Lightweight QoE Driven and Invulnerability Guarantee Opportunistic Control Scheme for Wireless Sensor Networks

http://dx.doi.org/10.3991/ijoe.v12i08.5726

Yong Jin[1], Jian Cai[2], Huan Dai[1], Kaijian Xia[2], Ping Xu[3]
[1]Changshu Institute of Technology, Changshu, China
[2]Changshu No.1 People's Hospital, Jiangsu, Changshu, China
[3]Nanjing Army Command College, Nanjng, China.

***Abstract*—this paper proposed the lightweight QoE driven adaptive invulnerability wireless communication control method, including the wireless communication terminal equipment with invulnerability antenna. According to the quality of wireless network channel quality, the lightweight QoE driven scheme was developed. According to user needs, the quality of the network, survivable ability of wireless communication terminal and wireless communication survivability requirements, we proposed three matching rules by considering the wireless hop number, data size and life cycle. The experiments demonstrated that the proposed scheme can optimize wireless communication terminal equipment and wireless opportunistic communication network construction, guarantee the user experience quality and improve wireless communication network survivability.**

***Index Terms*—Wireless sensor networks, Opportunistic Control, Lightweight QoE Driven, Invulnerability guarantee.**

I. INTRODUCTION

Opportunistic network technology needs to take up a large number of resources and equipment of wireless terminals, especially the wireless signal transmission and reception module. At the same time, the wireless communication network topology has dynamic characteristics. User experience quality has time variability characteristic. How to seek optimal control scheme between network robustness, user requirements and dynamic changes of wireless networks is a key problem. The existing intelligent control method considered one or two optimization goals of QoE (Quality of Experience) guarantee [1], lifetime [2] [3] and QoS (Quality of Service) support. When considering the three goals at the same time, it is difficult to satisfy the user experience quality directly [4] [5], which leads to the consumption of a large number of resources in the wireless communication network.

How to improve the implementation efficiency of network based on the quality of user experience has been the key issue. Gómez G et al [6] proposed a novel architecture based on quality of experience (QoE) awareness for mobile operator networks. In article [7], the uncertainties of QoE model and playout time were considered jointly for resolving the inherent tension between the test and optimization. A mixed preemptive and non-preemptive resume priority (PRP/NPRP) M/G/1 queuing model was developed by Wu Y et.al [8] for modeling the spectrum usage behavior. A novel architecture was proposed by Lin K et.al[9] for guaranteeing 5G spectrum management based on the various requirements for QoE as the design objective. The self-optimisation video streaming use case was researched by Nightingale J et.al[10] for addressing the network management. The authors combined the monitoring and analysis components for facilitating the user-oriented, quality of experience (QoE) and energy-aware approach. However, Over QoE protection may reduce the life cycle. So we studied the strength of QoE protection.

About Invulnerability guarantee issue, Zhao D J et.al [11] studied the invulnerability method of space information network based on the composition and characteristic of space information network, which includes three research levels from microcosmic to macrocosmic. Cheng Ju et.al [12] studied the opinion dynamics in social networks and present a new strategy to control the invasive opinion. Qin X H et.al [13] abstracted enterprise marketing network as complex network for improving the management level of enterprise marketing network. In article [14], the invulnerability problem of combined operations combat network was studied under repair. A key distribution scheme was researched by You L et.al [15] for WSN based on hash chains and deployment knowledge. However, the above researches ignored the relationship between Invulnerability guarantee and QoS support.

For improving the network efficiency, a new method for opportunistic power control was proposed by Javan M R et.al [16] in multi-carrier interference channels for delay-tolerant data services. An Opportunistic Access Scheme was discussed in article [17] through Distributed Interference Control for MIMO Cognitive Nodes. The impacts of cooperative communications were studied in article [18] on topology control in wireless ad hoc networks (WANETs) and the authors proposed a distributed cooperative topology control scheme with opportunistic IC. An automatic control framework was proposed by De S C F et.al [19] to address the problem of distributed and opportunistic transmission power control in wireless communication networks. According to the Energy Conservation requirements in Hybrid Cellular Network, the distributed power control was demonstrated in article [20] with device-to-device communication. The optimal design of channel-aware scheduling and power allocation was formulated in article [21], which could minimize the total power consumption and satisfy the control performance requirements.

In this paper, we analyze the opportunistic control scheme for wireless sensor networks, by considering the QoE driven scheme and invulnerability guarantee issue. We use analytical and simulation approaches to compare and transmission delay, bit error rate, and lifetime of QoE driven alone and the proposed scheme with distance and channel quality. The results show that our proposed mechanism is capable of utilizing the network resource and achieve good invulnerability guarantee for wireless sensor networks.

II. LIGHTWEIGHT QOE DRIVEN SCHEME

In wireless sensor networks, we assume that the set NS is composed of n neighbor node of data sending node S. The state of wireless communication node is defined with distance d, antenna area TA_S and frequency f_{OC}. The antenna gain of S node is G_t. The work voltage of S node is V_m. The sending power of S node is P_t. The antenna gain of node in NS set is G_r. The remaining energy of node in NS set is E_S. The work voltage of node in NS set is V_S. The receiving power of node in NS set is P_S. The antenna signal angle between S node and node in NS set is w. According to formula (1), we can obtain the effective energy ratio μE_R of nodes in NS set. We also can calculate the effective voltage ratio μV_R of nodes in NS set based on formula (2) and the effective power ratio $\mu P_R$of nodes in NS set based on formula (3).

$$\mu E_R = \frac{P_t G_t}{4\pi d^2 E_S} \quad (1)$$

$$\mu V_R = \frac{V_m}{V_S}\cos\left(\omega t + TA_S\pi\right) \quad (2)$$

$$\mu P_R = \frac{P_t}{P_S} G_r \left| f_{OC} \right|^2 \quad (3)$$

According to formula (1), (2) and (3), the network quality could be evaluated. Figure 2 shows the influence of communication distance d on effective energy ratioμE_R. Figure 3 gives the influence of antenna area TA_S on effective voltage μV_R. Figure 4 shows the influence of working frequency f_{OC} on effective power μP_R.

From figure 2, we found that the effective energy μE_R would be increasing with the rising of SNR (Signal to Noise Ratio). When the distance between S node and nodes in NS set is bigger, the effective ratio μE_R would be also increasing. The higher the energy utilization rate the smaller the distance with the same network quality.

When the network quality is poorer, distance effect on energy utilization rate is low. When the network has good quality, short distance communication could improve energy utilization ratio. Here, the opportunity network has better anti-destroying ability. The above analysis shows that the optimal neighbor nodes should be selected to comprise the opportunistic network based on network quality.

From figure 3, the effective voltage would be increasing by improving the network quality. When the network quality reaches a certain value, the effective voltage would be stable. The effective voltage would be bigger with the increasing of antenna area. However, when the network quality is better, there is the small impact of antenna area on effective voltage with better network quality. So, we should consider the antenna area when we recombine the opportunistic network.

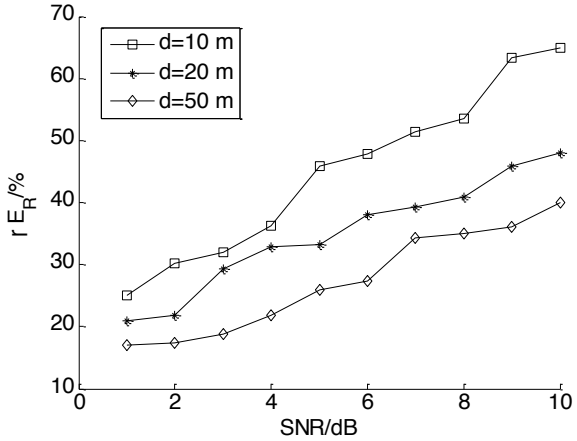


Figure 1. analysis of effective energy.

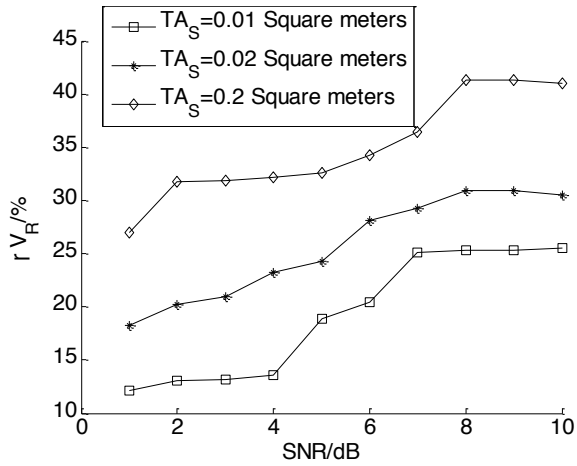


Figure 2. analysis of effective voltage

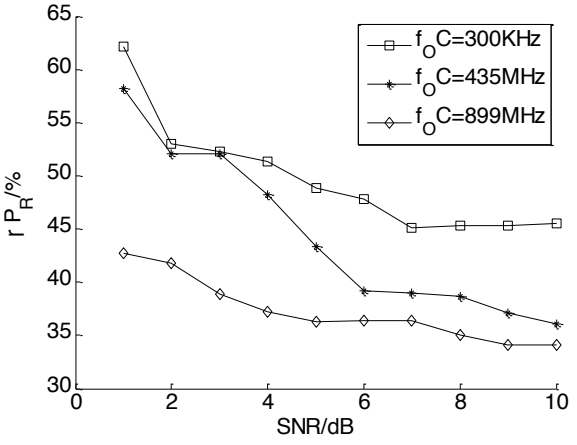


Figure 3. analysis of effective power

Figure 4 showed that the higher the working frequency, the smaller the effective power ratio when network quality is better. Therefore, we could improve the effective power and the invulnerability of the opportunistic network by adjusting the working frequency of the nodes.

In conclusion, the node selection scheme of opportunistic network based on the effective energy ratioμE_R, effective voltage ratio μV_R and effective power ratio μP_R is as follows.

Step 1: the effective energy, voltage and power of nodes in NS set could be calculated based on formula (1), (2) and (3).

Step 2: evaluation threshold of network quality could be obtained by formula (4).

$$ET_{NQ} = \frac{1}{n}\left(\sum_{i=1}^{n}\left(\mu E_R(i) + \mu V_R(i) + \mu P_R(i)\right)\right) \quad (4)$$

Step 3: the average SNR_{avg} could be obtained by measurement. If SNR_{avg} is larger than ET_{NQ}, go to the step 4. Otherwise, go to the step 5.

Step 4: the nodes would be selected, effective energy ratio, voltage ratio and power ratio of which are larger than $\frac{1}{n}\left(\sum_{i=1}^{n}\left(\mu E_R(i)\right)\right)$, $\frac{1}{n}\left(\sum_{i=1}^{n}\left(\mu P_R(i)\right)\right)$ and $\frac{1}{n}\left(\sum_{i=1}^{n}\left(\mu P_R(i)\right)\right)$ respectively, to rebuild the opportunistic network nodes set NS_1.

Step 5: the nodes would be selected, distance d of which is smaller than $\frac{1}{n}\sum_{i=1}^{n}(d)$, antenna area of which is larger than $\frac{1}{n}\sum_{i=1}^{n} TA_S$ and working frequency of which is smaller than $\frac{1}{n}\sum_{i=1}^{n} f_{OC}$, to rebuild the opportunistic network nodes set NS_1.

Step 6: send NS_1 set to sending node S.

Assuming that channel quality of the receiving node U is SNRU and lightweight QoE driven weight is α. Let denote the tolerance factor of data different types of U. Quality of experience of users is defined with the bear delay DU, and tolerate data quantity DSU and the transmission time TDU, which could be obtained with formula (5), (6) and (7).

$$DU = \frac{1}{TM_U}\sqrt{\frac{C_U}{M_U}\beta DM_U} \quad (5)$$

$$DSU = \beta TM_U\sqrt{\frac{\left|TV_U C_U - DM_U\right|^2}{M_U}} \quad (6)$$

$$TDU = TM_U\sqrt{\frac{\left|C_U - \frac{M_U}{TV_U}\right|^2 \beta}{M_U}} \quad (7)$$

Here, let C_U denote the computing ability of U and M_U denote storing ability of U. Let DM_U denote the displaying ability of U and TV_U denote wireless transmission port receiving rate of U. TM_U is the user number. The above parameters could be got from U.

Above all, the algorithm process of lightweight QoE driven scheme is as follows.

(1) The channel quality of U SNR_U is obtained from measurement.

(2) If SNR_U is smaller than $\frac{1}{n}\left(\sum_{i=1}^{n}\left(\mu E_R(i) + \mu V_R(i) + \mu P_R(i)\right)\right)$, $\alpha \in (0.5,1]$ and $\beta \in [1,1.5)$. Otherwise, αis 0.5 and β is 1.5.

(3) According to formula (5), (6) and (7), the value of DU, DSU and TUD could be obtained.

(4) Send the parameters value of step (3) to sending node S.

III. INVULNERABILITY GUARANTEE OPPORTUNISTIC CONTROL SCHEME

Based on the nodes set NS_1 from section 2, we designed the following three matching rules for satisfy the QoE driven and invulnerability requirements. These rules could optimize the opportunistic network, which is denoted by NS_F.

Matching rule 1: Maximum hops and tolerate delay matching. That means $HOP_{max}*T_{HOP}=DU$. Here, let HOP_{max} denote the maximum hops. Let T_{HOP} denote the one hop delay. Sending power of each node of NS_F set must be larger than minimum power $\bar{P}_{min}$, which is given by formula (7).

$$\bar{P}_{min} = \frac{1}{2}\left|P_S\right|^2\left|\frac{\sum_{i=1}^{m} P_i}{P_{max} + P_{min}}\right|^2 \frac{m}{\sum_{i=1}^{m} P_i} \quad (7)$$

Here, P_{max} is the maximum power of nodes in NS_1 set. P_{min} is the minimum power of nodes in NS_1 set.

Matching rule 2: The smallest size and tolerance data matching. That means $DS_{min}=DSU$. Here, DS_{min} is the minimum data scale of opportunistic network. The smallest data size of NS_F must be greater than or equal to the minimum required data amount of the user. The average transmission power P_{avg} and the average packet loss rate PER_{avg} have to satisfy the relationship as formula (8).

$$\begin{cases} P_{avg} = \frac{1}{2}\left|P_S\right|^2 \frac{m\sum_{i=1}^{m} DS_i\left(1 - PER_{avg}\right)}{\left(P_{min}^{\ 2} + P_{max}^{\ 2}\right) HOP_{max} T_{HOP}} \\ PER_{avg} = \frac{m}{4}\left|\frac{P_{avg}}{\sum_{i=1}^{m} P_i}\right| \end{cases} \quad (8)$$

Here, DS_i is the sending data scale of i node in NS_F. Let P_i denote the sending power of i node.

Matching rule 3: Minimum life cycle and tolerance transmission length matching. That means $LC_{min}=TDU$. Here, LC_{min} is the Minimum life cycle of opportunistic. The average energy E_{net} and working voltage V_{net} have to satisfy the relationship as formula (9).

$$\begin{cases} E_{net} = \frac{\sum_{i=1}^{m} E_i}{2\pi d^2 G_U} \\ V_{net} = \frac{V_m}{\sum_{i=1}^{m} E_i}\sqrt{G_U \cos\left(\omega t + TA_S 2\pi\right)} \end{cases} \quad (9)$$

Here, let E_i denote the energy of i node.

According to the above matching rules, we improve the opportunistic network NS_1 set based on the following steps.

Step 1. Computing the maximum hops of NS_1 set. If the hop number matches the rule 1 NS_F=NS_1, go to step5. Otherwise, NS_1 would be improved according to formula (7). We will obtain the optimized NS_2 set.

Step 2. Computing the minimum data scale of NS_2. If the data scale matches the rule 2 NS_F=NS_2. Otherwise, NS_2 would be improved according to formula (8). We will obtain the optimized NS_3 set.

Step 3. Computing the minimum life cycle of NS_3. If the life cycle matches the rule 3 NS_F=NS_3. Otherwise, NS_3 would be improved according to formula (9). We will obtain the optimized NS_4 set.

Step 4. NS_F=NS_4

Step 5. Sending the NS_F to the sending node S.

For implementing the three matching rules, we designed the antenna pair with invulnerability as shown in figure 4 and 5. The antenna pair of figure 4 would be deployed in S. The antenna pair of figure 5 would be deployed in nodes of opportunistic network. Figure 6 demonstrate the invulnerability opportunistic coupling way for supporting the above request-response antenna.

In figure 4, end a and b are the opportunistic coupling ports, which are used to receiving the feedback signal from neighbor nodes or users. End c is the internal components for enhancing the antenna information. End d is the internal components for enhancing the invulnerability. Port is the serial port or wireless module, which is used to connected with the servers. The proposed opportunistic scheme algorithm is stored in EEPROM. MCU is the micro controller, which is used to control the working sequence and task assignment of the antennas.

In figure 5, port is used to obtain the equipment electrical property parameters from opportunistic network. EEPROM is used to store the opportunistic control algorithm. Component d, e and f are the invulnerability guarantee parts, which could amplify the signal and coupling modulation. End h and l are the antenna pair ends, which would couple modulate with end *a* and *b* in figure 4. In figure 6, there is the opportunistic coupling equivalent circuit between sending node and node in opportunistic network.

Based on the research results of section 2 and this section, we propose the opportunistic control scheme with lightweight QoE driven and invulnerability guarantee, as shown in figure 7.

IV. PERFORMANCE EVALUATION

In this section, we designed the experiment for evaluating and analyzing the QoS and QoE guarantee ability, as well as invulnerability guarantee of the proposed scheme denoted as LQIOC (Lightweight QoE driven and Invulnerability guarantee Opportunistic Control scheme) with different distance and channel quality. We also compare the above performance with QoE alone scheme. The parameters of experiment are given by Table 1. The parameter metrics are transmission delay, lifetime and bit error rate.

Figure 8 gives the performance comparison results of QoE alone scheme and proposed LQIOC as terms of real time, reliability and lifetime. We found that the performance of LQIOC is superior to the QoE alone. About short distance communication, the proposed scheme can reduce bit error rate and prolong the network life cycle by

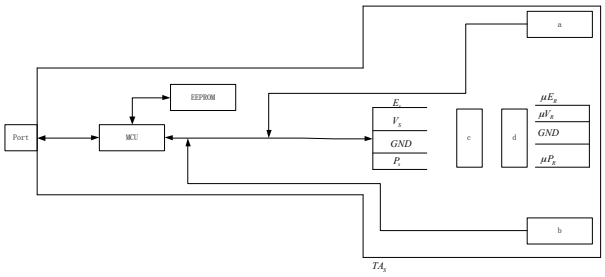


Figure 4. Invulnerability request antenna

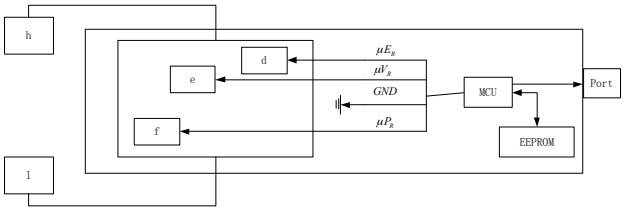


Figure 5. Invulnerability response antenna

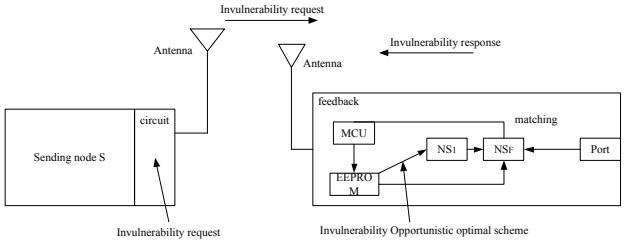


Figure 6. A opportunistic coupling equivalent circuit

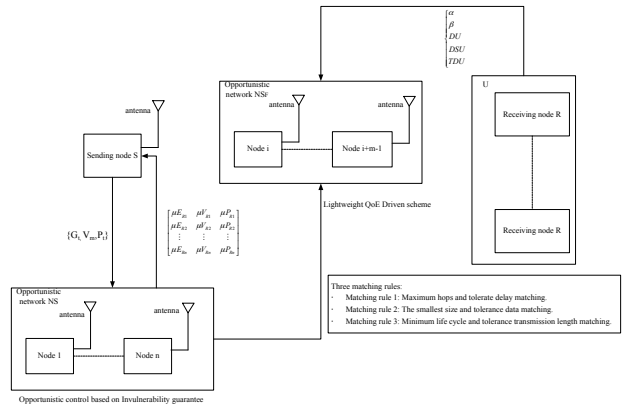


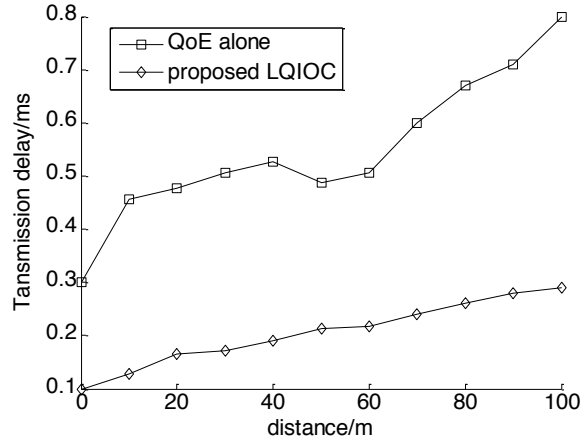
Figure 7. opportunistic control scheme with lightweight QoE driven and invulnerability guarantee

TABLE I. PARAMETER SETTINGS

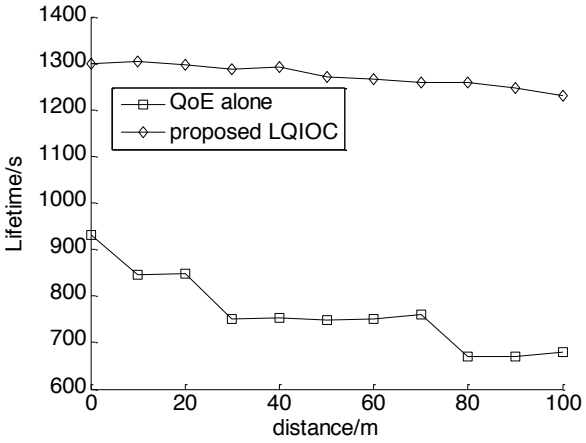
Parameters	Value
Packet size	1024 bytes
Antenna gain of S	[2, 10] dpi, step is 1
Antenna gain of nodes	8dpi
Node number	50
Voltage of nodes	12V±2
Frequency	2.4GHz
distance	[0, 100]m, step is 10m
MAC protocol	IEEE 802.15.4
Antenna type	Plate antenna
MCU	STC89C52RC
User application space	8 K bytes
On chip RAM	512 K bytes

using the invulnerability of antenna array. About long-distance communication, the proposed scheme can not only reduce the transmission delay, but also smooth the data jitter through the opportunity control. In addition, the sensitivity of the proposed scheme is significantly lower than that one of the QoE alone scheme. This is achieved through the lightweight QoE driven mechanism.

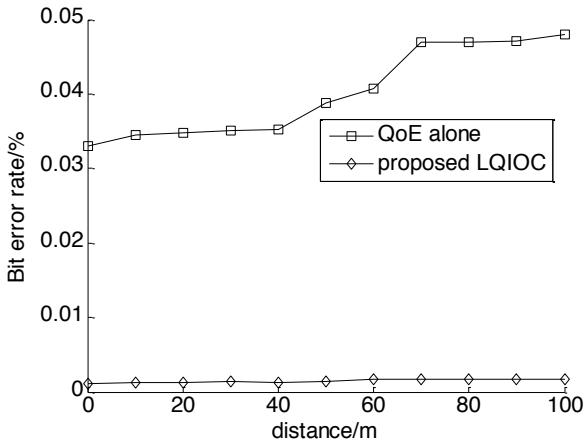
Fig. 9 shows the performance evaluation results with different SNR. In the high quality channel environment, the proposed scheme can improve the performance of QoE alone scheme, such as reducing the time delay, improving the utilization ratio of network resources and the reliability. This is due to the comprehensive consideration of and QoS and QoE support request. In particular, with the poor channel quality, the proposed scheme adjusted and balanced the relationship between user experience and the network service quality. The proposed scheme updated the network topology and node collection with opportunistic control, which can guarantee the best user experience quality with the minimal resource cost.



(a)

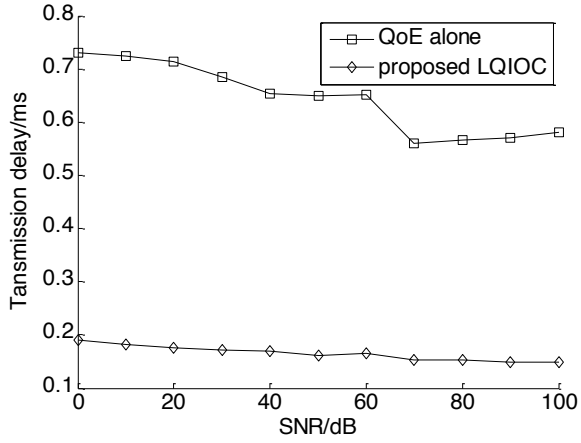


(b)

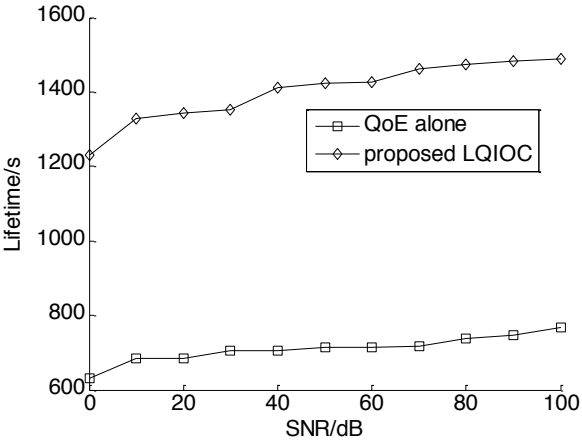


(c)

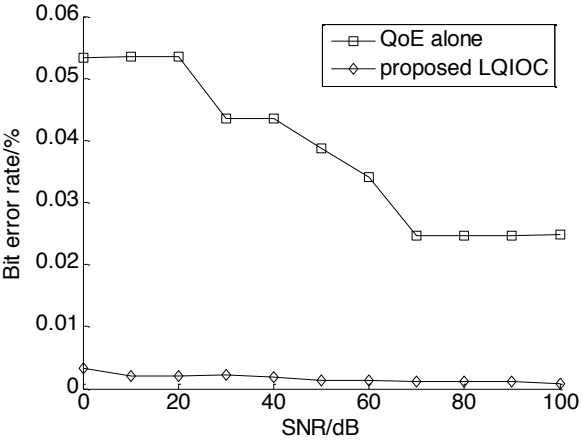
Figure 8. Performance with distance. (a) Transmission delay, (b) Lifetime, (c) Bit error rate



(a)



(b)



(c)

Figure 9. Performance with SNR. (a) Transmission delay, (b) Lifetime, (c) Bit error rate

V. CONCLUSIONS

In this paper, we designed the survivable antenna elements, which can launch opportunity survivability control requirements or accept the opportunity request. According to the wireless network quality, distance, antenna area and working frequency, we compute the effective energy, voltage and power, for selecting the optimal invulnerability nodes, which could improve the resource utilization and lifetime. Based on the channel quality of user, we designed the QoE driven scheme. Then, we calculate the tolerate delay, data scale and transmission cycle. Accordant the use requirements, network scale, invulnerability ability of nodes, we proposed the opportunistic network transmission scheme with hops, data scale and lifetime. The experiment results prove that the proposed scheme can effectively solve the contradiction between the quality of user experience intense demand and wireless source utilization, as well as life cycle.

REFERENCES

[1] Ehsan S, Hamdaoui B. A Survey on Energy-Efficient Routing Techniques with QoS Assurances for Wireless Multimedia Sensor Networks[J]. IEEE Communications Surveys & Tutorials, 2012, 14(2):265-278. http://dx.doi.org/10.1109/SURV.2011.020211.00058

[2] Aziz A A, Sekercioglu Y A, Fitzpatrick P, et al. A Survey on Distributed Topology Control Techniques for Extending the Lifetime of Battery Powered Wireless Sensor Networks[J]. IEEE Communications Surveys & Tutorials, 2013, 15(1):121-144. http://dx.doi.org/10.1109/SURV.2012.031612.00124

[3] Zhang Q, Deng H, Zhang M, et al. Notice of Retraction Invulnerability of colored networks: A survey[C]// Quality, Reliability, Risk, Maintenance, and Safety Engineering (QR2MSE), 2013 International Conference on. IEEE, 2013:71-74.

[4] Soelistijanto B, Howarth M P. Transfer Reliability and Congestion Control Strategies in Opportunistic Networks: A Survey[J]. IEEE Communications Surveys & Tutorials, 2014, 16(1):538-555. http://dx.doi.org/10.1109/SURV.2013.052213.00088

[5] He Z, Mao S, Jiang T. A survey of QoE-driven video streaming over cognitive radio networks[J]. IEEE Network, 2015, 29(6):20-25. http://dx.doi.org/10.1109/MNET.2015.7340420

[6] Gómez G, Lorca J, García R, et al. Towards a QoE-driven resource control in LTE and LTE-A networks[J]. Journal of Computer Networks & Communications, 2013, 2013(2)

[7] Zhou L, Yang Z, Wen Y, et al. Resource Allocation with Incomplete Information for QoE-Driven Multimedia Communications[J]. IEEE Transactions on Wireless Communications, 2013, 12(8):3733-3745. http://dx.doi.org/10.1109/TWC.2013.051413.120597

[8] Wu Y, Hu F, Kumar S, et al. A Learning-Based QoE-Driven Spectrum Handoff Scheme for Multimedia Transmissions over Cognitive Radio Networks[J]. IEEE Journal on Selected Areas in Communications, 2014, 32(11):2134-2148. http://dx.doi.org/10.1109/JSAC.2014.141115

[9] Lin K, Wang W, Wang X, et al. QoE-driven spectrum assignment for 5G wireless networks using SDR[J]. IEEE Wireless Communications, 2015, 22(6):48-55. http://dx.doi.org/10.1109/MWC.2015.7368824

[10] Nightingale J, Wang Q, Calero J M A, et al. QoE-driven, energy-aware video adaptation in 5G networks: The SELFNET self-optimisation use case[J]. International Journal of Distributed Sensor Networks, 2016, 2016.

[11] Zhao D J, Yang H T, Jiang J, et al. Modeling and Simulation of the Invulnerability of Space Information Network[C]// Internet Technology and Applications, 2010 International Conference on. 2010:1 - 5.

[12] Cheng Ju, Jinde Cao, Weiqi Zhang, and Mengxin Ji, "Influential Node Control Strategy for Opinion Evolution on Social Networks," Abstract and Applied Analysis, vol. 2013, Article ID 689495, 6 pages, 2013.

[13] Qin X H, Ge W. Study on Invulnerability of Enterprise Marketing Networks[C]// Proceedings of the 2013 International Conference on Computational and Information Sciences. IEEE Computer Society, 2013:355-358.

[14] Di P, Li F, Hu B. Research on invulnerability of combined operations combat network under repair[C]// Information Science, Electronics and Electrical Engineering (ISEEE), 2014 International Conference on. IEEE, 2014.

[15] You L, Yuan Y, Yu W, et al. A key distribution scheme for WSN based on hash chains and deployment knowledge[J]. International Journal of Distributed Sensor Networks, 2015, 2015(1). http://dx.doi.org/10.1155/2015/640792

[16] Javan M R, Sharafat A R. Interference-Dependent Opportunistic Power Control for Multicarrier Interference Channels[J]. IEEE Transactions on Vehicular Technology, 2011, 63(2):953 - 958. http://dx.doi.org/10.1109/TVT.2013.2278920

[17] Biagi M, Cuomo F. An Opportunistic Access Scheme Through Distributed Interference Control for MIMO Cognitive Nodes[J]. Wireless Communications IEEE Transactions on, 2013, 12(12):6500 - 6513. http://dx.doi.org/10.1109/TWC.2013.103013.130939

[18] Ao X, Yu F R, Jiang S, et al. Distributed Cooperative Topology Control for WANETs With Opportunistic Interference Cancelation[J]. IEEE Transactions on Vehicular Technology, 2013, 63(2):789-801. http://dx.doi.org/10.1109/TVT.2013.2278101

[19] De S C F, Abbas-Turki M, Abou-Kandil H, et al. Transmission Power Control for Opportunistic QoS Provision in Wireless Networks[J]. IEEE Transactions on Control Systems Technology, 2013, 21(2):315-331. http://dx.doi.org/10.1109/TCST.2011.2181080

[20] TANG, ZHAO, Jihong. Distributed Power Control for Energy Conservation in Hybrid Cellular Network with Device-to-Device Communication[J]. Communications China, 2014, 11(3):27-39. http://dx.doi.org/10.1109/CC.2014.6825256

[21] Gatsis K, Pajic M, Ribeiro A, et al. Opportunistic Control Over Shared Wireless Channels[J]. IEEE Transactions on Automatic Control, 2015, 60(12):1-1. http://dx.doi.org/10.1109/TAC.2015.2416922

AUTHORS

Yong Jin is with School of Computer Science & Engineering, Changshu Institute of Technology, Changshu 215500, China (jinyong@cslg.cn).

Jian Cai is with Changshu No.1 People's Hospital, Jiangsu, Changshu, China.

Huan Dai is with School of Computer Science & Engineering, Changshu Institute of Technology, Changshu 215500, China.

Kaijian Xia is with Changshu No.1 People's Hospital, Jiangsu, Changshu, China.

Ping Xu is with Operation Research Center, Nanjing Army Command College, Nanjng, 210045, China.

This work is supported in part by the Science and Technology Development Project of Changshu (Social Development category) Grant No. CS201503, National Natural Science Foundation of China Grant No. 61300186, Suzhou science and technology development project NO. SYSD2015014, and the practice innovation training program projects for the Jiangsu College students NO. 201510333034Y. Submitted 05 April 2016. Published as resubmitted by the authors 17 May 2016.