Journal of Computer Applications (JCA)
ISSN: 0974-1925, Volume IV, Issue 3, 2011

Energy Aware Routing Protocol For Zigbee Networks

P. Anitha ^{a,*}, Dr. C. Chandrasekar ^{b,1},

Abstract - Wireless ADHOC networks are self organized dynamic networks can share wireless channel without any established central control standard for IEEE 802.11. The most common protocols are AODV, DSDV, DSR, IRAODV in ADHOC used to ensure the data transmission among them selves. To meet the need of low power and low cost IEEE 802.15.4 standard was developed for sensor networks. In this paper we focus how Improved Energy Efficient Ad hoc on Demand Distance vector routing (IEEAODV) routing protocol performs in sensor networks. At this point, in this protocol we are going to present an algorithm to select maximum suitable path between source and destination on the basis of energy of nodes, stability of nodes and hop-count of paths.

Index Terms - *Zigbee /IEEE 802.15.4, IEEE 802.11, low data rate, low power, energy, IEEAODV.*

I. INTRODUCTION

Wireless networks provide advantages in size, deployment, cost, and distributed intelligence compared with wired networks. Wireless technology not only enables users to set up a network quickly, but also enables them to set up a network where it is inconvenient or impossible to wire cables. The “care free” feature and convenience of deployment make a wireless network more cost-efficient than a wired network in general.

Conventional ADHOC routings can be divided into two categories. On-demand or reactive and Table driven or proactive protocols. The route path established only when a node has data packets to send by means of the best known protocol of On-Demand – reactive protocols are AODV, DSR. In contrast the proactive routing protocols constantly update in spite of the traffic activity in the network. Each node generates control packets periodically by the way of topology changes. The well known protocol is DSDV.

Energy is a concern in wireless sensor network that require working for an extensive period on battery power. As soon as a node exhausts its energy it cannot sense or relay data to any further extent. The main objective of this paper is to analyze the performance of these Sensor nodes working under ADHOC routing protocols. In section 2, we give a brief description of 802.15.4. In section 3, Routing Protocols for Wireless Network, Next, in section 4, Modified Reverse Ad Hoc on Demand Distance Vector (MRAODV) routing algorithm. In section 5, Proposed Improved Energy Efficient AODV routing protocol. Then, in section 6, we define a set of performance metrics.

Manuscript received, 2011.

P.Anitha ^{a,*},
Associate Professor(sr) ,
Department of Master of Computer Applications,
K.S.R. College of Engineering, Tiruchengode
E-mail: psp03ster@gmail.com
Dr.C..Chandrasekar ^{b,1},
Prof & Reader,
Department of Computer Science Periyar University, Salem

II. AN OVERVIEW OF IEEE 802.15.4

The IEEE 802.15.4 is a new standard, which defines the physical layer (PHY) and medium access control sub layer (MAC) specifications for low data rate wireless connectivity among relatively simple devices that consume minimal power and typically operate in the Personal Operating Space (POS) of 10 meters or less. An 802.15.4 network can simply be a one-hop star, or, when lines of communication exceed 10 meters, a self-configuring, multi-hop network. A device in an 802.15.4 network can use either a 64-bit IEEE address or a 16-bit short address assigned during the association procedure, and a single 802.15.4 network can accommodate up to 64k (216) devices. Wireless links under 802.15.4 can operate in three license free industrial scientific medical (ISM) frequency bands. These accommodate over air data rates of 250 kb/sec (or expressed in symbols, 62.5 ksym/sec) in the 2.4 GHz band, 40 kb/sec (40 ksym/sec) in the 915 MHz band, and 20 kb/sec (20 ksym/sec) in the 868 MHz Total 27 channels are allocated in 802.15.4, with 16 channels in the 2.4 GHz band, 10 channels in the 915 MHz band, and 1 channel in the 868 MHz band. Wireless communications are inherently susceptible to interception and interference. Some security research has been done for WLANs and wireless sensor networks [3]–[6], [7], [8], but pursuing security in wireless networks remains a challenging task. 802.15.4 Employs a fully handshaked protocol for data transfer reliability and embeds the Advanced Encryption Standard (AES) [10] for secure data transfer. In the following subsections, we give a brief overview of the PHY layer, MAC sublayer and some general functions of 802.15.4.

III. ROUTING PROTOCOLS FOR WIRELESS NETWORK

There are two types routing protocol for wireless network. First, proactive type is operating routing path before sending data. If it changes topology of nodes, this information sends neighbor nodes. And neighbor nodes updated it. The wellknown proactive routing protocol is DSDV. Second, reactive type is setting routing table on demand, and it maintains active routes only. The well-known reactive routing protocols are DSR and AODV. Wireless Network makes frequent movement. So it needs supporting movement of reactive routing protocol. In this section, we study well-known reactive routing protocol.

3.1 DSR (Dynamic Source Routing)

DSR is being standardized in the IETF MANET (Mobile Ad-hoc Network) working group [16]. DSR is a well-known, reactive routing protocol. It computes a route only if one is needed. The route discovery consists of route request and route reply. The route request is broadcast into the wireless network. However, instead of setting the reverse paths in the routing tables of the nodes, the route request collects the addresses of the traversed nodes on its way to the destination. Route reply sends this path back to the source where all paths are stored in a route cache. The path, that is, the list of addresses from the source to the destination, is included in the header of each packet by the source node. Each node forwards a received packet to the next hop based on the list of addresses in the header (source routing). DSR uses PERR (Packet Error) messages for the notification of route breaks [17].

The Ad-hoc On-Demand Distance Vector outing Protocol (AODV), is one of more common routing algorithm in ad hoc networks and is based on the principle of discover routes as needed. One disadvantage of AODV and most on-demand routing protocols is a route reply message loss. In reverse AODV algorithm this problem concerned and one efficient approach proposed. AODV and most of on-demand routing is based on single route reply message. The lost of route reply message may cause a significant degradation of performance. In rout discovery phase, a *route reply message* (RREP) of AODV obtains by the spending cost of flooding the entire network or a partial area. RREP loss leads to source node reinitiate route discovery process which causes degrade of the routing performance, like high power consumption, long end-toend delay and inevitably low packet delivery ratio. In RAODV algorithm, loss of RREP messages considered. In reverse AODV (RAODV), destination node uses reverse RREQ to fmd source node. It reduces path fail correction messages and can improve the robustness of performance. Therefore, success rate of route discovery may be increased even though high node mobility situation [18].

IV. IMPROVED REVERSE AD HOC ON DEMAND DISTANCE VECTOR (IRAODV) ROUTING ALGORITHM

RAODV routing algorithm increases performance and when route fails occurs, the source node should select the best route between available routs. In this paper, we apply stability estimation method for route selection and to increase performance. Breaking radio links among nodes may easily happen due to the changing network topologies.

Therefore, a good design of the ad hoc routing protocol is needed to overcome these problems. Several ad-hoc routing protocols for MANETs have been proposed in recent years. RAODV algorithm solves this problem with selecting the route with minimum length in available set of routes that have been already found. Here we change this stage with our approach. One kind of link stability is used in AOSV [6]. In AOSV algorithm for computing link/rout stability, initially every node begins to estimate the stabilities of radio links to its neighbors and for keeping track of the link stabilities between a node and its neighbors, each node periodically broadcasts *Hello message*(HELLO) including the location of the broadcasting node toward its neighbors. In this protocol, when a node receives *Hello messages,* this node first calculates the distance between neighboring node and itself from the received HELLOs and for sake of awareness of distance, evaluates the stability of radio link to the broadcasting neighbor. This information is recorded for estimating stabilities of multi-hop routes in follow-up processes. In path discovery process, source node broadcasts RREQ which has new link stability field. Intermediate node sends receive RREQs and rebroadcast them. The intermediate nodes rebroadcast only the RREQ with the maximum value in route stability among received RREQs. In our proposed routingalgorithm (IRAODV), when a source node wants to communicate with a destination node, first it broadcasts a RREQ packet. This stage is the like of AODV algorithm. When destination receives a RREQ message, it broadcasts R-RREQ message to find source node. Each intermediate node which receives the R-RREQ message, calculates route stability by equation (2) and the route stability for each router is calculated by the following equation.

$$RSr = \Pi \ \mathbf{nsi}$$

Where *RSr* is the route stability of the route r, *Lr* is the set of available routes and *nsi* is the stability of node *i* .

The stability of each route can be calculated by following

$$\mathbf{nsi=(t-t')/(ln-ln')}$$

Where *Ln* denotes the location of node ni at the time t. For *t* computation of stability for each node we need to obtain *t* - t′ delay. When source node receives R-RREQ, it will have multiple routes to destination, so it selects stable route to destination node. According to this when one intermediate node moves and causes link breaks then active route fails and a new route must be selected. In AODV, this process is done by initializing route discovery procedure and in RAODV with selecting one available route with minimum hop count. In IRAODV, a new route with maximum stability is selected between available routes. We add link stability field to R-RREQ packet. When destination node receives first RREQ, it broadcasts R-RREQ. Every intermediate node which receives R-RREQ packet, it computes link stability and records it. When source node receives R-RREQ packets, it has information about stability of available routs to destination node. So it can select a route with highest stability. When data transmission is started then this information is applied for route maintenance.

When a route established between source and destination, data transmission stage can be started. In high mobility environments, link failure is a common phenomenon which can be occurred. We claim that the MRAODV routing algorithm is suitable for these environments. Source node is aware to stability of the routes which it has found in path discovery stage If an intermediate node in active route moves and link breaks source node cane select a stable route instead of failed rout. Iboth reverse RAODV and AODV routing algorithms, source node selects new path based on shortest path method and when mobile node moves quickly, these algorithms can not show good performance. Here, we add link stability parameter to RAODV algorithm to select the best route between available routes set, when active route fails.

V. IMPROVED ENERGY EFFICIENT AODV ROUTING PROTOCOL

In MRAODV we calculate the stability of each nodes and using this we estimate the relative stability of paths, and we select the path having maximum stability, but one lagging point of this protocol is that it doesn’t consider about the energy of nodes, what will happen if we select a path having maximum stability and a node with very less energy in the path? Using MRAODV we will choose that path because there is no consideration of energy in MRAODV, this may cause a breakage in path having maximum stability.

In IEEAODV the concept of energy is also included and so assigns the priority of different dedicated paths between source and destination on the basis of both energy as well as the stability of nodes or paths.

IEEAODV: In this protocol if there is need of path then source would broadcast a RREQ message to it’s neighbors and any of the neighbor is either destination or knows path to destination then it will broadcast the R-RREQ message to it’s neighbors otherwise rebroadcast the RREQ message to all it’s neighbors. Here in this protocol format of RREQ is same as IEEAODV but the format of R-RREQ packet slightly differ from that of MRAODV.

R-RREQ in IMRAODV contains following fields-

TYPE	RESERVE	HOP COUNT
Broadcast ID		
Destination IP address		
Destination Sequence number		
Source IP Address		
Reply time		
Energy		

When a node receives a R-RREQ message then it first compares its Energy with Energy of R-RREQ packet. After assigning the priorities to paths Source will select the path having higher priority, if this path breaks then next higher priority path will be selected.

VI. PERFORMANCE METRICS

We define the following metrics for studying the performance of 802.15.4. All metrics are defined with respect to MAC sub layer and PHY layer in order to isolate the effects of MAC and PHY from those of upper layers.

• Packet delivery ratio: The ratio of packets successfully received to packets sent in MAC sub layer. This metric does not differentiate transmissions and retransmissions, and therefore does not reflect what percentage of upper layer payload is successfully delivered, although they are related.

• Hop delay: The transaction time of passing a packet to a one-hop neighbor, including time of all necessary processing, back off as well as transmission, and averaged over all successful end-to-end transmissions within a simulation run. It is not only used for measuring packet delivery latency, but also used as a negative indicator of the MAC sub layer capacity. The MAC sub layer has to handle the packets one by one and therefore a long delay means a small capacity.

• RTS/CTS overhead: The ratio of request-to-send (RTS) packets plus clear-to-send (CTS) packets sent to all the other packets sent in 802.11. This metric is not applicable to 802.15.4, in which RTS/CTS mechanism is not used. We compare the performances of 802.11 and 802.15.4 to justify the dropping of RTS/CTS mechanism in 802.15.4.

VII. CONCLUSIONS

This paper presented a new protocol for Zigbee networks based on link stability and energy of paths. We changed MRAODV routing algorithm and made an optimized version of AODV. New method shows good performance in some ways. In IEEAODV we changed route replay packet content of MRAODV. These packets should be transmitted to destination node for building multiple routes. According to the theoretical concept, this algorithm is better than other version of AODV algorithm.

REFERENCES

[1]. IEEE 802.11, Part 11: Wireless LAN medium access control (MAC) and physical layer (PHY) specifications, IEEE, Aug.1999.

[2]. Will IEEE 802.15.4 Make Ubiquitous Networking a Reality?:A Discussion on a Potential Low Power, Low Bit Rate Standard by Jianliang Zheng and Myung J. Lee, The City College of CUNY

[3]. C. Karlof and D. Wagner, “Secure routing in wireless sensor networks: attacks and countermeasures,” In First IEEE International Workshop on Sensor Network Protocols and Applications, 2003.

[4]. A. Perrig, R. Canetti, D. Song, and D. Tygar, “The TESLA broadcast authentication protocol,” In RSA Cryptobytes, summer 2002.

[5]. Y. Hu, D. B. Johnson, and A. Perrig, “SEAD: Secure efficient distance vector routing for mobile wireless ad hoc networks,” In Proceedings of the 4th IEEE Workshop on Mobile Computing Systems & Applications (WMCSA 2002), pp. 3-13, IEEE, Calicoon, NY, June 2002.

[6]. L. Eschenauer and V. Gligor, “A key-management scheme for distributed sensor networks,” Conference on Computer and Communications Security. Proceedings of the 9th ACM conference on Computer and communications security, Washington, DC, 2002.

[7]. R. D. Pietro, L. V. Mancini, and A. Mei, “Random key assignment for secure wireless sensor networks,” In Proceedings of the 2003 ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN ’03), October 2003.

[8]. A. D. Wood and J. A. Stankovic, “Denial of service in sensor networks,” IEEE Computer Magazine, October 2002, pp. 54-62.

[9]. IEEE P802.15.4/D18, Draft Standard: Low Rate Wireless Personal Area Networks, Feb. 2003.

[10]. FIPS Pub 197 Advanced Encryption Standard (AES), Federal Information Processing Standards Publication 197, US Department of Commerce/N.I.S.T, Springfield, Virginia, November 26, 2001. (http://csrc.nist.gov/)

[11]. J. H. Schiller, Mobile Communications, Addison-Wesley, 2000.

[12]. Mehdi Zarei, Karim Faez and Javad Moosavi Nya ,”Modified Reverse AODV Routing Algorithm using Route Stability in Mobile Ad Hoc Networks” Proceedings ofthe 12th IEEE International Multitopic Conference, December 23-24, 2008.

[13]. Tarng, B.Chuang and F. Wu , "Link Stability-based Routing Protocol for Mobile Ad Hoc Networks", 2006 IEEE Conference on Systems, Man, and Cybernetics October 8-11, 2006, Taipei, Taiwan.

[14]. L. Layuan, L. Chunlin, Y. Peiyan, "Performance evaluation and simulations of routing protocols in ad hoc networks", s.l. : Elsevier, Computer Communications, 2007.

[15]. Izhak Rubin and Y. C. Liu, "Link Stability Models for QoS Ad Hoc Routing Algorithms," Vehicular Technology Conference, 2003. VTC 2003-Fall. 2003 IEEE 58th.

[16]. D. Johnson; Y. Hu; and D. Maltz. (2007). The dynamic source routing protocol (DSR) for mobile Ad Hoc networks for IPv4, *IETF RFC4728*.

[17]. Charles E. Perkins; Elizabeth M. Belding-Royer; Samir R. Das; and Mahesh K. Marina. (2001). Performance comparison of two on-demand routing protocols for Ad hoc networks, *IEEE Personal Communications*, 8(1), 16-28.

[18]. R. Dube, C.D. Rais, K.-Y. Wang, and S.K. Tripathi, Signal Stability-Based Adaptive Routing (SSA) for Ad Hoc Mobile Networks", IEEE Per-sonal Communications Magazine, vol. 4, no. 1, February 1997, pp.36-45.

BIOGRAPHY

P. Anitha is currently working as Associate Professor(sr) in the Master of Computer Applications at K.S.R. College of Engineering. She received her B.Sc degree and M.C.A degree in Madras University. Her research interest includes Mobile computing, Networks, Image processing, Zigbee Networks. She is a member of ISTE, CSI.

Dr.C.Chandrasekar is currently working as Reader in the Department of Computer Science at Periyar University, Salem. He received his B.Sc degree and M.C.A degree. He completed PhD in Periyar University, Salem at 2006. His research interest includes Mobile computing, Networks, Image processing, Data mining. He is a senior member of ISTE, CSI.