Routing Protocols for Border Surveillance Using ZigBee-Based Wireless Sensor Networks

Hoda Sharei-Amarghan[1], Alireza Keshavarz-Haddad[2], and Gaëtan Garraux[1]

[1] Centre de Recherche du Cyclotron, Université de Liege, Belgium
[2] School of Electrical and Computer Engineering, Shiraz Universtity, Iran
{h.sharei,ggarraux}@ulg.ac.be, keshavarz@shirazu.ac.ir

Abstract. In this paper, we study proper routing protocols for border surveillance missions using wireless sensor networks (WSNs). We assume that the sensor nodes are equipped with ZigBee transceivers for wireless communications. Three well known routing algorithms (AODV, DSR, and OLSR) are simulated in a WSN surveillance scenario. The performances of these routing algorithms are compared in terms of traffic load, delay, packet loss, and energy consumption. Our results indicate that DSR performs better than other algorithms for border surveillance applications. Moreover, a novel algorithm called "DSR_OP" is proposed for improving DSR routing in terms energy management in the network and extending the network life time. However Comparisons of WSN routing protocols (DSR, AODV, OLSR and others) are presented since many years ago, but there is no simulation with OPNET, so our novelty is that the validity of proposed method and the comparisons are confirmed by simulations in OPNET.

Keywords: WSN, routing protocols, OPNET, border surveillance.

1 Introduction

The technology of sensor networks has paved the way for an accurate and intangible monitoring of an environment or a process in a large physical space. Such networks are comprised of many sensor nodes. These nodes can cover a very large physical environment and gather information. Besides, nodes can help each other to gather the information in a centralized unit for decision making.

Therefore today, world is witnessing a growing interest on the topic of Wireless Sensor Networks (WSNs) and their applications in different fields. Some of these applications include monitoring environment, detection and identification of vehicles, hacker detection machine, sanitary and medical care, environmental control, monitoring the quality of agricultural products, etc [1]. The nodes of a WSN, encounter many limitations in energy consumption and processing power. Besides, the technology of WSN is not reached the required maturity yet. Therefore, these networks are facing many challenges such as: energy consumption, latency, scalability, lower cost, communication security, robustness against technical problems, and optimal routing algorithms.

A. Kwiecień, P. Gaj, and P. Stera (Eds.): CN 2013, CCIS 370, pp. 114–123, 2013.

In this paper, we study proper routing protocols for border surveillance missions using wireless sensor networks (WSNs). Border is defined as any physical region which we want to monitor it and dependent on its applications, the entrance or exit of an intruder should be detected. We assume that the sensor nodes are equipped with ZigBee transceivers for wireless communications. Using Zigbee protocol is due to its good feature in comparison with other protocols such as Wi-Fi.

There are various types of routing protocol. To have a good conception of two Proactive and Reactive catagory of routing, three well known routing algorithms (AODV, DSR, and OLSR) are simulated in a WSN surveillance scenario. The performances of these routing algorithms are compared in terms of traffic load, delay, packet loss, and energy consumption. Our results indicate that DSR performs better than other algorithms for border surveillance applications. Moreover, a novel algorithm called "DSR_OP" is proposed for improving DSR routing in terms of energy management in the network and extending the network life time. The validity of proposed method and the comparisons are confirmed by simulations in OPNET software.

The rest of this paper is organized as follows: in Sect. 2, border surveillance mission is briefly described. In Section 3, preliminaries on ZigBee standard and routing protocols are presented. A novel optimized routing protocol is proposed in Sect. 4, and simulation results and comparisons of different routing algorithms are presented in Sect. 5. Finally, conclusion and future work are included in Sect. 6.

2 Realated Works on Border Surveillance

The nodes of a WSN can be set up on the ground, in the air, under water, on a vehicle or even in a human's body [2]. In a border surveillance mission, the border is defined a physical region which should be monitored accurately, and dependent on its applications, the entrance or exit of an intruder should be detected. Basically, a linear structure of sensors can be used for coverage of a marginal region for detection of unauthorized activities and crossings [3,4]. A sample structure is shown in Fig. 1. As it shows, the network topology is a collection of nodes, randomly distributed throughout the area. Traffic is sent from all the sensor nodes to the sink. The region may be hundreds of kilometers, so it can be handled by partitioning the area into multiple parts and putting a sink for each area, then all sinks can send their information to a central sink [4].

The existing works that address the border surveillance problem, consider different aspects of it. One of the challenging subjects, which should be considered, is routing.

In [5] the quality of deployment issue is surveyed and analyzed. Suitable measures are discussed for the assessment of the deployment quality. Also some simulation results evaluate the impact of the node density on the detection ratio and on the time-to-detect an intruder. In [6], a method is proposed which specifies the breach paths and the deployment quality is defined as the minimum of

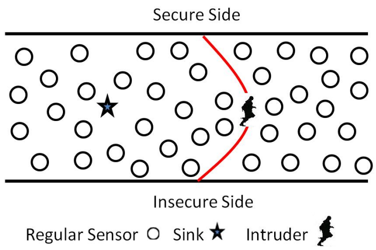

Fig. 1. Intruder detection in border surveillance scenario

the maximum detection probabilities on the breach paths in the presence of obstacles. In [7], two protocols are discussed to provide secure detection of trespass within the monitored area and also node failures. The sensor type which is used in this paper, is a simple Passive Infra-Red sensor (PIR sensor).

This paper focuses on routing w.r.t. the detection of intruder across an area monitored by a sensor network. The paper presents a novel algorithm called "DSR_OP" for improving DSR routing in terms of energy management in the network and extending the network life time, and evaluate the system by means of simulation.

3 Preliminaries

In this section, we present a brief introduction on ZigBee standard and three well-known routing protocols are described.

3.1 ZigBee Standard

In 2000, IEEE Standards introduced a low rate wireless personal area network standard, called 802.15.4. In 2003, Zigbee Alliance introduced Zigbee standard protocol. In a technical view, the stack of the ZigBee protocol has four main layers [8]: Physical layer, Media Access Control layer, Network layer, Application layer.

In particular, the first two layers are defined by IEEE 802.15.4, and the other two layers are defined by ZigBee alliance [9]. Network layer provides routing.

The main specifications which have concluded to the vast development of ZigBee standard include but are not limited to: low cost, security, self-healing, flexibility, and high potential for further developments, low power consumption, cheap and easy placement, using free radio bounds.

3.2 Routing Protocols

Routing is one of the key issues in WSN, so a lot of routing protocols has already been proposed [10,11]. Since our simulation region is two-dimensional, so it's better to apply two-dimensional routing protocols in order to increase efficiency. On the other hand, from the point of topological view, two main routing protocols are defined: Proactive, and Reactive. So, we use the AODV, and DSR protocols from Reactive category, and OLSR from Proactive categories and all are two-dimensional. In this subsection, we have a quick overview on these protocols.

Ad hoc On-Demand Distance Vector (AODV) is an on-demand routing algorithm in that it establishs a route to a destination only when a node wants to send a packet to that destination. Such behavior is very useful in networks with low traffic load to keep the routing overhead small. In AODV, every node maintains a table, which stores the information about the next hop to the destination and a sequence number which is received from the destination and ensures the freshness of routes. It is one of the key features of AODV, to avoid counting to infinity that is why it is loop free [12,13]. There are three AODV messages: Route Request (RREQs) which is sent when the host does not know the route to the needed destination host or the existed route is expired, Route Replies (RREPs) which is sent by a node when it has a route to the destination or to a node which has a route to destination, and Route Errors (RERRs) which is sent when the link breakage happens [14,15]. The route discovery is used by broadcasting the RREQ message to the neighbours with the requested destination sequence number, which prevents the old information to be replied to the request and also prevents looping problem. Each passed host makes update in their own routing table about the requested host. The route reply use RREP message that can be only generated by the destination host or the hosts who have the information that the destination host is alive and the connection is fresh [13].

Dynamic Source Routing (DSR) protocol is a reactive routing protocol and like AODV, is known as an on demand routing protocol. It is a source routing protocol which means that the originator of each packet determines an ordered list of nodes through which the packet must pass while traveling to the destination [16]. Each node along the route forwards the packet to the next hop. If, after a limited number of retransmissions of the packet, nest node doesn't recieve the packet, it returns a ROUTE ERROR to the original source of the packet and it means the link from itself to the next node was broken. The sender then removes this link from its Route Cache and tries to discover another route to this destination.

The DSR network is totally self organizing and self configuring. This protocol is comprised of two mechanisms: *Routh Discovery* and *Routh Maintanance*:

– Route discovery is used by a source node S, when it aims to find a route to a sink node D. This process is used just when no route from S to D is known in advance.
– Route maintenance is used to maintain and rebuild the routes which are already known. Therefore, when a path between S and D is know, due to some topological changes, this route might change. At this point, the maintenance algorithm might prefer to use replace another path from its database,

or start a discovering process. However, the Maintenance mechanism is only used when a package is already sent from S to D [14,15].

Optimized Link State Routing (OLSR) is a proactive routing protocol and is also called as table driven protocol because it permanently stores and updates its routing table and so the routes are always immediately available when needed [17,18]. It is an optimization of pure link state protocols in that it reduces the message overhead in the network by using MPR. MPRs are an arbitrary subset of one-hop neighbors of a node N while they could cover all the nodes that are two hops away. Each node in the network keeps a list of MPR nodes. Information is rebroadcast only by MPRs, Whenever a packet is received, a node checks its sender; if it is MPR, the packet is forwarded, otherwise the packet is discarded [14,15].

The performances of these routing algorithms are compared in terms of delay, traffic load, packet loss, and energy consumption. Therefore, a brief description of these parameters are presented as following [15]:

Delay – the time which is needed for packets to go from source to sink. This time is expressed in seconds, and have different kinds such as *processing delay*, *transmission delay*, and *propagation delay.*

Network Load. The network load shows the overall load (bps) of every node in a wireless network. In other words, the network load is the sent packets of the network in each second.

Packet loss which could occur for different reasons, such as the distance, battery depletion, collision and etc.

Energy consumption is the total amount of the consumed energy during simulation runtime.

Throughput. Throughput is defined as the ratio of the total data which reaches a receiver from the sender. Different factors affect this power, such as various changes in network topology, non-reliable links between nodes, limited bandwidth, and energy limitation. In every network, the highest throughput is the optimal one.

4 DSR_OP: A Novel Routing Protocol

In [19], Bashyal and Venayagamoorthy stated that knowing the number of alive nodes in a sensor network does not reveal how effective the system is, except when all, or none of the sensor nodes are alive. What should also be known is the distribution of the surviving nodes in the sensor network so that the area that is being monitored could be estimated. Figure 2 and the discussion following it show the importance of sensor node distribution for effectiveness of the wireless sensor network.

As we explained earlier in this paper, in DSR the source S might receive several routing replies from the network. In DSR protocol, it chooses the best route which is the shortest one, and saves the other routes in its table. Whenever a link breaks down, then it uses the stored data for choosing another route.

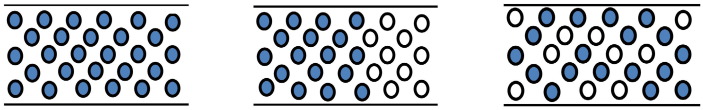

Fig. 2. Different possible sensor node distribution: (a) initial network with all surviving nodes, (b) uneven distribution of surviving sensor nodes, (c) more uniform distribution of surviving sensor nodes

Therefore, the nodes used for transferring data, are used as much as possible until they are impaired of any reason, including the battery loss, and at this time another route is replaced. So the effectiveness of the system is decreased.

The main objective of this novel optimized DSR algorithm (DSR-OP) is to address this problem and suggest a way for preventing the complete break down of nodes. In a normal situation the nodes will randomly get involved in a route and in case of failure of some nodes, the remaining nodes shall take the place. In our method, we suggest that when one node reaches a predefined threshold energy, it leaves the network for a random time period. In this way, other nodes of the network get involved, and the energy consumption is uniformly dispersed in the network.

5 Results

In this section, we first present detailed comparisons between three well known routing protocols, and then simulation results of the novel DSR_OP algorithm proposed in this paper are illustrated.

In all simulations of this subsection, following parameters are considered:

- Simulation region is 10 km × 4 km, it is selected a rectangular area to be similar to border.
- One sink node, one source node which generate traffic, and 28 normal nodes.
- Time of the simulation is 1:00 hour.

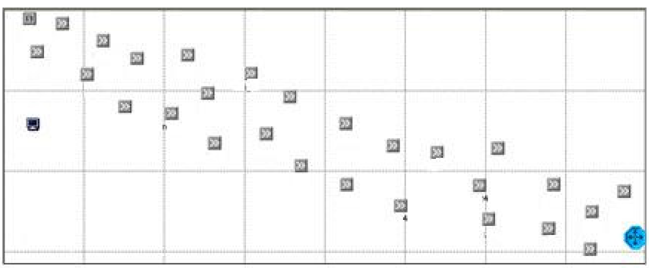

Fig. 3. Network topology

It's noteworthy to say that we have continuous communication between the fixed sender and the fixed receiver. Figure 3 shows the overall diagram of nodes deployment in the environment. As mentioned before, the parameters which will be used to compare three routing protocols are: network load, time delay, number of dropped packets, and energy consumption.

For all simulations, every parameters are considered to be unique in order to make the protocols comparable.

5.1 Comparison on DSR, AODV, and OLSR Protocols

In Figure 4a, the network load in terms of bit-per-second is illustrated for all three protocols. As expected, the OLSR protocol which is a proactive protocol, has the highest network load. After that, we have AODV, and finally DSR with less network loads.

In Figure 4b, the time averaged energy consumption is depicted in term of Joule. We can see that the highest energy consumption belongs to OLSR algorithm for its being proactive, and then AODV, and DSR are the next ones.

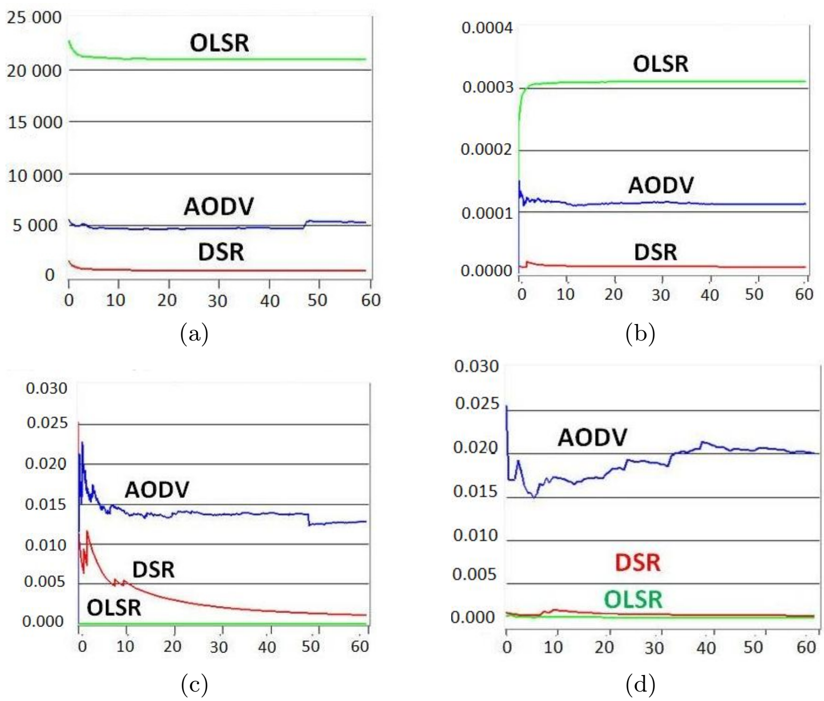

Fig. 4. Comparison of: (a) network load, (b) energy consumption, (c) dropped packets, (d) network delay (horizontal axis is time)

In Figure 4c, the time averaged dropped packets of the network are shown. Generally, this packet drop is a result of TTL time finishing. If one protocol, uses much time for choosing a route to sink, then the packets with limited life length are possible to be dropped. However, the effective protocols can decrease the packet dropping rate intelligently. Therefore, we anticipate that DSR has a lower packet drop rate than AODV [20]. In OLSR, almost no packet is dropped which is a result of predetermined routes for the source-sink connection. Besides, the AODV has the most packet dropping rate.

In Figure 4d, the time averaged overall delay of the network is shown. In AODV and DSR, based on its specific conditions, it takes a fixed time for the route from source to sink to be established. Therefore, the starting delay of the network is initialized by a large value [21]. Again, we see that OLSR has the least delay among other methods, and DSR has a less delay than AODV which are both of the on-demand kind.

Based on the presented simulation results in this subsection, it is intuitively clear that the DSR protocol has the best responses for a network with limited number of nodes.

5.2 Simulation Results for DSR_OP Protocol

As shown in previous subsection, the DSR routing technique has a higher performance than AODV and OLSR techniques. Therefore, in this subsection, we analyze performance of the proposed DSR_OP technique. The conditions for simulations of this subsection are considered as following:

- Simulation region is 10 km × 4 km.
- One sink node, two source node which generate traffic, and 4 normal node.
- Time of simulation is 20:00 hours.

In Figure 5a, the $n-3$ node is the bottleneck and both $N-1$ and $N-2$ sources communicate with the sink via $n-3$. In our proposed DSR_OP algorithm, in order to prevent $n-3$ from being died, after consumption of 30 % of the node battery, it is departed from the $n-4$ route for a random time. However, the link $n-3$ and $n-5$ remains connected. Therefore, $n-4$ is forced to maintain its connection with the sink (in this example, via $n-6$). The new links of the network are depicted in Fig. 5b.

After about 15 hours, with 30 % of energy consumption in node $n-3$, this node is withdrawn of the communication link and $n-6$ is used for establishing the connection. The energy consumption of node $n-3$ is depicted in Fig. 5c, which shows that its energy consumption is decreased after the 15th hour.

In Figure 5d, the routing traffic received in the nodes $n-3$ and $n-6$ are shown. After the 15th hour, traffic of $n-3$ is decreased and instead traffic of $n-6$ is increased.

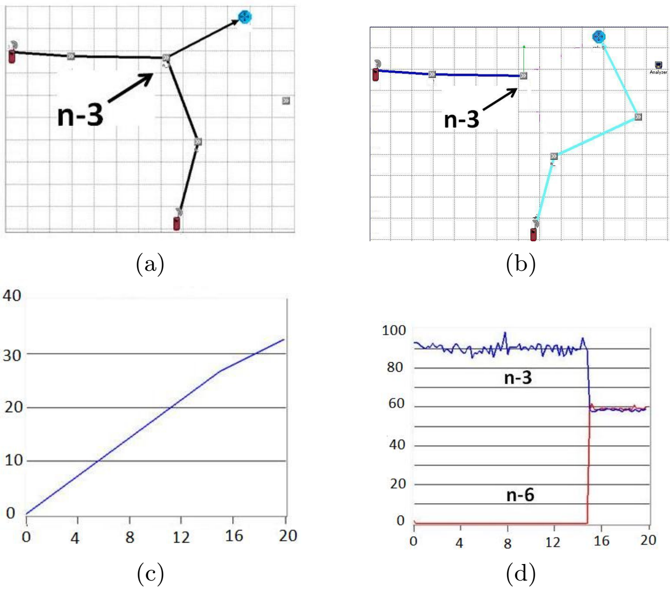

Fig. 5. Simulation of DSR_OP: (a) routes before leaving $n-3$, (b) routes after leaving $n-3$, (c) energy consumption in $n-3$, (d) routing traffic received by nodes $n-3$ and $n-6$ (horizontal axis is time)

6 Conclusion

In this paper, the routing protocols for ZigBee-based WSNs were studied, where the WSN was designed for a border surveillance scenario. Three well-known routing protocol were compared in detail which showes that DSR is suitable for border surveillance applications and outperforms in all specified scopes (i.e. traffic load, delay, packet loss, and energy consumption). Next, the AODV protocol has better result in comparison with OLSR. Finally, the OP-DSR was suggested as an improved version of the DSR in terms energy management in the network and extending the network life time. The validity checks were all confirmed by simulations in OPNET.

References

1. García-Hernández, F., Ibargüengoytia-González, H., García-Hernández, J., Pérez-Díaz, A.: Wireless Sensor Networks and Applications: a Survey. IJCSNS International Journal of Computer Science and Network Security 7(3) (March 2007)
2. Arora, A., et al.: A line in the sand: A wireless sensor network for target detection, classification, and tracking. Computer Networks Special Edition 46(5), 605–634 (2004)

3. Chen, Y., Chuah, C.-N., Zhao, Q.: Network Configuration For Optimal Utilization Efficiency of Wireless Sensor Networks. In: IEEE MILCOM 2005, Atlantic City, NJ, USA, pp. 17–20 (2005)
4. Jawhar, I., Mohamed, N.: A Hierarchical and Topological Classification of Linear Sensor Networks. In: Wireless Telecommunications Symposium, Prague, pp. 1–8 (2009)
5. Onur, E., et al.: Surveillance Wireless Sensor Networks: Deployment Quality Analysis. IEEE 21(6), 48–53 (2007)
6. Onur, E., et al.: Surveillance with wireless sensor networks in obstruction: Breach paths as watershed contours. Computer Networks Special Edition 50(3), 428–441 (2010)
7. Dudek, D., et al.: FleGSens – Secure Area Monitoring Using Wireless Sensor Networks. World Academy of Science, Engineering and Technology (2009)
8. http://www.zigbee.org/
9. Severino, R.: On the use of IEEE 802.15.4/ZigBee for Time-Sensitive Wireless Sensor Network Applications. In: School of Engineering. Polytechnic Institute of Porto (2008)
10. Al-Karaki, J.N., Kamal, A.E.: Routing techniques in wireless sensor networks: A survey. IEEE Wireless Communications 11(6), 6–28 (2004)
11. Akkaya, K., Younis, M.: A survey on routing protocols for wireless sensor networks. Ad Hoc Networks 3(3), 325–349 (2005)
12. Perkins, C., Belding-Royer, E., Das, S.: Ad hoc On-Demand Distance Vector (AODV) Routing (February 2003)
13. Huhtonen, A.: Comparing AODV and OLSR Routing Protocols. In: Seminar on Internetworking, Sjökulla (2004)
14. Holter, K.: Comparing AODV and OLSR. Helsinki University of Technology (2005)
15. Ali, S., Ali, A.: Performance Analysis of AODV, DSR and OLSR in MANET. Department of Computing Systems. School of Engineering Blekinge Institute of Technology, Sweden (2009)
16. Poonia, R., Sanghi, A.K., Singh, D.: DSR Routing Protocol in Wireless Ad-hoc tworks: Drop Analysis. International Journal of Computer Applications 14(7), 975–8887 (2011)
17. Clausen, T., Jacquet, P.: Optimized Link State Routing Protocol (OLSR). Project Hipercom, INRIA (2003)
18. Jacquet, P., et al.: Optimized link state routing protocol for ad hoc networks. In: IEEE INMIC 2001 (2001)
19. Bashyal, S., Venayagamoorthy, G.K.: Collaborative Routing Algorithm for Wireless Sensor Network Longevity. In: 3rd International Conference on Intelligent Sensors, Sensor Networks and Information (ISSNIP) (2007)
20. Narsimha, V.B.: Comparison of Routing Protocols in Mobile Ad Hoc Networks. Global Journal of Advanced Engineering Technologies (2012)
21. Ali, A., Akbar, Z.: Evaluation of AODV and DSR Routing Protocols of Wireless Sensor Networks for Monitoring Applications. Department of Electrical Engineering Blekinge Institute of Technology, Sweden (2009)