ISSN 2047-3338

Wireless Sensor Network Design for Security Systems

Ali Dadashzadeh, Rashid Ghorbani Afkhami and Amir Habibi Daronkola

***Abstract*— One of the interesting applications of wireless sensor networks is the security systems. A network of sensors with a well-designed communication system can detect unauthorized intrusions to a defined area. In this paper we propose a network configuration based on the specifications of the nRF24L01+ transceiver module. The module has advanced power management technology providing long battery-dependent life while having a high transmission range compared to other modules like Bluetooth. Sensed information are relayed towards a base station with the help of router nodes. The empirical results align with our calculations in the sense of routing time and data transmission time.**

***Index Terms*— Wireless, Sensor Network, Area Monitoring And Security System**

I. Introduction

THE technology of sensor networks is one of the popular and thriving matters of the twenty first century. As the production of sensors in low dimensions with low price got easier, the idea of using randomly dispersed sensors in large amount emerged [1]. A wireless sensor network (WSN) is made up of number of sensing nodes which are densely located inside or near a phenomenon [2]. The position of sensing nodes is usually not prearranged and this feature eases the use of WSN in dangerous and inaccessible situations. However, these nodes might easily crash and usually are limited in memory and power. Thus constructing and designing a network needs extra attention. Each node has a radio transceiver, a microcontroller, a sensor and a battery. In an appropriate network configuration the environment, the nodes lifetime and the importance of the data should all be considered. Even though the wireless sensor network has been successfully used in smart homes for power consumption control, we have considered the security matters which can be used even in intelligent houses [3]. In this paper we focus on an area monitoring application which probably is the most common filed for WSN. In area monitoring the network is deployed over a region to detect any intrusions. Our network design is based on the specifications of the nRF24L01+ transceiver and our routing protocols are suitable for the security requirements. The nRF24L01+ has advanced sleep modes, making is suitable for ultra-low power applications; it also has low cost and small size and its air data rate is up to 2Mbps. These advantages make the nRF24L01+ one of the most popular modules. Although the proposed design can be implemented with other modules like Bluetooth, we choose the nRF24L01+ based on the advantages it offers. The proposed network doesn't need periodic sleeping and awaking times because the software advances of nRF24L01+ let the nodes go to standby mode and extend the battery life. In many applications it is possible to use scheduled sleeping strategy and reduce the power consumption noticeably [4], but this technique is not applicable for the security systems. The proposed method also utilizes clear channel assessment which provides safe data transmission and lowers the power consumption as nodes go to the standby mode after each transmission. While it is common to use commercially available development boards for WSN systems [5], [6], [7], we designed these boards tailored for the application with lower cost.

An example of WSN for security is introduced by [5] which adopts Bluetooth technology. The sensed data by the sensor nodes are directly shared with the controlled node or conveyed through the router nodes; router nodes also have embedded sensors. The control node is in contact with a local security control system via UART. The tree topology has been used for network configuration and routing, since it is considered as the natural choice for the Bluetooth network.

Paper is organized as follows: in section II we will talk in details the proposed system design. In section III we present the experimental results and section IV has the conclusion.

II. Proposed System Design

In this section we explain in details the steps taken in design and configuration of the network. We will review the communication protocols, network initiation procedure and message relaying.

A. Dadashzadeh (Email: dadashzadeh_68@yahoo.com) and R. Ghorbani Afkhami (corresponding author, Email: ghorbani.rashid@gmail.com) are with the Electrical & Computer Engineering Department, University of Tabriz, Tabriz, Iran

A. Habibi Daronkola is with the Electrical Engineering Department, University of Imam Hossein, Tehran, Iran, (Email: amirhabibi@chmail.ir)

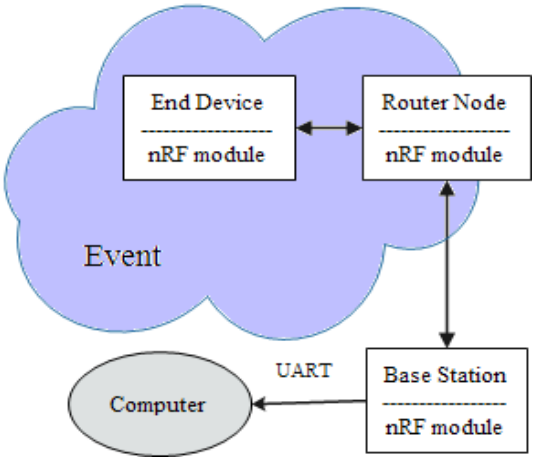

Fig. 1. Node connections in the network

A. *Overall View of the Network*

We have considered three kinds of nodes based on the application; sensor nodes or the end devices, router nodes and a base station. In our network only the sensor nodes have implemented sensors, however, other nodes can also have sensors. Sensors sense a specific feature of the environment e.g. in our project we have used motion detection sensors. A sensor node might be in direct contact with the base station, otherwise it has to use the router nodes to relay its data. Router nodes relay the information towards the base station. Base station is in contact with a central computer which monitors the received information so the appropriate processing can be done.

As illustrated in Fig. 1 the base station is connected to the central computer via UART and when a motion is detected the according end device sends the information to be finally received by the base station. All the nodes are familiar with these type of information and relay them towards the base station. The network actually forms an electronic border and detects any invasion to a specific area. After detecting the point of invasion the system informs the center with a message. As mentioned before, all the nodes use nRF24L01+ transceivers and are equipped with 4.5 volt batteries promising a long lifetime (about a year).

B. *Network Configuration*

In general the sensor nodes don't have direct access to the base station so they use the routers to connect to the base station. This is called routing and while the procedure is described in Fig. 2 we will explain it step by step here.

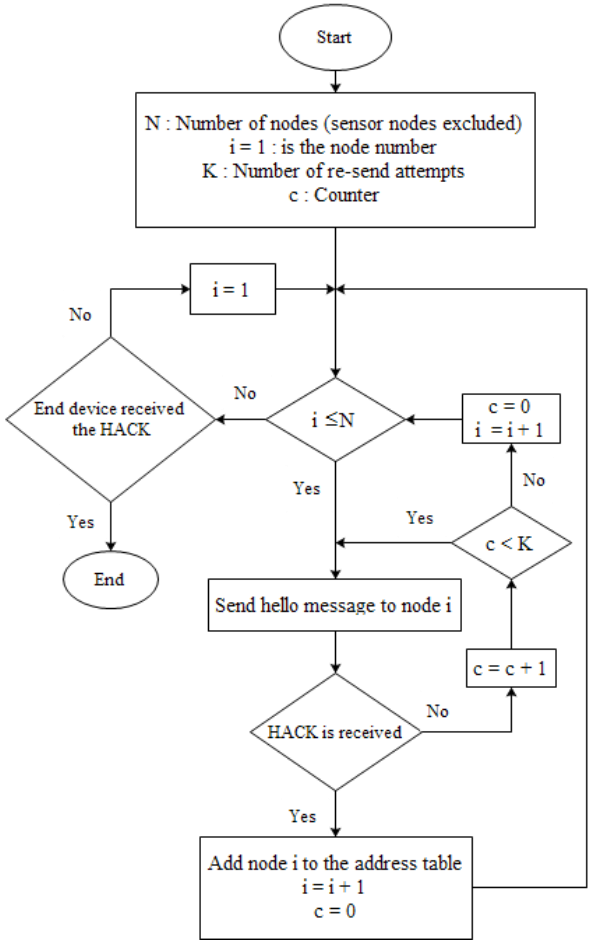

Fig. 2. Routing (procedures for sensor nodes)

The nRF24L01+ has three to five bytes of address which should be programmed beforehand. When the sensor nodes are placed randomly, the network will be initiated with a "hello message" (HM). The packet format for the nRF24L01+ is illustrated in Fig. 3 and we will use the 0-32 bytes of payload as mentioned in the figure.

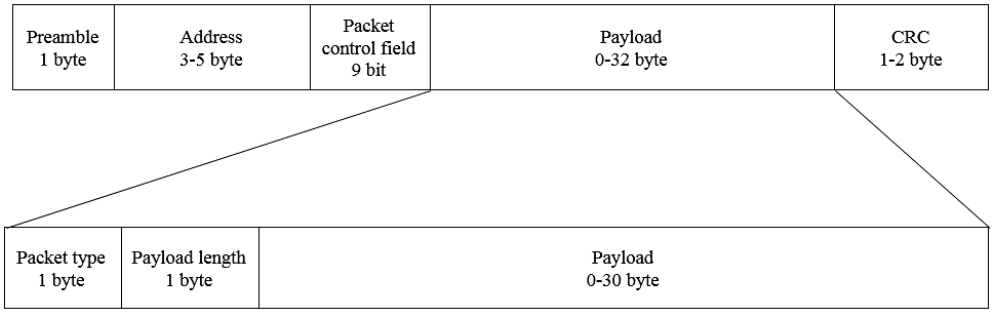

Fig. 1. Packet format for nRF24L01+ module

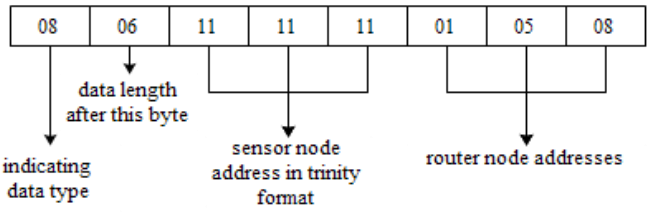

Fig. 4. Example of payload

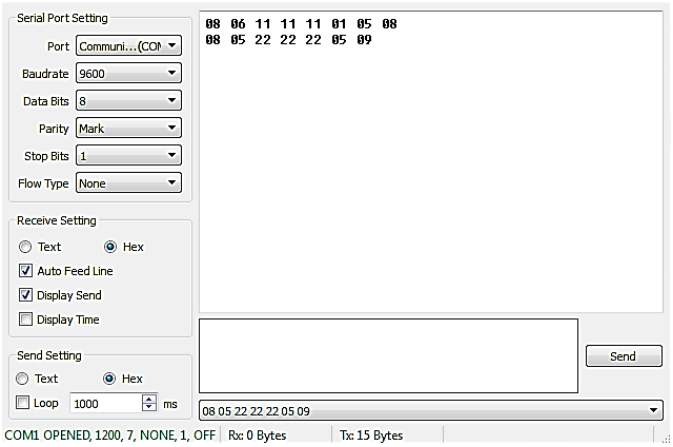

Fig. 5. "Serial Port Utility" software interface

When an end device wakes up it sends a HM to the first router node in its initial address list (The first address might even be the base station). It should be mentioned that each node has an initial address list of all other nodes before the network is configured. After sending the message the end device waits for a response, if it receive a "hello acknowledge" (HACK) it will save the corresponding address in its address table. However, if the end device doesn't receive any HACKs it will continue sending HMs for k times. It is possible that the end device doesn't receive any HACKs even after k times so it understands that there is no node with that address in the one hop distance. Then the end device goes to the next node in its initial list and does the process again.

All the nodes that respond to the HM with a HACK are considered as the one hop neighbors to that node. By the end of this process the sensor node will have an address table with the one-hop neighbors listed there. Each end device shares its address table with its one-hop neighbors. If the base station is in the one-hop distance of the end device it will also receive the address table and responds with an ACK. The routing is a bit different for the router nodes and will be explained next.

When a router node wakes up it listens to the channel until a HM is received, which will be answered with a HACK. This means that the router's address is being added to an address table. When the router node receives an address table it will check it against its initial list of addresses and send the HM to the nodes that aren't in the table (i.e. the N in Fig. 2 is the number of nodes in the network minus the number of sensor nodes and the nodes in the address table). This is the only difference between routing of sensor nodes and router nodes. The fact that the router nodes send the HMs only to the nodes that haven't received it by the previous node, brings a kind of optimization to the network and guarantees that the base station will receive the message in the shortest time. While it prevents messages from going backwards, it reduces the energy loss. After routing if the router receives another address table from other sensor node it won't do the routing process again since it has already found a route to the base station.

After the router sends the HMs to the nodes that aren't in the address table it waits for HACK and adds the new one-hop neighbors to the its address table. The new address table is then sent to the one-hop neighbors. The node that receives this address table repeats routing until the message reaches to the base station. When the base station gets the message it sends HACK in response so the node that has sent the message understands that the base station is in its one-hop distance. Of course the base station might be receiving the message through different routes.

It should be mentioned that all the nodes check the

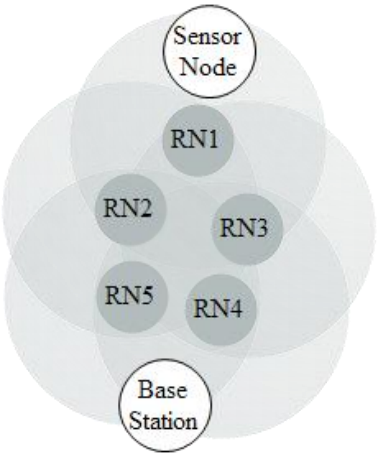

Fig. 6. Network structure (two-neighbor design)

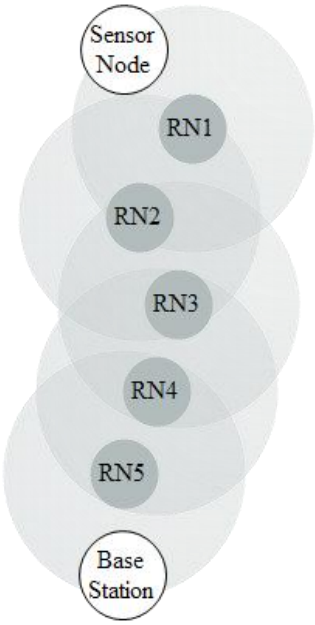

Fig. 7. Network structure (one-neighbor design)

presence of the base station by sending hello messages when the network is first constructed. In this network there is a specific answer for each packet so the transmitter will be notified of a successful transmission. The data and the routing (address table forwarding) messages are responded with an ACK and hello messages are responded with a HACK.

Before the network is initiated the address tables of the routers are empty. Thus if a router node receives any packets other than the hello message during this time, it won't give any answers. The routing procedure is done periodically depending on the network. In this process the address table is refreshed and all the nodes that are turned off or doesn't work anymore will be cleared off the table. The new nodes, on the other hand, will be added to the address tables.

C. Sending Data

Whenever a sensor node senses an event it sends the according data to one of the routers in its address table provided that the base station is not in its one-hop distance. When the sensor receives an ACK for its message it will stop sending the data and will wait for a new sense. However, if the sensor node doesn't receive an ACK it will continue sending data for k times. Each time it picks a new node from its address table and sends the data but if no ACK is received the packet will be labeled as failed. When the data is being forwarded, if a router doesn't find any nodes in its one-hop distance it will not send an ACK. This way the data will be sent through another router node which has other nodes in its one-hop neighbor. The routers forward the data like the sensor nodes; the only difference is that the router nodes choose the next node from their one-hop neighbors not from the address table.

We have also used clear channel assessment (CCA) in this network. Thus, before sending data each node measures the energy of the channel; if it is higher than a certain value, the node notices another data transmission and waits until the channel is clear. CCA reduces the probability of data collusion in the network.

D. Receiving Data

When an end device senses an intrusion it will write its own address in the payload and passes the message to the routers. When a router node receives the data it adds its own address and increases the data length by one. When data reaches the central station, it will be easy to track the sense using "serial port utility", "hyper terminal" or other similar software. Fig. 5 shows the "serial port utility" interface used in the experiments.

As shown in Fig. 3 the address in the nRF24L01+ packet must be at least 3 bytes. Thus the sensor node which is always the first node, uses a trinity format to write down its address (i.e., the sensor node repeats its address to fill the three bytes, shown in Fig. 4). But as we have a 32-byte limit for the payload, the router nodes write their addresses in one byte each. So the 01 in the Fig. 4 belongs to the router node with address 010101. Using data length in the payload as in Fig. 4 lets us detect errors when there is inconsistency with the payload length.

Fig. 5 shows an example of received messages by the central computer. The first line for example indicates that the SN_{11} (e.g., sensor node with address 111111) has sensed an event and passed the data through RN_{01} (e.g., router node with address 010101), RN_{05} and RN_{08}.

III. Experimental Results

In this section we will present the experimental results and compare them with the expected theoretical ones. The experiments measure the routing times and data transmission times in the network, designed in two different schemes. In the first design each node has only one other node in its one-hop distance. In the second experiment, however, there are two one-hop neighbors for each node.

First of all some constant values should be introduced. The changeover time which is the time needed for the module to change from receiver mode to transmitter mode or vice versa is set to 200ms. The time to choose a target node and send data to it, is about 200ms as well.

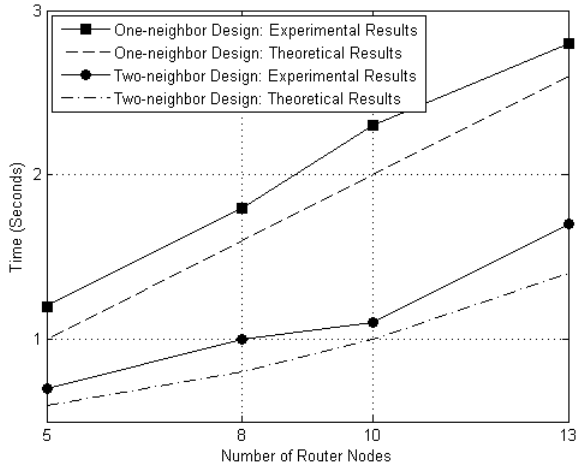

Fig. 8. Data transmission time for different network designs

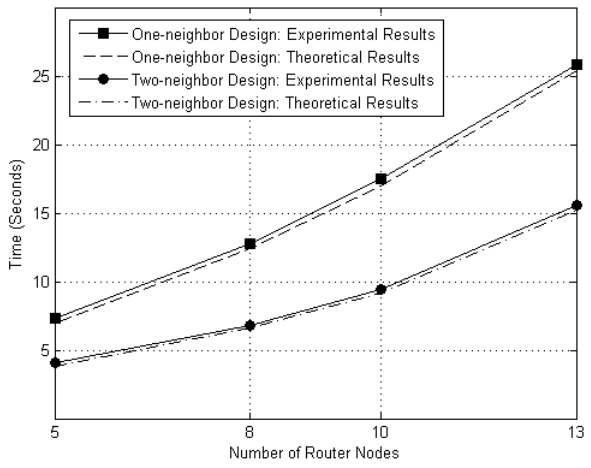

Fig. 9. Routing times for different network designs

The two network schemes are shown in Fig. 7 and Fig. 6, namely one-neighbor design and two-neighbor design. Figures show the wireless communication range for the nodes. In one-neighbor design each node will find only one neighbor to share its data. In the two-neighbor scheme each router node can send the data to two other routes, considering that they are not programmed to send data backwards. While the both network schemes show five router nodes, the results are prepared for 5, 8, 10 and 13 router nodes over the same schemes. Also note that in the two-neighbor scheme if any of the nodes in a path are disabled, the end device or router will automatically choose the other path to send its data. Fig. 9 and Fig. 8 show the routing times and data transmission times for the networks respectively. It is obvious that the two-neighbor design is faster in both routing and data transmission times. Although the practical results confirm what we were expecting, the big part of the gap between theoretical and experimental results come from the measurement errors.

IV. CONCLUTION

WSN has many applications ranging from biodiversity mapping to battlefield surveillance. This paper presents a novel network configuration for a WSN designed for security. In the network, when a sensor senses an event it sends the data to the nodes in its address table. The routers do the same, and they don't send the message to the nodes which already have the data so the message always moves towards the base station. Each node is aware of its neighbors since it creates an address table when the network is initiated and corrects it progressively. The network is practically implemented and the routing times and the data transmission times are measured and compared with the expected ones.

The nRF24L01+ has some advantages over Bluetooth modules; while the number of active members in a classical Bluetooth transmission is up to 7, the nRF24L01+ can support more active transmissions. The maximum current for nRF24L01+ is only 13 mA with transmission range of 100 meters while a Bluetooth module draws up to 30 mA with transmission range of 50 meters. On the other hand, the nRF24L01+ doesn't support broadcasting which makes the routing process more difficult. Although each module has its own advantages, the nRF24L01+ seems more suitable for our application and this is the reason for reporting the implementation based on this module.

REFERENCES

[1] V. C. Gungor and G. P. Hancke, "Industrial wireless sensor networks: Challenges, design principles, and technical approaches," IEEE Transactions on Industrial Electronics, vol. 56, no. 10, pp. 4258-4265, 2009.

[2] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam and E. Cayirci, "A survey on sensor networks," IEEE Communications Magazine, vol. 40, no. 8, pp. 102-114, 2002.

[3] M. Li and H.-J. Lin, "Design and Implementation of Smart Home Control Systems Based on Wireless Sensor Networks and Power Line Communications," IEEE Transactions on Industrial Electronics, vol. 62, no. 7, pp. 4430-4442, 2015.

[4] W. Ye, J. Heidemann and D. Estrin, "Medium access control with coordinated active sleeping for wireless sensor networks," IEEE/ACM Transactions on Networking, vol. 12, no. 3, pp. 493-506, 2004.

[5] S.-H. Choi, B.-K. Kim, J. Park, C.-H. Kang and D.-S. Eom, "An implementation of wireless sensor network," IEEE Transactions on Consumer Electronics, vol. 50, no. 1, pp. 236-244, 2004.

[6] M. Carlos-Mancilla, J. G. Olascuaga-Cabrera, E. López-Mellado and A. Mendez-Vazquez, "Design and Implementation of a Robust Wireless Sensor Network," in International Conference on Electronics, Communications and Computing, Cholula, 2013.

[7] J. John, V. S. Palaparthy, S. Sarik, M. S. Baghini and G. S. Kasbekar, "Design and implementation of a soil moisture wireless sensor network," in Twenty First National Conference on Communications, Mumbai, 2015.