Adaptive Routing in Wireless Sensor Networks under Electromagnetic Interference

Trung Hoang*, Ruslan Kirichek*, Alexander Paramonov*, Franck Houndonougbo *, Andrey Koucheryavy*

*The Bonch-Bruevich State University of Telecommunications, 22 Prospekt Bolshevikov, St. Petersburg, Russia

hoangtrung@spbgut.ru, kirichek@sut.ru, alex-in-spb@yandex.ru, franckyrusse@spbgut.ru, akouch@mail.ru

***Abstract*—This paper is dedicated to the study of the functioning of wireless sensor networks under electromagnetic interference. As a result of electromagnetic interference, there is a degradation of channel quality down to interruption of nearby nodes, which leads to disruption of route. To maintain the stability of the network operation, a sensory field map is built based on RSSI measurements and an alternative route is created, that distant from the affected area. Thus, the problem of increasing the probability of data delivery in wireless sensor network under the effect of electromagnetic interference is solved.**

Keywords—wireless sensor network; sensor node; route; algorithm; electromagnetic interference; distance; location.

I. Introduction

At the present time, the development of the Internet of Things has significant influence on the development of communication networks [1]. The concept Internet of Things is based on the idea that the most important part of the customer base networks will constitute things. The technological base for the introduction of the concept Internet of Things currently is wireless sensor networks, which belong to a class of ubiquitous sensor networks [2-5]. Wireless sensor networks have a number of features compared to the existing networks, the keys of which are their self-organization and low power consumption. Great interest to the study of such networks is caused mostly by wide possibilities of their application: environment monitoring, industrial plant monitoring, transport monitoring, intrusion detection and target tracking, fire security, automobile production, medicine and others [6-8].

In the connection with various tasks, which are performed (WSN) in different fields, the task of ensuring the ability of WSN to perform specified functions in a variety of conditions, including the presence of external destabilizing factors are relevant. One of the new types of destabilizing influences in the wireless sensor networks is electromagnetic interference (EMI) [9-12]. Influence of interference sources in the WSN creates a threat of infringement of the entire network or parts of it. As a result of such exposure, it violates not only the functioning of the individual sensor nodes, but also the integrity of the wireless sensor network and leads to the degradation of channel quality located in the electromagnetic impact zone [13-16]. Thus, it is relevant to the development of methods to ensure maximum stability functioning of WSN under EMI.

II. Statement of the Research Problem

In the presence of significant electromagnetic interference, reaction of WSN is to rebuild route traffic transmission (configuration changes), which is produced by the used routing protocol. The network-based security for sensor networks has specific features, which are covered in ITU-T Recommendation X.1312 [17]. In this particular case, the network expends the operation (and energy). Periodic or random interference can cause excessive traffic congestion on the network by causing rebuilds of the routes and as a consequence, the quality of service desired traffic and increase energy expenditure has been reduced. To ensure the functioning of the WSN, it should be possible to select a configuration that provides the most sustainable (stable) network conditions, in which the maximum interference is reduced.

ZigBee network can be considered as WSN, since ZigBee is an open standard for wireless communications for collection and management systems. Protocol ZigBee allows creating self-organizing and self-healing wireless networks with automatic retransmission of messages, with support for battery and mobile nodes [18]. We assume that for network operation we only need one coordinator (gateway).

To maintain the functioning of the WSN under EMI, it is supposed to solve the following tasks:

- Developing an analytical model for selection of routes based on network parameters and geolocation of sensor nodes.
- Carrying out an experiment on the geolocation of sensor nodes on the base of ZigBee network.

III. Analytical Model for Selecting Routes Based on Network Parameters and Geolocation of Sensor Nodes

In the presence of influence source in the network's service zone, some proportion of nodes may not be available to reach, or the quality of connection with those nodes could significantly worsen. If there is a focused interference source in the network, its coordinates (x_S, y_S) can be estimated using the method described in [19]. In this case, to ensure that the network functions properly, routes between nodes should be changed. When solving this task a formal search of the shortest paths will be used to find the routes according to the selected criteria, such as, channel quality indicators between nodes. However, the presence of periodic or random noise may pass unnoticed, if at the time of search such interference was not observed. Also,

accidental changes of the degree interference on the quality of connection are possible due to changes in the reception conditions, and this probability is higher for the nodes that are located closer to the interference source. So, on that basis, it can be assumed that in some cases, when choosing the route, the geographical proximity of its elements to the interference source should be taken into account.

It is possible to consider two options to solve this problem:

- Finding several (k) shortest routes in the network and choosing elements which are distant from the noise source;
- Finding the shortest route on the changed initial data considering the proximity of the network elements to the interference source.

In the first case, we can use a known algorithm, such as Yen's algorithm [20], to find k shortest paths. The proximity assessment of the route elements to the interference source can be considered as the sum of the squares of the distances from the route nodes to the interference source. For r[th] route this sum will be equal to:

$$\delta_r = \sum_i^{n_r}[(x_i - x_S)^2 + (y_i - y_S)^2] \qquad (1)$$

where (x_S, y_S) is coordinate assessment of interference source,

(x_i, y_i) is coordinate of i[th] node in r[th] route,

n_r is amount of nodes in r[th] route.

Route selection is made according to the criterion:

$$R = arg\, min_r \delta_r, r = 1 \dots k \qquad (2)$$

The present method guarantees the route finding if the Yen's algorithm finds at least one route. However, it is not priori known which value of k should be chosen for the search. A small value of k cannot give the desired results (all routes can be close to the interference source), for large values of k may require a lot of heavy workload to their search.

In connection with the second variant, it is possible to consider possibility to change the initial matrix of distances between nodes. The matrix should be changed so that the distance to adjacent nodes from the nodes located closer to the interference source, has increased to a greater extent than to nodes, which are distant from the interference source. According to the most models of radio propagation, it can be assumed that the extent of influence source on the network nodes is inversely proportional to the square of the distance to them. Based on this assumption, we modify the distance between nodes $\tilde{d}_{ij}$ according to the:

$$\tilde{d}_{ij} = \tilde{d}_{ji} = \begin{cases} \frac{d_{ij}}{a + d^2_{iS}} & d_{ij} \le R \\ \infty & d_{ij} > R \end{cases}, i, j = 1 \dots n \qquad (3)$$

where d_{iS} is distance from i[th] node to interference source,

n is amount of nodes in the network,

a is coefficient determining the sensitivity of route selection to interference source,

R is communication range of nodes.

To find the shortest routes on the modified matrix we can use any of the shortest paths search algorithm.

Figure 1 shows an example of selecting the shortest paths (Floyd's algorithm was used) between the vertices b and t without regarding to the interference source (p1), considering interference source, the value of the constant a = 2000 (p2), a value of the constant a = 1 (p3). Interference source in the figure is marked with symbol S. Network is situated on the territory of 200 x 200 m, the radius of the communication center 60 m.

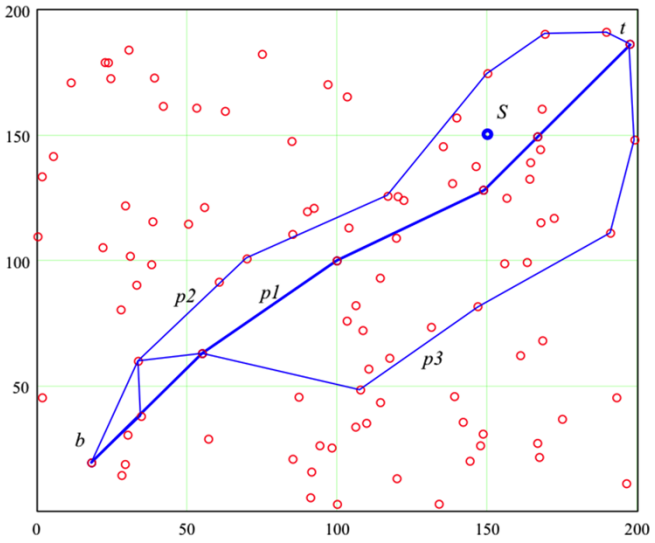

Fig. 1. Change of route considering the interference source

As can be seen from the figure, in the presence of the interference source, the route has been chosen, elements of which are located at a distant from this source. Beside, the more distant of elements of the selected route from the interference source, the smaller the value of the constant a.

It should be noted that when applying the transformation (3) will increase the length (number of hops) of the route. In the above example the shortest route (without the interference source) is composed of three sections (hops) and "bypass" routes contain 4 hops.

IV. Experiment on the Geolocation of Sensor Nodes on the Base of ZigBee Network

We assume it is possible to determine the coordinates of the routers and coordinator, for example, using GPS module installed in them.

Figure 2 presents ZigBee network scheme on the plane.

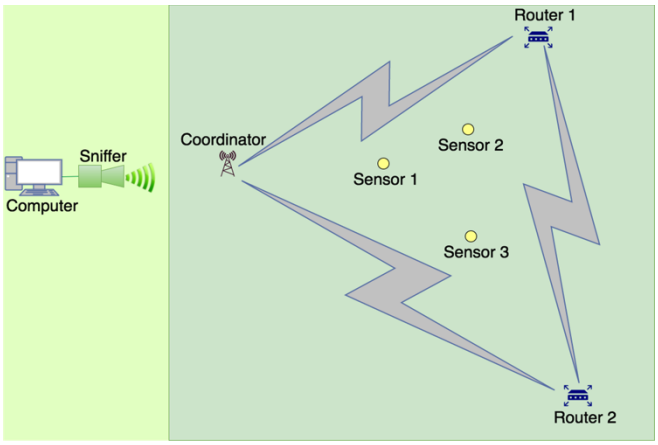

Fig. 2. ZigBee network model

To determine the coordinates of an unknown point in two-dimensional space is necessary to measure the distance to it by any three points with known coordinates.

To calculate the coordinates of the nodes, a trilateration method can be used for three defined nodes. In general, the problem is solved by minimizing multilateration expression:

$$(x_S, y_S) = arg\ min \sum_{i=1}^{k} \left(\sqrt{(x_i - x_S)^2 + (y_i - y_S)^2} - d(p_i, p_S)\right)^2 \quad (4)$$

where k is the number of neighbor node,

$d(p_i, p_S)$ is distance assessment between nodes,

x_S, y_S is the unknown coordinates of nodes

x_i, y_i is coordinates of neighbor nodes.

Substituting into formula of estimate distance between two points in two-dimensional space and the values of the coordinates of defined nodes, we obtain a system of three equations with three unknowns, deciding which receives an evaluation of the coordinates of unknown point. Thus, in the available system, a coordinate of new node is positioned.

One of the parameters of the radio channel at the receiving point is the indicator of the level of the received signal RSSI (Received Signal Strength Indicator). Table 1 shows the results of RSSI measurements depending on the distance between the two devices:

TABLE I. DEPENDENCE OF THE DISTANCE BETWEEN TWO DEVICES BY RSSI

d, m	RSSI, dBm
0,1	-17
1	-39
2	-57
4	-60
6	-63
8	-69
10	-70
15	-73
20	-80
30	-89

By approximating the obtained values of the logarithmic function we obtain the distance dependence of the RSSI values:

$$d = -12{,}12\ ln(RSSI) - 43{,}445 \quad (5)$$

In the real case, to determine the values of d, we carry out an experiment on the deployed network. The measurement results are shown in Table. 2

TABLE II. DEPENDENCE OF RSSI TO EACH SENSOR

	RSSI, dBm
Coordinator – sensor 1	-75,2
Coordinator – sensor 2	-79
Coordinator – sensor 3	-74,6
Router 1 – sensor 1	-56,8
Router 1 – sensor 2	-56,4
Router 1 – sensor 3	-56
Router 2 – sensor 1	-74,6
Router 2 – sensor 2	-70,8
Router 2 – sensor 3	-72,5

According to (5) determining the distance from each sensor, the results of which are shown in table 3

TABLE III. DISTANCE TO EACH SENSOR

	d, m
Coordinator – sensor 1	13,7
Coordinator – sensor 2	18,8
Coordinator – sensor 3	13,1
Router 1 – sensor 1	3,0
Router 1 – sensor 2	2,9
Router 1 – sensor 3	2,8
Router 2 – sensor 1	13,1
Router 2 – sensor 2	9,5
Router 2 – sensor 3	10,9

Figure 3 shows the network card in the presence of the distance from any three points with known coordinates. In this

experiment, three coordinates of any points, respectively coordinator [0, 0], router 1 [20 2], router 2 [2, 25]

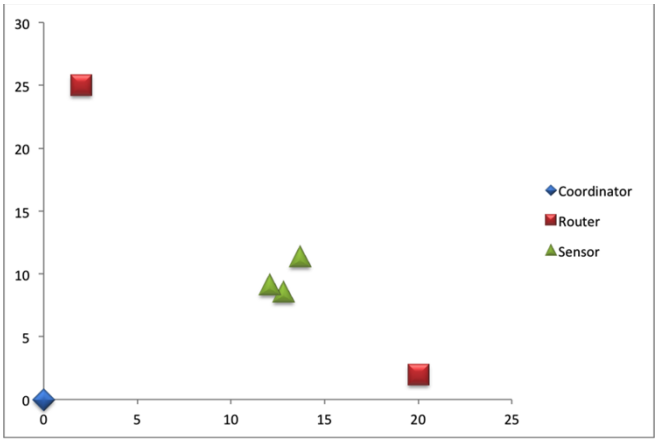

Fig. 3. Wireless sensor network map

V. CONCLUSION

In the study, the following results were obtained:

1. To solve the problem of stability of WSN in electromagnetic interference conditions, we should ensure the choice for the most stable of network configuration.
2. The proposed solution to this problem is based on the calculation the coordinates of the nodes, localization of interference source and route selection, geographically of which is most distant from the interference source.
3. The solution to this problem is using a multilateration method in the presence of several (minimum of three) nodes with known coordinates. To measure the distances to those nodes using an analysis of RSSI values.
4. Based on the calculated of the coordinates of nodes and data of the localization of the interference source is proposed to construct a modified matrix with distances between nodes considering the influence of the interference source.
5. Based on the modified matrix, by using a shortest path search algorithm, routes between nodes are selected. These obtained routes are the shortest distance from the source of interference, which improves the stability of the structure of the network, by reducing the impact of noise on the traffic transmission routes

REFERENCES

[1] Recommendation Y.2060. Overview of Internet of Things. ITU-T, February 2012, Geneva.

[2] Kirichek, R., Koucheryavy, A.: Internet of things laboratory test bed. In: Zeng, Q.A. (ed.) Wireless Communications, Networking and Applications. LNEE, vol. 348, pp. 485–494, 2016.

[3] Koucheryavy A., Vladyko A., Kirichek R. State of the Art and Research Challenges for Public Flying Ubiquitous Sensor Networks. Lecture Notes in Computer Science. Vol. 9247, pp.299–308, 2015.

[4] Kirichek R., Paramonov A., Koucheryavy A. Swarm of Public Unmanned Aerial Vehicles as a Queuing Network. Communications in Computer and Information Science. Vol. 601, pp. 111-120, 2016.

[5] Kirichek R. The model of data delivery from the wireless body area network to the cloud server with the use of unmanned aerial vehicles. Proceedings of the European Council for Modeling and Simulation, ECMS 2016, pp. 603-606, 2016.

[6] Kirichek, R., Vladyko, A., Zakharov, M., Koucheryavy, A.: Model networks for internet of things and SDN. In: 2016 18th International Conference on Advanced Communication Technology (ICACT), pp. 76–79, 2016

[7] Vladyko A., Muthanna A., Kirichek R. Comprehensive SDN Testing Based on Model Network. Lecture Notes in Computer Science. Vol. 9870, pp.539-549, 2016.

[8] KIRICHEK, Ruslan, et al. Development of a node-positioning algorithm for wireless sensor networks in 3D space. In: *2016 18th International Conference on Advanced Communication Technology (ICACT)*. IEEE, 2016. p. 279-282.

[9] Li, Xinfeng, et al. Research on in-band electromagnetic interference effect of communication system. In: *Advanced Materials and Processes for RF and THz Applications (IMWS-AMP), 2016 IEEE MTT-S International Microwave Workshop Series on*. IEEE, 2016. p. 1-4.

[10] Hwang, Jung-Hwan, et al. "Effect of Electromagnetic Interference on Human Body Communication." *IEEE Transactions on Electromagnetic Compatibility*. IEEE, 2016. p. 1-10.

[11] Betta, Giovanni, et al. "Experimental investigation of the electromagnetic interference of ZigBee transmitters on measurement instruments." *IEEE Transactions on Instrumentation and Measurement* 57.10 (2008): 2118-2127.

[12] DELSING, J., et al. Susceptibility of sensor networks to intentional electromagnetic interference. In: *2006 17th International Zurich Symposium on Electromagnetic Compatibility*. IEEE, 2006. p. 172-175.

[13] Radasky, William A. The threat of intentional interference (IEMI) to wired and wireless systems. In: *2006 17th International Zurich Symposium on Electromagnetic Compatibility*. IEEE, 2006. p. 160-163.

[14] KUNE, Denis Foo, et al. Ghost talk: Mitigating EMI signal injection attacks against analog sensors. In: *Security and Privacy (SP), 2013 IEEE Symposium on*. IEEE, 2013. p. 145-159.

[15] Zhukovsky M., Kirichek R., Larionov S., Chvanov V. Testing of Technical Security Equipment for Stability to Intentional Electromagnetic Interference // Proceedings of EMC Europe 2011 York - 10th International Symposium on Electromagnetic Compatibility 2011. pp. 820-823.

[16] Hoang T., Kirichek R., Paramonov A., Koucheryavy A. Influence of Intentional Electromagnetic Interference on the functioning of the Terrestrial Segment of Flying Ubiquitous Sensor Network // Lecture Notes in Electrical Engineering. 2016. Vol. 376. pp. 1249-1259.

[17] Recommendation, X.1312 “Ubiquitous sensor network middleware security guidelines" ITU-T (2011).

[18] Mukherji, Arup, and Subbanarasaiah Sadu. "ZigBee performance analysis."*Wireless Communications, Signal Processing and Networking (WiSPNET), International Conference on*. IEEE, 2016.

[19] Hoang T., Kirichek R., Paramonov A., Koucheryavy A. Supernodes-Based Solution for Terrestrial Segment of Flying Ubiquitous Sensor Network Under Intentional Electromagnetic Interference. Lecture Notes in Computer Science. Vol. 9870, pp. 351-359, 2016.

[20] N. Christofides Graph Theory. An Algorithmic Approach. Hardcover – October, 1975.