

Direct Communication: A CM is an intermediate node between sensor nodes and the observer. All sensor nodes are data gatherers and they transmit their results directly to a CM. It is extremely inefficient energy, since the long distance transmission in direct communication consumes more power[3].

Clustering Routing Algorithms: Clustering divides the network into some clusters. Each cluster has a head pointed to cluster, which is a central controller, and only the head of the cluster can communicate with CM. Members, other sensor nodes in the same cluster, may become the head of cluster through adjusting the pointer's position[4].

Multi-hop Routing Algorithms: Multi-hop routing is another communication scenario. All sensor nodes in the network act as routers for other sensor nodes and the transmitting packages are routed to the one or some CM. Multi-hop routing minimizes the distance that an individual sensor node must transmit, and hence minimizes the power consumption[5].

Flooding algorithm: Flooding algorithm uses a simple store-and-forward mechanism to propagate data packages hop by hop. Node's mobility and change of topology can be supported[6]. Route discovery and route information exchange are unnecessary.

III. THE STATES OF NOVEL POWER SAVING ALGORITHM FOR WSNs

In this section, we propose a simple mechanism called power saving algorithm (NPSA) in order to save power for applications that sensor nodes are movable in a proactive approach. This algorithm integrates routing and power-management function to satisfy the requirement.

Our goal is to use the least power to transfer more data packages successfully to CM in applications with movable sensor nodes. The proposed NPSA is a routing algorithm which supports mobility on sensor nodes and has three major characteristics in power saving: 1) A periodic round is employed for nodes to get active and suspend, 2) Unimportant data packages are dropped, and 3) It can be implemented in both hardware and software.

Firstly, since the traffic load in WSNs is considered to be low, a periodic round is used for all sensor nodes intending to successfully transmit one package from sensor node to CM. Sensor nodes should resume from the suspend state at almost the same time when a round starts. When a sensor node is in active state in a round, it can prepare a data package transmission for itself or forward one data package from other sensor nodes. Once finishing the transmission or forwarding a data package, the sensor node turns to suspend state immediately and the data package is deleted from its buffer, otherwise, sensor node keeps in its active state until time is over. Consequently, this avoids overhearing the same data package in this round and more power is preserved. The time slice, is called suspend timeout, is the maximum period of the active state when sensor nodes are forced to suspend state. It is unnecessary to check up on duplicated data package using other mechanisms and to transfer data package from a sensor node just lives in this round.

Secondly, sensor node's transmission efficiency will go down when a sensor node receives more duplicate data packages[7-8]. Consequently, Sensor node will decide to

drop the duplicated data package. Because only one data package is allowed to be sent in a round, the sensor node should not initiate a data package transmission and could drop the received data package when the medium is sensed busy by one bit of the correct reception from the radio.

Last but not least, the received data packages are not passed to the processor and the NPSA would be so simple that it can be implemented in both hardware and software. That is, the following energy-aware package forwarding architecture should be used. The first layer is the radio part which contains RF front-end and network controller implemented in hardware. Two types of packages are processed by the radio part: the package originated from the processor and the forwarded package received from the RF front-end. The radio part is responsible for the transmission of original and forwarded packages, dropping of forwarded packages, and control of the RF front-end by turning on or off. The other layer is the sensor node part, which includes a processor and some sensors. The sensor node part gathers sensed data continuously and generates data packages periodically. Once data packages was generated, it would be transferred to the radio part for transmission. Based on the architecture, both data package transmission and reception are processed in the radio part. The processing capacity of the processor and the power for MAC processing and network routing are thus conserved[9].

As mentioned before, the design concepts of the NPSA are three folds: a periodic round for sensor nodes to get active and suspend, dropping unimportant data packages, and hardware implementation. It uses broadcast to transmit data package to neighbor sensor nodes without having the information of other sensor nodes. The power cost in duplication, processing, collision, overhearing, controls package overhead, and idle listening is avoided or reduced by data package dropping, hardware control, duplicate reduction, suspending after transmitting, no control package, and timeout to suspending. Power is saved but data package loss incurred, however, data package loss during a long-term periodical report is acceptable in WSNs.

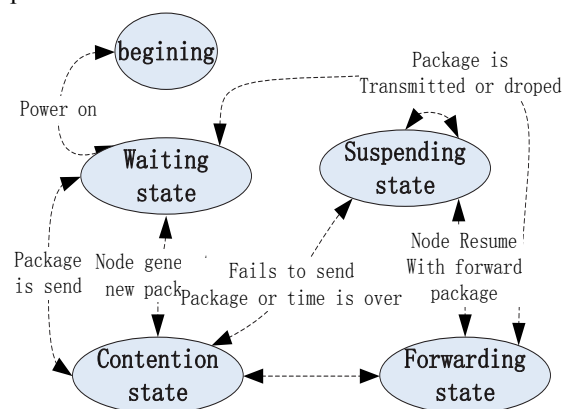


Figure 2. The state transition diagram

During a round, a node can be in four possible states: *waiting state*, *contention state*, *forwarding state*, and *suspending state*. Fig. 2 describes the state transition diagram. When all sensor node power on, they are all in the waiting state. As soon as a sensor node in waiting state finished its sensed data, a data package would be

originated. This may cause sensor node's state transfer. A round starts from either the contention state or the If there is a data package originated, the sensor node in waiting state transits to contention state.

Waiting state- When the entire sensor node is power on, firstly they are all in this state. Once a data package is originated by sensor node in this state, the sensor node enters into contention state, otherwise sensor node continue to stay in this state.

Contention state – When a round starts, a sensor node comes from waiting state, which means there are data package originated by sensor node. Sensor node enters into this state. Note that whatever states a sensor node is in, “active” and “suspend” indicate the operating mode of the RF front-end, and the processor is indifference to the wireless network. Before the beginning of this round, the originated data package should be given from the processor to the network controller. Sensor nodes in this state content with other sensor nodes for the medium. Sensor node uses a number of contention tags to run for medium access.

Then the priority can be given to the data package with a small number of contention tags for winning the channel in the space away from source sensor node. The sensor node can check the state of medium. When the sensor node received a binary bit from the RF front-end, that means the medium was occupied by other sensor node, this sensor node can only enter into suspending state. The residual contention tags and the original package are kept for the next contention. Alternatively, contention tag is decreased when the medium is idle. When the contention time counts down to zero, the original data package is transmitted and then the node goes to waiting state directly.

Forwarding state – When a sensor node resumes from suspending state and there is no data package generated, sensor node will transmit to forwarding state. A sensor node in forwarding state stays active, but transmits the forwarded data packages instead of its original data packages.

After a sensor node receives a forwarded data package, it schedules a time for this data package. The time in forwarding state is similar to that in contention state,

At the end of forwarding time, the data package is forwarded. During the forwarding time, if a sensor node receives one binary bit from other sensor node, which implies that its neighbor has rebroadcast this data package, the sensor node will stop the forwarding procedure and drop this data package, and then enters into waiting state. Alternatively, at the end of the forwarding time, this data package is forwarded.

In addition, if a sensor node keeps in active state over suspending time slice, it enters into suspending state despite that there is a data package to transmit or not.

Suspending state – A sensor node goes to this state when a data package transmission is not completed because it fails in contending for the medium or it's time slice is over. When a sensor node enters this state, the RF frond-end is turned off. Sensor node leaves the suspending state at the beginning of the next round. The suspending state is used for power saving, and the duration of this state adapts to the data rate of the WSNs. When the data rate is low, one can prolong the duration of this state. On

the other hand, the duration of this state can be shortened down to zero.

IV. FUNCTION OF POVER SAVING ALGORITHM FOR WSNs

The NPSA is described by flowchart in Fig. 3. The round time and the suspending time slice can adapt to the data rate and the extent of the sensor field. By fixing the suspending time slice, the round time can be prolonged for the low data rate and more power is saved in suspending state. With a fixed round time, large suspending time slice will allow more data packages propagate farther to CM while sensor nodes consumed more power on idle listening.

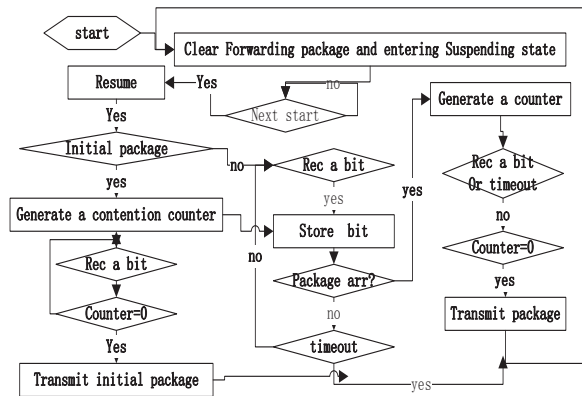


Figure 3. The state transition diagram

To assure that all sensor nodes in WSN can resume almost at the same time, some synchronous mechanisms are required. However, the study of the synchronization is out of the scope of this paper and we assume that the system is synchronous in our simulation with the cost of timestamp in the header.

In order to allow more sensor nodes in a WSN, an additional state called initial state is introduced for the newly joined nodes. This state is a sub-state of forwarding state, and the time to next round and suspending time slice is set to the maximum. So sensor nodes in this state turn the radio on and wait to receive the first package to synchronize its local timer. Having received the first package, the time that the next round will start is known. The sensor node is synchronized, and then transmission of packages is allowed.

Comparing with simple other algorithm, the NPSA does not need extra power to record a unique sensor node identifier and a sequence number used to detect the duplication in each received data package. Sensor node running the NPSA operates with its current state and sensed events. It is possible that NPSA could be implemented in both hardware and software. In addition, the NPSA would drop some unimportant packages and does not accept completely. Thus the bandwidth in the medium and power consumption in this sensor node is saved. On the other hand, the NPSA also includes power-management function. The power consumption is further reduced. However, some duplicated data package was dropped by the NPSA, communication module may not receive these dropped data package. In addition, the NPSA uses the periodic round in the result that quasi-synchronization is required and packages are queued in

buffer. In fact, package loss might occur in any algorithms. Losing some data packages is permitted in WSNs in the long-term. We use the factor, the average power cost per reached data package, to evaluate the performance of our algorithm. Moreover, the package delay is the cost of the NPSA and is also estimated in the future study.

V. CONCLUSIONS

The proposed NPSA not only supports the moving nodes, but is also power-efficient and suitable for WSNs which has high node density. It may works on the basis of node state and can be implemented in both hardware and software easily, so more resources of the processor can be saved. Moreover, not only at light load but also at heavy load, the NPSA is applicable to various system loads by adjusting the round time at the planning stage. Though the NPSA may consume lower power than other algorithms, it has some costs as the average latency and loss of packages. But those are tolerant or can be improved by increasing the number of CM. Although the NPSA can work well in WSNs, it is just a proactive approach. More related topics need to be further studied in the future.

ACKNOWLEDGMENT

This paper is supported by National Natural Science Foundation of China (No.61263023 No. 61064010, No. 61063006).

REFERENCES

- [1] I. F. Akyildiz, Su Weilian, Y. Sankarasubramaniam, E. Cayirci, "A Survey on Sensor Networks," *IEEE Commu. Mag.*, vol. 40, no. 8, 2002, pp. 102-114. <http://dx.doi.org/10.1109/MCOM.2002.1024422>
- [2] H.R. Wang, Y. li, "A Novel Dynamic Key Management Algorithm for Wireless Sensor Networks" *Advan. Sci. lett.*, May 2012, pp.263-270.
- [3] A. Wang and A. Chandrakasan, "Energy-Efficient DSPs for Wireless Sensor Networks," *IEEE Signal Processing Mag.*, vol. 19, no. 4, 2002, pp. 68-78. <http://dx.doi.org/10.1109/MSP.2002.1012351>
- [4] Y. -C. Tseng, S. -Y. Ni, Y. -S. Chen, and J. -P. Sheu, "The Broadcast Storm Problem in a Mobile Ad Hoc Network," *Wireless Networks*, Vol.8, no. 2/3, 2002, pp. 153-167. <http://dx.doi.org/10.1023/A:1013763825347>
- [5] Baker, N. ZigBee and Bluetooth strengths and weaknesses for industrial applications. *Comput. & Control Eng. J.*, vol. 16, pp. 20-25, 2005. <http://dx.doi.org/10.1049/cee:20050204>
- [6] R. Pietro, L. Mancini, and A. Mei, "Random key-Assignment for Secure Wireless Sensor Networks", *ACM workshop on Security of ad hoc and sensor networks*, pp. 62-71, October 2003.
- [7] D. Liu and P. Ning, "Establishing Pairwise Keys in Distributed Sensor Networks," *ACM conf. on Comput.& commun. security*, Vol. 8, pp. 41-77, February 2005.
- [8] Y. Cheng and D. P. Agrawal, "An improved key distribution mechanism for large-scale hierarchical wireless sensor networks," *ACM Security Issues in Sensor and Ad Hoc Networks*, Vol.5, pp.35-48, January 2007. <http://dx.doi.org/10.1016/j.adhoc.2006.05.011>
- [9] H. Soroush, M. Salejegheh, T. Dimitriou, "Providing Transparent Security Services to Sensor Networks", *IEEE Int. Conf. Commun.*, 2007, pp.3431-3436.

AUTHORS

H. R. Wang. is with the Faculty of information engineer and Automation of Kunming University of Science and Technology, Kunming, Yunnan Province, China (e-mail:hrwang88@163.com).

Y. Li, is with the Faculty of information engineer and Automation of Kunming University of Science and Technology, Kunming, Yunnan Province, China (e-mail:sherly2001@sina.com)..

J. Y. Wang is with the Electrical Engineering Department, Zhaotong University Yunnan Province, China (e-mail:hrwang88@163.com) ,

Submitted 18 May 2013. Published as re-submitted by the authors 15 September 2013.