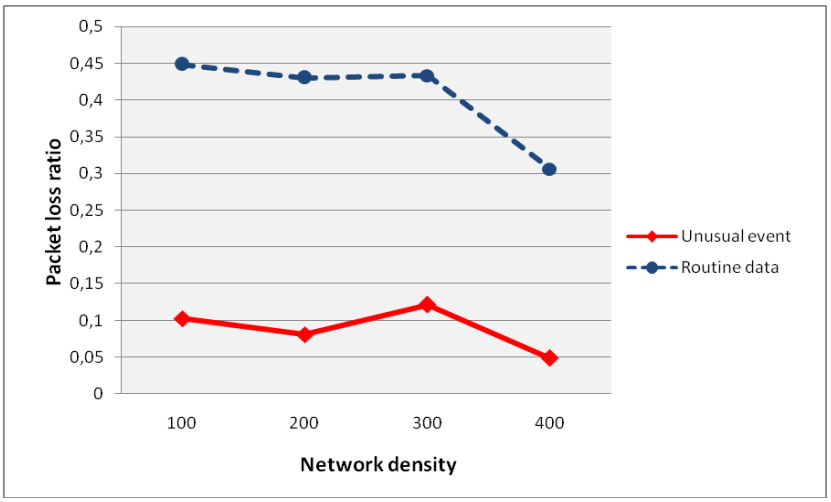

Fig. 9. Packet loss rate performance in congested traffic.

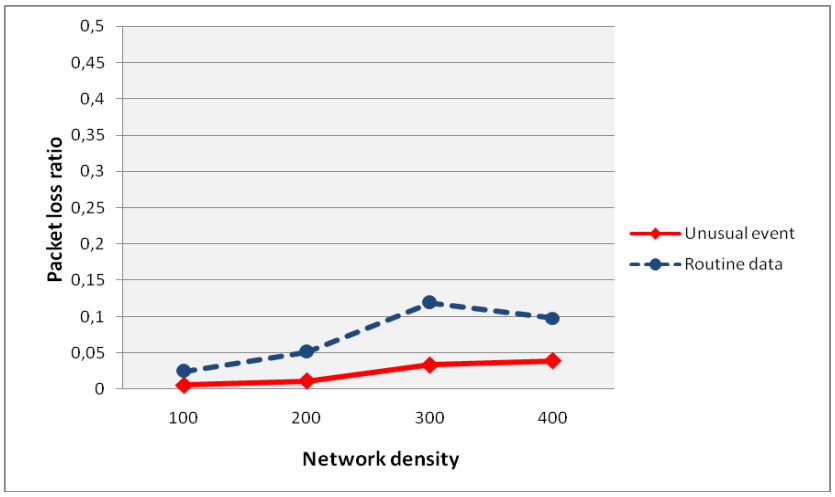

Fig. 10. Packet loss rate performance in not congested traffic.

4.3. Energy Consumption

To study the energy consumption of the network layer, we performed two different simulations. First, we compare it to another network layer which uses energy efficient and QoS based routing protocol for WSN. Second, we evaluate the energy threshold performance.

- **Energy consumption:** we had chosen to compare our solution with a network layer which uses FELGossiping routing protocol [8]. We had also implemented

FELGossiping with Castalia simulator. We considered nodes with an initial energy equal to 18760 Joules. We measured the average energy consumed by the network nodes in different periods of time. The simulation result is shown in figure 11. We observe that RRR achieves more energy savings than FELGossiping because RRR protocol does not use any control messages, the routing decision is done using the neighbors table built in the initialization phase. The analysis of trace files showed that FELGossiping protocol has a bigger throughput than RRR which gives a higher packet transmission number and so a higher energy consumption. Therefore, our network layer optimizes more the energy consumption and therefore ensures a long network lifetime than the FELGossiping based network layer.

- **Energy threshold evaluation:** now we consider nodes with limited energy and we simulate the network traffic until the first node dead first for the initial RRR protocol and then for the RRR with our energy threshold. The effect of the energy threshold is shown in table 1, the table shows death time of the first node for both protocols. Nodes tend to die faster in the initial protocol. With our threshold, the probability of choosing the same node as the next hop for long time is reduced. Thereby, the energy has been more balanced and fairly used. The threshold leads to saving energy and hence prolonging the overall network lifetime.

Table 1. Death time of first node (in seconds)

	Initial RRR	RRR with energy threshold
Death time (s)	58,309	59,15

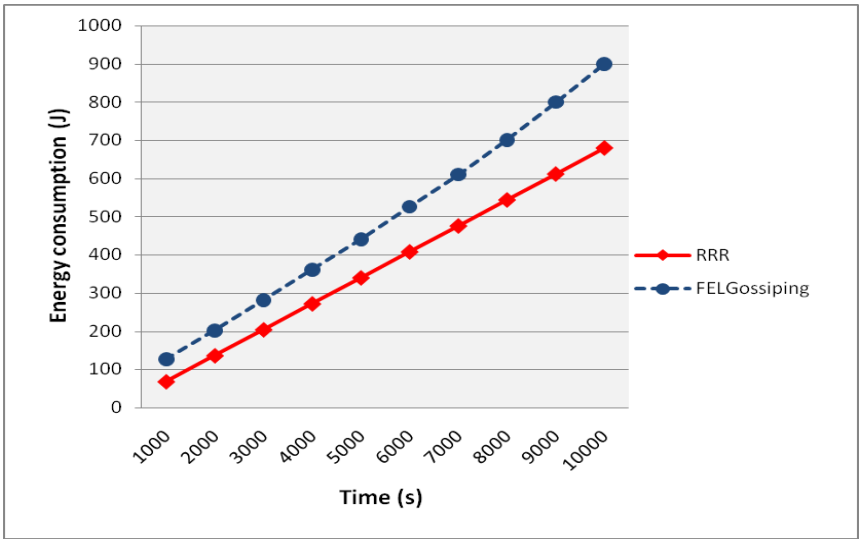

Fig. 11. Energy consumption performance.

5. Conclusion

In this paper, we realized a network layer for security management application of chemical products warehouse. We used Random Re-Routing (RRR) protocol that is designed to react to network congestion so as to provide better quality of service to alert packets caused by unusual and critical events. We added an energy threshold to improve RRR protocol for saving more energy and prolonging the network lifetime. We also proposed a solution for network self-organization when chemical units are added or removed from the warehouse. Simulation results showed that the network layer can achieve short average end to end delay and low packets loss rate for alert packets, and RRR showed its improvement in the network lifetime when we used the energy threshold. As a future project, we will improve the network layer to be fault-tolerant and to react when node becomes unreachable.

References

1. A. Zouinkhi, E. Bajic, E. Rondeau and M. N. Abdelkrim, "Simulation and modeling of active products cooperation for active security system management", International Journal Transactions on Systems, Signals and Devices, Vol. 5, No. 3, 2011, pp. 1-23.
2. A. Zouinkhi, E. Bajic, R. Zidi, M. Ben Gayed, E. Rondeau and M. N. Abdelkrim, "Petri nets modeling of active products cooperation for active security management", 6th International Multi-Conference on Systems, Signals and Devices, Djerba, Tunisia, 23-26 March 2009, pp. 1-6.
3. J. Chen , M. Diaz, L. Llopis, B. Rubio and J. M. Troya, "A survey on quality of service support in wireless sensor and actor networks: Requirements and challenges in the context of critical infrastructure protection", Journal of Network and Computer Applications, Vol. 34, No. 4, 2011, pp. 1225-1239.
4. Tian He, J. A. Stankovic, C. Lu and T. Abdelzaher, "SPEED: A stateless protocol for real-time communication in sensor networks", 23rd International Conference on Distributed Computing Systems, 19-22 May 2003, pp. 46–55.
5. E. Felemban, C. G. Lee and E. Ekici, "MMSPEED : Multipath multi-speed protocol for QoS guarantee of reliability and timeliness in wireless sensor network", IEEE Transactions on Mobile Computing, Vol. 5, No. 6, 2006, pp. 738–754.
6. O. Chipara, Z. He, G. Xing, Q. Chen, X. Wang, C. Lu, J. Stankovic and T. Abdelzaher, "Real-time power-aware routing in sensor network", 14th IEEE International Workshop on Quality of Service, 19-21 June 2006, pp. 83–92.
7. Y. Li, C. S. Chen, Y. Song, Z. Wang and Y. Sun, "Enhancing Real-Time Delivery in Wireless Sensor Networks with Two-Hop Information", IEEE Transactions on Industrial Informatics, Vol. 5, No. 2, May 2009, pp. 113-122.
8. A. Norouzi, F. S. Babamir and A. H. Zaim, "A Novel Energy Efficient Routing Protocol in Wireless Sensor Networks", Journal of Wireless Sensor Network, Vol. 3, 2011, pp. 350-359.
9. B. Nefzi and Y.Q. Song, "Performance analysis and improvement of zigbee routing protocol", 7th IFAC International Conference on Fieldbuses and Networks in Industrial and Embedded Systems, Toulouse, France, 2007.

10. E. Gelenbe and E. Ngai, “Adaptive QoS Routing for Significant Events in Wireless Sensor Networks”, 5th IEEE International Conference on Mobile AdHoc and Sensor Systems, September 2008, pp. 410–415.
11. J. B. Othman and B. Yahya, “Energy efficient and QoS based routing protocol for wireless sensor networks”, Journal of Parallel and Distributed Computing, Vol. 70, No. 8, August 2010, pp. 849-857.
12. J. Sen and A. Ukil, “An Adaptable and QoS-Aware Routing Protocol for Wireless Sensor Networks”, 1st International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology, May 2009, pp. 767–771.
13. K. Mekki, A. Zouinkhi and M. N. Abdelkrim, “QoS based routing protocol for security management: Application in dangerous chemical products”, 4th Symposium of Applied Research and Technology Transfer, Rades, Tunisia, 30-31 October 2012.
14. X. Zhang, J. He and Q. Wei, “Energy-Efficient Routing for Mobility Scenarios in Wireless Sensor Networks”, Proceedings of the 3rd International Symposium on Electronic Commerce and Security Workshops, Guangzhou, P. R. China, 29-31 July 2010, pp. 80-83.
15. A. Boulis, “Castalia, a simulator for wireless sensor networks and body area networks, version 3.2”, User’s manual, NICTA, March 2011.
16. A. Zouinkhi, A. Ltifi, E. Bajic, R. Zidi, M. Ben Gayed, E. Rondeau and M. N. Abdelkrim, “Simulation of Active Products Cooperation for Active Security Management”, 8th International Conference of Modeling and Simulation, Hammamet, Tunisia, 10-12 May 2010.
17. H. Sundani, H. Li, V. Devabhaktuni, M. Alam and P. Bhattacharya, “Wireless Sensor Network Simulators, A Survey and Comparisons”, International Journal Of Computer Networks, Vol. 2, No. 5, 2011, pp. 249-265.
18. L. Hey and E. Gelenbe, “Adaptive Packet Prioritisation for Wireless Sensor Networks”, Proceedings of the 5th Euro-NGI Conference on Next Generation Internet Networks, Aveiro, Portugal, 1-3 July 2009.