TELKOMNIKA, Vol.11, No.2, June 2013, pp. 363~372
ISSN: 1693-6930
accredited by DGHE (DIKTI), Decree No: 51/Dikti/Kep/2010

Fault-tolerant and QoS based Network Layer for Security Management

Kais Mekki[1], Ahmed Zouinkhi[2], Mohamed Naceur Abdelkrim[3]
Research Unit MACS (Modeling, Analysis and Control of Systems)
National Engineering School of Gabes, 6029 Gabes, Tunisia.
e-mail: mekki.kais@gmail.com[1], ahmed.zouinkhi@enig.rnu.tn[2], naceur.abdelkrim@enig.rnu.tn[3]

Abstrak

Jaringan sensor nirkabel (Wireless sensor networks) memiliki peranan yang dominan pada berbagai bidang aplikasi, salah satunya di bidang manajemen keamanan yang membutuhkan route yang langsung, cepat dan efisien (hemat energi). Pada paper ini, kami mendefinisikan sebuah layer jaringan yang bersifat fault-tolerant dan berbasis pada QoS untuk manajemen keamanan dari gudang produk kimia yang dapat diklasifikasikan sebagai sebuah aplikasi yang bersifat real time dan mission critical. Aplikasi ini membangkitkan paket data rutin dan paket waspada(alert packets) yang disebabkan adanya kejadian-kejadian yang tidak biasa yang membutuhkan reliabilitas tinggi, tundaan yang singkat dan tingkat kehilangan paket yang rendah. Setelah setiap node melakukan hop count dan membangun tabel ketetanggaan pada fase inisialisasi, maka paket dapat diarahkan menuju ujung rute. Pada paket biasa digunakan protokol FELGossiping dan protokol routing node disjoint multipath. Lebih jauh lagi, pada fase pengumpulan informasi FELGOssiping dimanfaatkan juga untuk memperbaharui tabel ketetanggaan dan mendeteksi node yang gagal dan dilakukan adaptasi perubahan topologi jaringan dengan melakukan inisialisasi ulang ketika suatu bahan kimia ditambahkan ataupun dikerluarkan dari gudang. Analisis menunjukkan bahwa layer jaringan yang diperoleh hemat nergi dan memenuhi syarat QoS dari paket yang tidak biasa.

Kata kunci: *jaringan sensor nirkabel, sekuriti, protokol routing, quality of service, fault-tolerant.*

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 fault-tolerant and 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 routine data packets and alert packets caused by unusual events which need a high reliability, 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 FELGossiping protocol for routine data packets and node-disjoint multipath routing protocol for alert packets. Furthermore, we utilize the information gathering phase of FELGossiping to update the neighbors table and detect the failed nodes, 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: *wireless sensor networks, security, routing protocol, quality of service, fault-tolerant.*

1. Introduction

Regarding the expansion of industrial field, security becomes a topic issue. Especially when we consider security in industrial environment, workers have to deal sometimes with unavoidable threats that are a part of work risks. 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 product. This subject attracted the interest of several research projects as Active Intelligent Products [1]-[2], RFID-Smart Objects [3], Object Safety Agents [4] and COBIS [5]-[6].

Active Intelligent Products is a new security system and it was developed in the research center for automatic control CRAN at Lorraine University in France. This project develops a security management application of chemical products warehouse by wireless

Received December 27, 2012; Revised February 15, 2013; Accepted February 25, 2013

sensor networks. The purpose of the application is to monitor chemical warehouse because such storage management products may cause great danger if safeguards are not respected. In this system, every chemical container is equipped with a wireless sensor node which controls the internal state of the product and the external changes of its environment (e.g. temperature, brightness and humidity) using different sensors modules. The node also control the distance between the containers by periodic exchange of greeting messages between neighboring nodes (RSSI method) to prevent the closeness of the products that are not compatible. If there are critical or unusual events (e.g. high temperature, incompatible products are very close), the node is able to make decisions and send alert packets to control center via the sink. In addition, the nodes periodically exchange configuration and information messages with the control center to monitor the temporal evolution of the chemical products.

This security system uses a centralized approach and point-to-point connection for the communication between nodes and sink. The nodes communicate directly with the control center by broadcast model [7] (Application Layer + Data link Layer + Physical Layer). For a large scale warehouse and high distance, the node will be unable to communicate with the control center due to the low transmission power of wireless sensor nodes. So, the node must greatly increase its transmission power to reach the sink which consuming huge amount of energy and greatly limits the lifetime of nodes and hence the network lifetime. To overcome this limitation, we proposed in this paper a multi-hops connection for nodes/sink communication. The messages passes from one node to another until it reaches the control center, this mechanism requires the development of routing protocol and the implementation of network layer.

Furthermore, the application generates security alerts. An alert message will be encapsulated in a high priority packet in our network layer and will be routed across the wireless network toward the sink node. An alert message requires strict constraints on both delay and loss ratio in order to report the data to the control center within certain time limits without loss. These performance metrics (delay and loss ratio) are usually referred to as Quality of Service (QoS) requirements [8]. Thus, enabling high priority packet for the security system in network layer requires QoS based routing protocol.

However, sensor nodes may fail due to various reasons including radio interference, de-synchronization, malfunctioning, battery exhaustion and dislocation. Such failures are caused by software and hardware faults, environmental conditions, malicious behavior or bad timing of a legitimate action [9, 10]. The consequence of such event is that a node becomes unreachable which could be very dangerous. The chemical container that is controlled by a failed node could lead to a great danger if unusual event happen in that product. So, it is important to identify the failed nodes to keep network connectivity and avoid container isolation, hence guarantee high security level. Thus, the network layer and the routing protocol have to be fault-tolerant in order to detect failed node and avoid chemical product isolation.

In this paper, a fault-tolerant and QoS based network layer for security management of chemical products warehouse is presented. The solution was implemented with Castalia-OMNET++ Tools language and evaluated with extensive simulations.

The rest of the paper is organized as follows. In the next section, we describe the security management application. 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. 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 container in communicating entities by wireless sensor nodes to collect information from its environment.

The sensors glued to container must periodically send information (routine data) about the status of the products (e.g. temperature and humidity) to monitor the temporal evolution. 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 1.

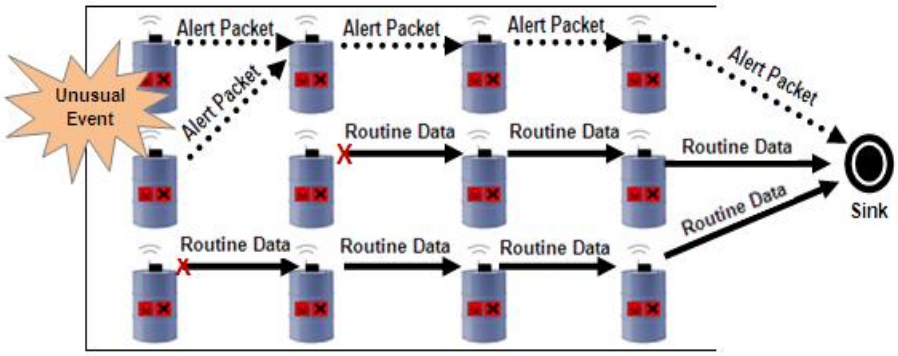


Figure 1. Routing of unusual event packet and routine data

3. Network Layer Solution

3.1. Network Initialisation Phase

The network initialization phase 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 [11]:

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 2, 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.

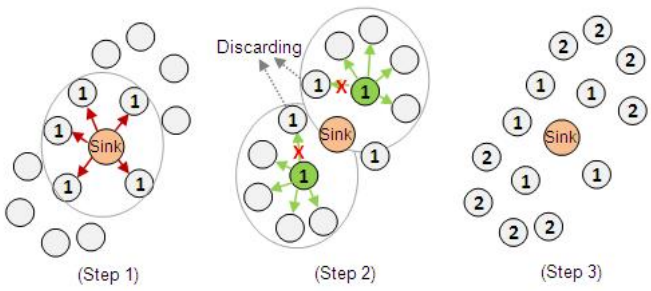


Figure 2. Network initialization phase

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.

3.2. Routing Protocol

The security management application has two types of packets, routine data packets which are sent periodically to the sink and alert packets which occurs when there is unusual event (e.g. high temperature) so it require high quality of service. Therefore, we had to use different strategy for the routing of such information.

In industrial environments, several faults could lead to failures in wireless sensor networks. For example, nodes can suffer power failure and stop responding to requests [12]. The failure of node mean that the chemical unit controlled by this node is isolated from the network and is not controlled, so it could lead to an emerging and critical problems. Thus, we have also to make our routing protocol fault-tolerant to resist and control failed nodes. When node is detected as failed, alert packet must be sent to the control center. The packet contains the ID and the location of the failed node.

Routing of alert packets:

For alert packets, we had chosen multipath routing to enhance the reliability and the fault tolerance. The alert source node starts multipath routing and creates a set of neighbors that able to forward data towards the sink. The constructed multipath are node-disjoint paths (have no common nodes except the source and the destination). In multipath routing, node-disjoint paths are usually preferred because they utilize the most available network resources, and hence are the most fault-tolerant [13]. If an intermediate node in a set of node-disjoint paths fails, only the path containing that node is affected. The multipath routing procedure is executed according to the following steps:

- **Primary path routing phase:** Through the neighbor table, the source selects the node which has the minimum hops to the sink as next hop, and sends the alert packet to this selected node. Similarly through its neighbor table, the next hop node of the source choose the closest node as next hop in the direction of the sink and sends out the alert packet. The operation continues until sink node as shown in Figure 3.

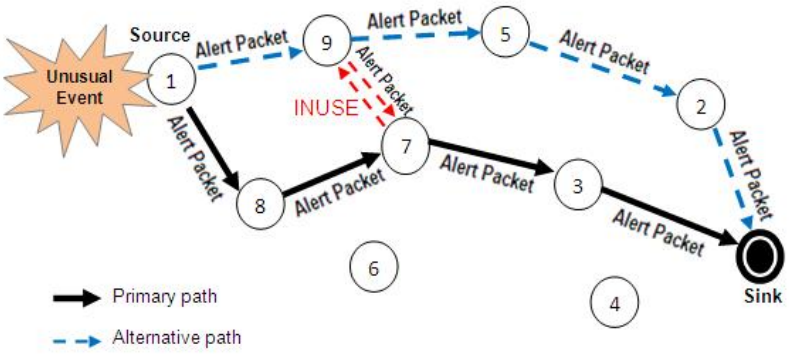


Figure 3. Example of node-disjoint paths routing

- **Alternative path routing phase**: For the second alternate path, the source node sends alert packet to its next most preferred neighbor (the second closest neighbor to the sink). To avoid having paths with shared node, we limit each node to accept only one alert packet. For those nodes that receive more than one alert packet, only accept the first one and reject the remaining packets. In the example of figure 3, node 9 computes it's next preferred neighbor and finds it node 7. Node 9 forwards the packet to node 7, but node 7 has been included in the primary path, then node 7 simply responds to node 9 with an

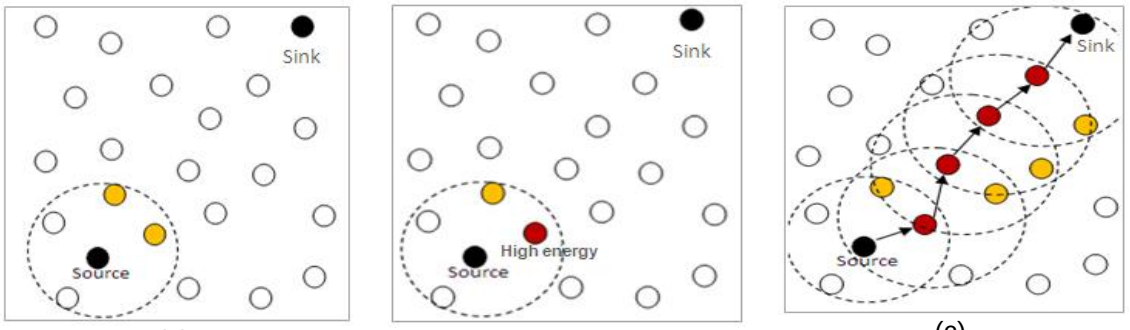
INUSE message [13] indicating that node 7 is already selected in a routing path. Immediately node 9 searches its neighboring table and selects the next preferred neighbor which will be node 5, and sends out alert packet to it. Node 5 accepts the packet and continues the procedure in the direction of the sink.

Routing of routine data packets:

For routine data packets, we had chosen Fair Efficient Location-based Gossiping (FELGossiping) protocol [14]. FELGossiping protocol consists of two phases for sending the packets to sink node, first information gathering phase and then routing phase.

- **Information Gathering Phase:** When node needs to send packet to the sink, it broadcasts a request message to acquire the information from the neighboring nodes in its transmission range. The nodes that received the request message send their information to the source, the response message contains the residual energy of the neighboring node. We use this phase to update the neighbor table of nodes which are involved in the route toward the sink. The source node gets the ID of all current neighboring nodes from the received response messages, and compare between the old neighbor table and the new one. The node from the old table which is absent in the new one, is considered as failed and therefore the source node must initiate alert packet which contain the ID and the location of the absent node and send it to the sink.

- **Routing Phase:** After the information gathering phase finishes, the routing phase will start. The source chooses from his neighbor table two nodes that have the minimum hop count towards the sink as shown in figure 4(a). Then, the source compare between these two nodes according to the residual energy, the nodes that had the highest residual energy level will be the next hop as shown in figure 4(b). If two nodes have the same residual energy level, the nodes that have a lower hop count to the sink will be taken. After that, the source node sends the packet to the selected node. Upon receiving the packet, the node as next hop repeats the information gathering phase and routing phase to transmit the packet to another node as shown in figure 4(c). The process continues until the packet reaches the sink or the TTL is finished [14].



(a) (b) (c)

Figure 4. Routing phase

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 containers broadcasts respectively a joining or leaving message to all nodes that are in its transmission range [15]. 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 the neighbor table of all nodes, hence adapting the network topology to change in the number of nodes.

4. Performance Study

In this section, we evaluate the packet average end to end delay, the packet loss ratio and the energy consumption of the network layer under different sensor nodes densities. Furthermore, we use Castalia simulator to implement the network layer [16]. 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 [17], [18].

The simulated networks consist of 100, 200, 300 and 400 nodes respectively with a single sink. The node positions are all uniformly distributed within a 300m x 300m square (m=meters). The communication range is 30 meters and the sink is located at the center of the square. The simulation parameters that we have chosen are summarized in table 1 and have been selected so as to be compatible with other studies of WSN [19], [20], [21].

Table 1. Simulation parameters

Items	Parameters
Network area	300m * 300m
Number of nodes	100 200 300 400
Nodes distribution	Uniform random
Location of Sink	Center of area
Radio range	30 m
MAC layer	TMAC
Initial energy	18720 J
Radio	Consistent with Telos components (CC2420)

We simulate the network under two state of traffic:

1. 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.
2. 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.

To evaluate the performance of our routing solution, we compared its performance with Random Re-Routing protocol (RRR) [20] [21] which uses also different strategy for routing of unusual event data and routine data. High priority packets of unusual events are routed along the preferred path (i.e. the shortest path), while the routine data packets are randomly shunted to slower and possibly longer secondary paths. In RRR, the sensor nodes change their routing policy adaptively according to the current traffic level. When the overall total traffic level is low, the preferred path will be shared by all packets. However, when the total traffic exceeds a given threshold (e.g. 3 pkt/s of unusual event packets), the preferred path will be reserved for forwarding only the unusual events packets and secondary paths will be used for the routine data packets. This mechanism provides significantly better QoS (i.e. low delay and high packet delivery ratio) to unusual events data.

4.1. Average end to end delay

End to end delay is an important metric in evaluating QoS based routing protocols [8]. Figures 5 and 6 show the average end to end delay for each protocol and each type of packet for four levels of network density (100, 200, 300 and 400 nodes).

Before analyzing the performance of our solution we present the result of RRR protocol. In congested traffic, the unusual event traffic rate at the intermediate nodes exceed the threshold of RRR 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 5, the unusual event data achieve lower packet delay than the routine data. Figure 6 shows that the delay made for both types of data for RRR are close, because this protocol does not differentiate between types of packets in not congested traffic (similar treatment for both packets).

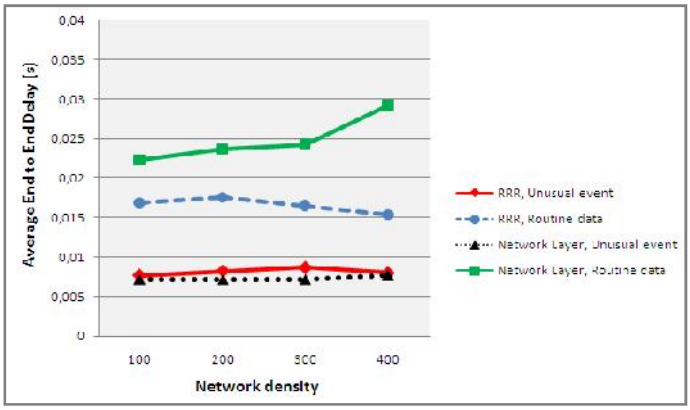


Figure 5. Average end to end delay performance in congested traffic

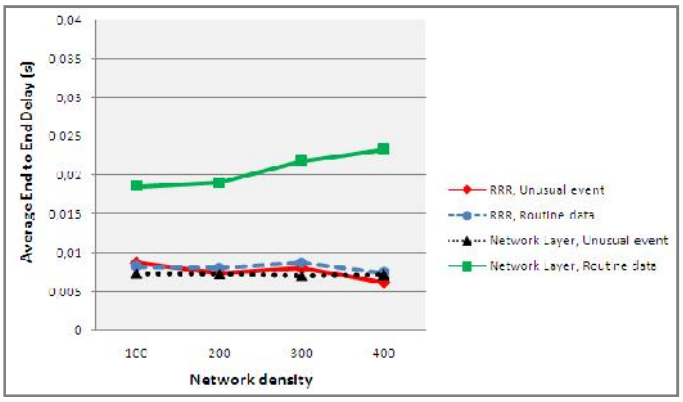


Figure 6. Average end to end delay performance in not congested traffic

For our network layer, figures 5 and 6 show that the developed protocol successfully differentiates routing services as RRR protocol. It is able to meet the time constraints for alert packets in both congested and not congested traffic, the alert packet delay is the lowest even with the increasing of the network density. RRR outperforms our protocol in the case of routing of routine data packet. Furthermore, the average delay of routine data is higher when density increases for our protocol because it suffers from a lost time on information gathering phase. In this phase and for each received packet, the protocol broadcasts a request and waits for responses from all the neighboring nodes to determine the next hop. So when the number of neighboring nodes increases, source node have to wait more time which causes more queuing and treatment delay for routine data packets despite it always chooses the paths that have the minimum number of hops to the sink.

In conclusion, our network layer performs better than RRR protocol in the end to end delay of alert packets but not for routine data packets.

4.2. Packet Loss Ratio

Another important metric in evaluating routing protocols is the packet loss ratio [8]. Figures 7 and 8 show the packet loss ratio for each protocol and each type of packet for four levels of network density (100, 200, 300 and 400 nodes). As expected, figures 7 and 8 show that our network layer guarantees a very low packet loss rate for the alert packets in the two classes of traffic due to multipath routing. Discovering and maintaining multiple paths between the source and the sink node improves the routing performance by providing alternative paths. Primary and alternative paths are used simultaneously for data routing by sending multiple

copies of alert packet across each path. Simultaneous multipath routing improves reliability. As long as, one of the multiple paths does not fail, the sink node will receive the packet.

RRR outperforms our protocol in the case of routine data packet because of the information gathering phase as delay performance. In not congested traffic, the routine data have a medium packet loss rate as shown in figure 8.

Lost packets increase in the case of congested traffic as shown in figure 7, the analysis of trace files of Castalia simulator showed that the majority of packets are lost due to:

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

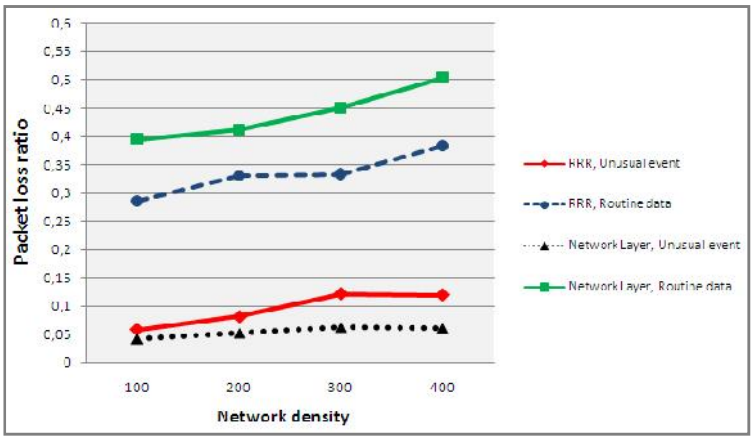


Figure 7. Packet loss ratio performance in congested traffic

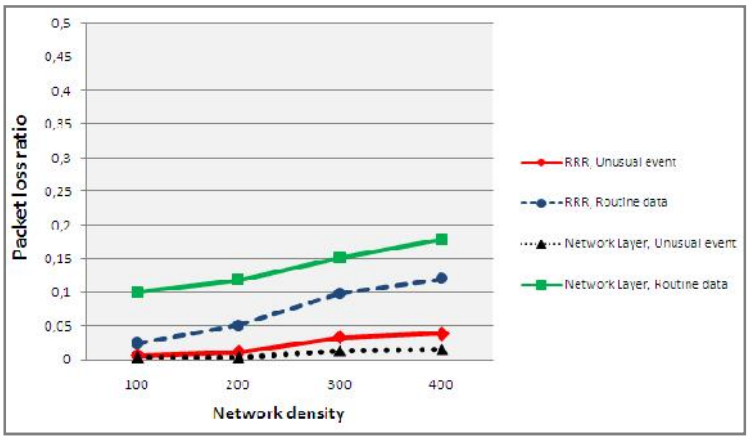


Figure 8. Packet loss ratio performance in not congested traffic

Reasoning according to the density of the network, figures 7 and 8 show that the network layer was able to maintain a low packet loss rate for alert packets due to multipath routing. For routine data, the number of lost packets increases because this protocol uses broadcast in the information gathering phase which causes many interference in case of high density.

In conclusion, our network layer is more efficient than RRR protocol because it ensures a very low packet loss rate for alert packets in both congested and not congested traffic but not for routine data packets.

4.3. Energy consumption performance

Figure 9 shows the average energy consumed by the network nodes in different periods of time. We observe that RRR achieves more energy savings than our protocol because RRR is an energy efficient and QoS based routing protocol and it does not use any control messages [20], hence it optimizes the energy consumption as well as guarantee high quality of service for alert packets.

The developed network layer exchange more control messages than RRR for routine data because it discover the neighbor nodes before sending data in information gathering phase, and exchange more packets for alert data because it use multipath routing. That's why the analysis of trace files of Castalia simulator showed that our protocol has more throughput than RRR which gives a more packets transmission number and so more energy consumption. Control messages exchanged by our solution (neighbor discovery in each hop) and multipath routing have one goal, to improve the transmission reliability and fault tolerance. Thus, for increasing the reliability and security we have to sacrifice energy consumption. But as presented in figure 9, the consumed energy of our solution does not have large difference compared to RRR. Therefore, our network layer is considered acceptable for energy consumption performance.

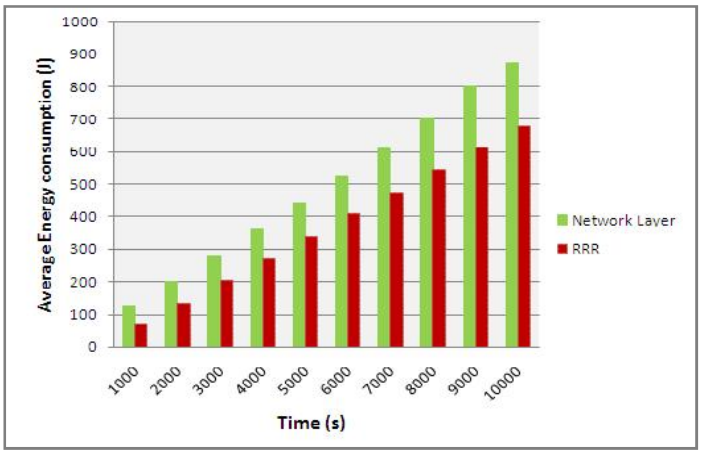


Figure 9. Energy consumption performance

5. Conclusion

In this paper, we realized a network layer for security management application of chemical products warehouse. We used node-disjoint multipath routing protocol to provide high quality of service to alert packets caused by unusual and critical events. And, we used FELGossiping protocol to route the routine data packets, update the neighbors table and detect the failed nodes. We also proposed a solution for network self-organization when chemical units are added or removed from the warehouse. Through computer simulation, we have evaluated and studied the performance of our solution under different network conditions and compared it with RRR protocol. Simulation results showed that the network layer can achieve short average end to end delay and very low packet loss rate for alert packets. Although, routine data packets have medium quality of service due to the information gathering phase which broadcasts a request and waits for responses from all the neighboring nodes in each hop toward the sink. Furthermore, this phase introduces a certain overhead in terms of energy consumption. Despite this, the information gathering phase is necessary to enhance security and fault tolerance of the network layer.

References

[1] Zouinkhi A, Bajic E, Rondeau E, Abdelkrim MN. Simulation and modeling of active products cooperation for active security system management. *International Journal of Transactions on Systems, Signals and Devices*. 2011; 5(3): 1-23.

[2] Zouinkhi A, Bajic E, Rondeau E, Ben Gayed M, Abdelkrim MN. Ambient Intelligence Awareness context application in industrial storage. *Journal of Wireless Sensor Network*. 2011; 3(4): 134-145.
[3] Bajic E. A Service-Based Methodology for RFID-Smart Objects Interactions in Supply Chain. *International Journal of Multimedia and Ubiquitous Engineering*. 2009; 4(3): 37-56.
[4] Quanz B, Tsatsoulis C. *Determining Object Safety Using a Multiagent Collaborative System*. Second IEEE International Conference on Self-Adaptive and Self-Organizing Systems. Venice. 2008: 25-30.
[5] Strohbach M, Kortuem G, Gellersen H. *Cooperative artefacts - A framework for embedding knowledge in real world objects*. International Workshop on Smart Object Systems. Tokyo. 2005: 91-99.
[6] Strohbach M, Kortuem G, Gellersen H, Kray C. *Cooperative artefacts - Assessing real world situations with embedded technology*. 6th International Conference on Ubiquitous Computing. Nottingham. 2004: 250-267.
[7] Dobre D, Bajic E, Zouinkhi A. Active product modeling based on smart object concept: application to chemical security management. *European Journal of Automated Systems*. 2009; 43(4): 561-579.
[8] Chen J, Diaz M, Llopis L, Rubio B, Troya JM. 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*. 2011; 34(4): 1225-1239.
[9] Yuan T, Zhang S. *Secure Fault Tolerance in Wireless Sensor Networks*. 8th IEEE International Conference on Computer and Information Technology Workshops. Sydney. 2008: 477-482.
[10] Paradis L, Han Q. A Survey of Fault Management in Wireless Sensor Networks. *Journal of Network and Systems Management*. 2007; 15(2): 171-190.
[11] Mekki K, Zouinkhi A, Abdelkrim MN. *Wireless Sensor Network Layer Solution for Security Management*. 13th International conference on Sciences and Techniques of Automatic control & computer engineering. Monastir. 2012: 1323-1335.
[12] Alwan H, Agarwal A. *A Survey on Fault Tolerant Routing Techniques in Wireless Sensor Networks*. 3rd International Conference on Sensor Technologies and Applications. Athens. 2009: 366-371.
[13] Othman JB, Yahya B. Energy efficient and QoS based routing protocol for wireless sensor networks. *Journal of Parallel and Distributed Computing*. 2010; 70(8): 849-857.
[14] Norouzi A, Babamir FS, Zaim AH. A Novel Energy Efficient Routing Protocol in Wireless Sensor Networks. *Journal of Wireless Sensor Network*. 2011; 3(10): 350-359.
[15] Zhang X, He J, Wei Q. *Energy-Efficient Routing for Mobility Scenarios in Wireless Sensor Networks*. Proceedings of the 3rd International Symposium on Electronic Commerce and Security Workshops. Guangzhou. 2010: 80-83.
[16] Boulis A. *Castalia: a simulator for wireless sensor networks and body area networks – User's Manual*. Australia's Information and Communications Technology Research Centre (NICTA). 2011.
[17] Sundani H, Li H, Devabhaktuni V, Alam M, Bhattacharya P. Wireless Sensor Network Simulators A Survey and Comparisons. *International Journal of Computer Networks*. 2011; 2(5): 249-265.
[18] Zouinkhi A, Ltifi A, Bajic E, Zidi R, Ben Gayed M, Rondeau E, Abdelkrim MN. *Simulation of active products cooperation for active security management*. 8th International Conference of Modeling and Simulation. Hammamet. 2010: 1-9.
[19] Sen J, Ukil A. *An Adaptable and QoS-Aware Routing Protocol for Wireless Sensor Networks*. 1st International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronics Systems Technology. Aalborg. 2009: 767-771.
[20] Gelenbe E, Ngai E. *Adaptive QoS Routing for Significant Events in Wireless Sensor Networks*. 5th IEEE International Conference on Mobile AdHoc and Sensor Systems. Atlanta. 2008: 410-415.
[21] Hey L, Gelenbe E. *Adaptive Packet Prioritisation for Wireless Sensor Networks*. 5th Euro-NGI Conference on Next Generation Internet Networks. Aveiro. 2009: 1-7.