Volume 5, Issue 7, July 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Analysing and Fortifying the AODV Protocol with New Rules for Handling Multiple RREQ Packets

Bhumika*, Archana Singh Parmar
Computer Engineering & The Technological Institute of Textile & Sciences,
Haryana, India

Abstract— In the field of networking routing protocols play the crucial role, as the communicating nodes in the network always need a path to send their information. In this paper, we have studied and designed new rules for the existing AODV protocol for the Zig-Bee networks. The AODV protocol is reactive type of protocol and is called when the nodes necessitate path for data transmission. This protocol is invoked only when a new path is requisite. This research work aims to create new rules for handling multiple RREQ Packets. RREQ packets are basically broadcasted by nodes to get a path to destination. Zig-Bee networks are wireless radio networks created by Zig-Bee alliance.

Keywords—AODV, Message Number, RREQ, RREP, Zig-Bee Coordinator(ZC), Zig-Bee Router(ZR), Zig-Bee End Devices(ZEDs).

I. INTRODUCTION

A. Zig-Bee Overview

Zig-Bee 802.15.4 is a robust wireless personal area network (WPAN) developed by the Zig-Bee Alliance and based on the IEEE 802.15 standard. Zig-Bee 802.15.4 WPAN provides communication in short range with low data rate in low cost. A Zig-Bee network is designed using three types of devices which can be static or mobile in nature:

- Zig-Bee Coordinator (ZC): The initialization, maintenance, and control functions for the network are handled by ZC. Only one ZC can be deployed in one network.
- Zig-Bee Router (ZR): The router has a forwarding capability to forward sensed data to the base station[1].
- Zig-Bee End Devices (ZEDs): The end device lacks forwarding capability. These devices can communicate with ZR and ZC [4].

Zig-Bee devices are considered into full function devices (FFDs) and reduced function devices (RFDs). FFDs are used to send the frames for other devices and activate the network as the coordinator of the WPAN. This coordinator periodically transmits beacon frames by using slotted CSMA/CA, which makes RFDs enables to discover it and join the WPAN[3].

Zig-Bee 802.15.4 WPAN arrange its devices using three network topologies – star, mesh and cluster-tree as in Fig. 1. The star topology uses the centralized mechanism i.e. the terminal nodes cannot directly communicate with each other; these transfer data to each other using the centre node as medium. These devices are radically connected as the star architecture based on one centre node. The sensor node selected as a ZC (centre node) depletes its power much frequently than other nodes. The mesh topology also includes a ZC that recognizes the intact network. The communication pattern of mesh topology is decentralized that means each device can directly communicate with one another. In this topology, end-to-end connectivity between all nodes increases the complexity of the network. It operates in an ad-hoc fashion and follows multiple hops to transmit the information from one node to another node. This topology is more power-efficient as the communication process does not depend on one specific node. Last is the tree topology, which is particularly appropriate for low-power and low-cost wireless sensor networks as it sustains power saving operations and light- weight routing.

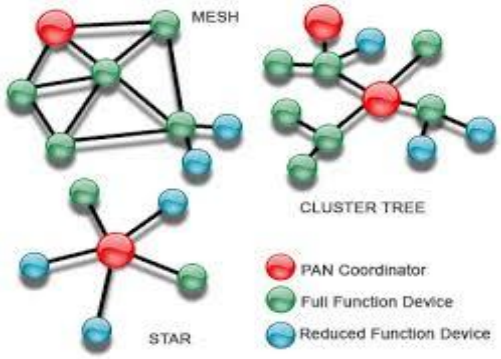


Fig. 1 Zig-Bee Topologies

IEEE 802.15.4 MAC super frame structure manages the power saving operation. The drawbacks of this topology are restricted routing and poor bandwidth utilization. Any link failure will abort the data delivery completely and the recovery operation incurs a significant overhead[1]. In a tree network, beacons can be announced by the ZC and ZRs. Though, in mesh network, regular beacons are not permitted. Basically beacons are vital method to hold up power organization. Consequently, when energy saving method is required, the tree topology is preferred[2].

Zig-Bee 802.15.4 WPAN exploits a non-persistent Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) Medium Access Control (MAC) protocol. A possible acknowledgement (ACK) message is needed as a conformance to the successful delivery of a data packet. The Zig-Bee protocol stack consists of four layers: the application (APL) layer, the network (NWK) layer, the medium access control (MAC) layer, and the physical (PHY) layer. The NWK and APL layers of the Zig-Bee protocol are defined by the Zig-Bee specification, where as the PHY and MAC layers are classified by the IEEE 802.15.4 standard. The APL layer provides an interface between the system and the end user. It also provides the framework for communication and applications in the network. The NWK layer handles maintenance, and provides routing over a multi hop network. The MAC layer facilitates the broadcasting of MAC frames with the help of physical channels, as well as handles the node associations also. The PHY layer finally offers the data transmission service. It provides an interface to the PHY layer management entity which keeps a record of WPAN information. The security aspect of Zig-Bee incorporates Frame Integrity Checking Function, Sequential Freshness, Data Encryption Entity Authentication Service, and Data Encryption. The security mechanism is implemented using a symmetric cipher to defend data to get enclosed by unauthenticated user[3].

B. Ad-hoc on-demand distance vector routing protocol (AODV)

AODV routing algorithm is a routing protocol design for mobile Ad-hoc networks and is using on-demand routing approach for establishment of route between nodes. As it uses on-demand routing therefore it built route to transmit data packets when the source node desired and is trying to maintain established route as long as they are needed. AODV protocol has quality to support unicast, multicast and broadcast routing with loop free, self starting and scalable characteristics. AODV protocol routes data packets between mobile nodes of ad hoc network. This protocol allows mobile nodes to pass data packets to required destination node through neighbour's node which cannot directly communicate. Nodes of network periodically exchange information of distance table to their neighbours and ready for immediate updates. AODV protocol is responsible to select shortest and loop free route from table to transfer data packets.

AODV routing protocol in ad hoc network communicate between mobile nodes through four types of different messages.

- Route Request
- Route Reply
- Route Error
- Hello Message

To establish a route between source and destination node Route Request (RREQ) and Route Reply (RREP) packet query cycle are used. Route Error (REER) and HELLO data packets are used for route maintenance [8].

This paper is organized in the following way: Section I gives the brief introduction about Zig-Bee WPAN and AODV protocol. Section II provides the literature review. Section III describes the proposed work and designed rules for the protocol. Finally Section IV gives the conclusion of the paper.

II. LITERATURE REVIEW

Wireless sensor networks (WSN) are regularly used for real-time applications, such as environment examination, therapeutic care, and automobile traffic control. The sensors nodes have depict some source limits, which are not withstanding accurate under these circumstances. WSNs have to afford an unwavering coverage of the area of curiosity and also to get together rigorous time control activities. Zig-Bee is a wireless personal area network based on IEEE 802.15.4 wireless protocol. Zig-Bee network defined first in 2004 and released in 2006. The second stack of the Zig-Bee network was defined as Zig-Bee 2006. It provides short distance communication with low complexity, low data rate and low power consumption. It is a two way technology which pointed to Wireless Sensor Network (WSN). Furthermore, it has several advantages such as self organization, smaller size of protocol stacks, and larger addressing space. Most commonly Zig-Bee also used in the medical field for patient monitoring or health and added together with self-care and self-management technologies can enhance their health outcomes. The main aim of this technology is remote control and sensor applications, which is appropriate to operate in ruthless radio environments and isolated locations [5].

Sukhvinder S. Bamber and Ajay K. Sharma investigated the performance of WPAN based on various topological scenarios like: cluster, star and ring. The comparative results have been reported for the performance metrics like: Throughput, Traffic sent, Traffic received and Packets dropped. Cluster topology is best in comparison with star and ring topologies as it has been shown that the throughput in case of cluster topology (79.887 kbits / sec) as compared to star (31.815 kbits / sec) and ring (1.179 kbits / sec) [6].

Amritpal Kaur, Jaswinder Kaur, Gurjeevan Singh implemented Zig-Bee using IEEE 802.15.4 protocol stack, it is most widely used technique in wireless sensor network for low rate wireless personal area network. Hybrid topologies are designed by using the possible combination of Zig-Bee network topologies and then analyze the affect of router and end devices failure. The performance of the network is evaluated by using parameters: throughput, delay, data dropped and

data traffic receive and sent. The results quantify that the combination of star and tree topologies gives good response and also effective to operate the network in worst condition [3].

Anantdeep, Sandeep kaur and Balpreet Kaur performed iterations by changing the Power of the transmitter and the throughput will has been analyzed to arrive at optimal values. An energy-efficient wireless home network based on IEEE 802.15.4, a novel architecture has been proposed. In this architecture, all nodes are classified into stationary nodes and mobile nodes according to the functionality of each node. Mobile nodes are usually battery-powered, and therefore need low power operation. In order to improve power consumption of mobile nodes, effective handover sequence based on MAC broadcast and transmission power control based on LQ (link quality) are employed [7].

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. 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.

P. Anitha and Dr. C. Chandrasekar gave the idea of IEEAODV in which 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. In this protocol if there is need of path then source would broadcast a RREQ message to its neighbours and any of the neighbours is either destination or knows path to destination then it will broadcast the R-RREQ message to its neighbours otherwise re broadcast the RREQ message to all its neighbours. When a node receives 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 [9].

III. PROPOSED MODEL

The AODV protocol is basically a reactive protocol that is called when a node in a network has some information to relay. It uses the concept of destination sequence number, the source node uses RREQ message to get the route by broadcasting the packet to its neighbouring nodes. The neighbouring nodes keep the packet which has the highest destination sequence number and drop other packets

In this modified protocol, a new field of message number is added in RREQ packet. Every node will have an attached message number and destination sequence number. The node which receives the multiple requests will enter the details of source node and compare the message number and destination sequence number using the rules of modified protocol which are explains in next section.

At a time, it will permit a single node to request the route for communication. Other RREQ messages are dropped.

A. Role of Message Number

Each node has a message number and destination sequence number. The message number is the message count of a node. Each node will have its own message count. If a new node starts communication for the first time, the message number of this node will be 1 and the complete transmission of this message, if it starts communication again, the message count will be increased by 1. So, the current node will have the message number 2 and so on. Each node has its message count depending upon the number of messages it has sent. In this proposed protocol, the message number works with destination sequence number to give it a complete form.

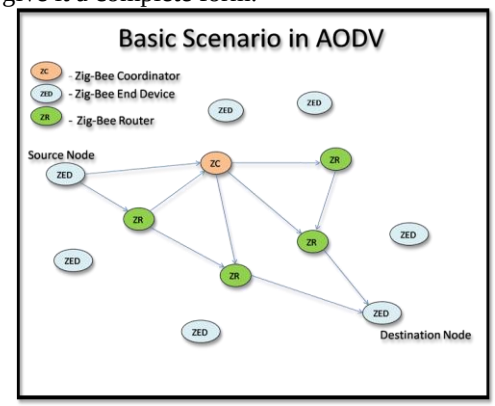


Fig. 2 Zig-Bee network in subnet

B. Proposed Protocol Rules:

Rules

Rule 1:

Node N1 broadcasts RREQ packet to its neighbor nodes. Let's say Neighbor nodes N3, N4.

Rule 2:
N3, N4 make their routing table and add the destination address, destination sequence number (SN) and message number (MN) of the source node.

Rule 3:
In between N2 starts sending RREQ packet to N3.

Rule 4:
N3 adds destination address, destination sequence number and message number of N2.

Rule 5:
N3 compares the message number and destination number of both the source nodes in its routing table according to following cases:

Case I:
If
MN of Node N1 = MN of Node N2
{
Then Check SN
}
If
SN of Node N1 < SN of Node N2
Then
N2 is allowed to get its route

Case II.
If
MN of Node N1 = MN of Node N2
{
Then Check SN
}
If
SN of Node N1 = SN of Node N2
Then
N1 is allowed to get its route

Case III.
If
MN of Node N1 > MN of Node N2
{
Then
N2 is allowed to get its route
}

Rule 6:
Select one request at a time and drops other requests.

Rule 7:
The request reaches to destination by broadcasting the RREQ packet to every neighbor node.

Rule 8:
The destination sends RREP packet in unicast manner in backward direction. Ultimately the route is sent to Source Node.

Rule 9:
Source Node starts sending information to the node specified in step 8.

Rule 10:
If any link is lost, RERR packet is sent by the node whose link has broken to the other nodes.

According to the proposed protocol, the upper defined rules are followed along with the basic mechanism of AODV protocol.

C. Protocol Description

This portion describes the protocol in stepwise manner. All the steps are explained following:

In step 1, when a node has some information and no route for transmission, it starts broadcasting RREQ message to its neighboring nodes. All the nodes use the same mechanism of passing the RREQ message to their own neighboring nodes. Ultimately, the RREQ is passed to destination node. In short, this message is passed over to find the route to reach up to destination.

In step 2, the nodes which receives the RREQ packet, they make their routing table and store the destination address, destination sequence number and message number to use by the protocol. They play a very important role in deciding which node will be allowed to request a route.

In subsequent steps, Suppose in between when the neighbouring nodes which received the RREQ message is making table entry for first route request, receives a new request that comes from any other node, then it will make table entry for that node too, stores the details and then compares using the defined cases.

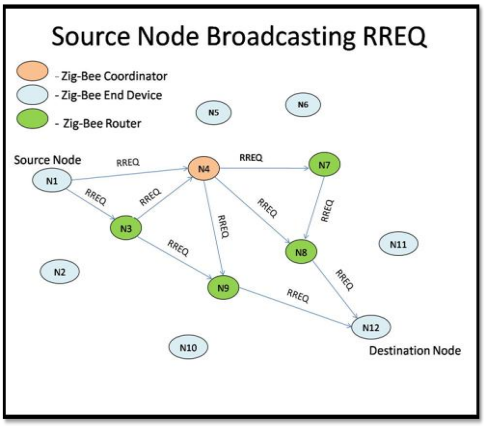


Fig 3 One RREQ Packets

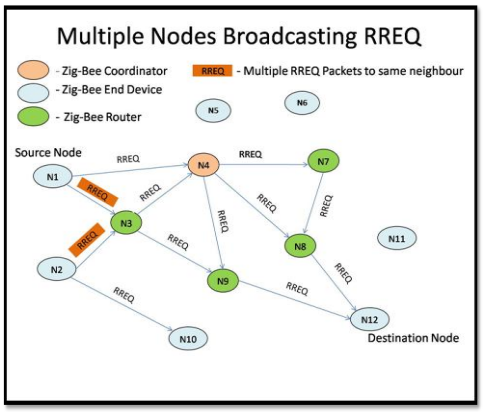


Fig 4 Multiple RREQ Packets

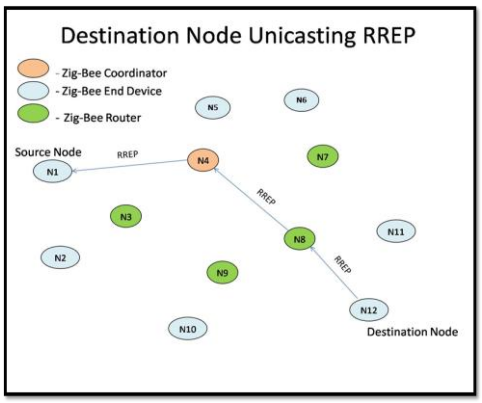


Fig 5 Sending Back RREP packet to Source

After comparison and selecting one RREQ message at a time, it discards all other request messages.

Case 1 shows if message number of both the source nodes is equal, then check the destination sequence number of both the nodes. The node which has higher destination sequence number will be permitted to send the RREQ message.

Case 2 shows if message number of both the source nodes is equal, then check the destination sequence number of both the nodes. If the destination sequence number is also equal then the node first come first serve (FCFS) method is deployed. The node which sends RREQ message first will be allowed to send the RREQ message.

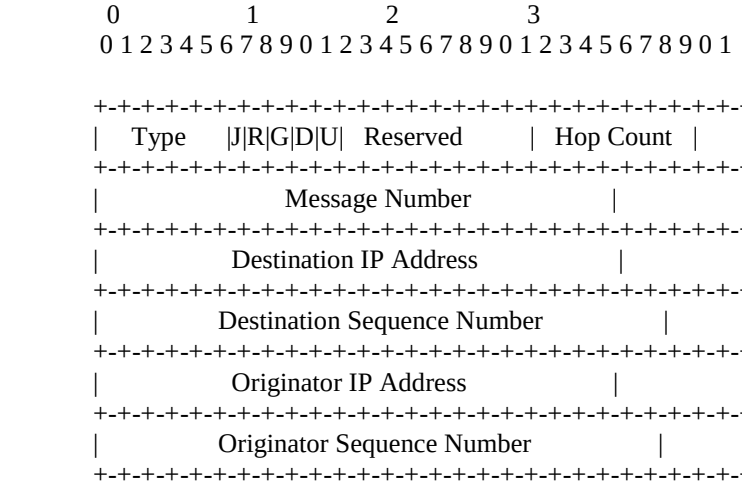
Case 3 shows if message number of source node 1 is greater than the message number of source node 2, then check the destination sequence number of both the nodes. And if the destination sequence number is equal then the source node which has lesser message number will be allowed to end the RREQ message.

Case 4 shows if message number of source node 1 is greater than the source node 2, then check the destination sequence number of both the nodes. And if the destination sequence number is also greater than the destination sequence number of source node 2 then the source node which has lesser message number will be allowed to send the RREQ message.

The chosen RREQ packet is broadcasted until it reaches the destination. The destination node unicast the RREP message in a single hop fashion and the route is informed to the source node. Then the source node starts communication

If any link is found broken, a RERR message is sent by the node to other nodes informing the link has broken and to reestablish a new route.

D. Modified Route Request (RREQ) Message Format



The modified format of the Route Request message is given above, and contains the following fields:

Type 1

J

Join flag; reserved for multicasts

R

Repair flag; reserved for multicast

G

Gratuitous RREP flag; indicates whether a gratuitous RREP should be unicast to the node specified in the Destination IP Address

D

It is Destination only flag; indicates only the destination may respond to this RREQ

U

This represents Unknown sequence number; indicates the destination sequence number is unknown

Reserved

Sent as 0; ignored on reception.

Hop Count

The number of hops from the Originator IP Address to the node handling request.

Message Number

It represents the message count of each node separately.

Sequence Number

A sequence number uniquely identifying the particular RREQ when taken in conjunction with the originating node's IP address

Destination IP Address

The IP address of the destination for which a route is desired

Destination Sequence Number

The latest sequence number received in the past by the originator for any route towards the destination

Originator IP Address

The IP address of the node which originated the Route Request

Originator Sequence Number

The current sequence number to be used in the route entry pointing towards the originator of the route

IV. CONCLUSIONS

In this paper, the proposed concept of AODV protocol has solved problems of handling the situation of multiple requests. Hence, this approach can perform better as newly proposed rules for AODV protocol are very useful because in the designed network, every node will get the chance to relay their data, the nodes will not have to wait for communication. As in the existing protocol the RREQ packets of the nodes are dropped whose destination sequence number is smaller. So, if multiple RREQ packets are received by a node, it will do accordingly and not let any message to wait for a long time.

REFERENCES

[1] Shayma Wail Nourildean, "Study of Zig-Bee NETWORK TOPOLOGIES for Wireless Sensor Network with One Coordinator and Multiple Coordinators," Tikrit Journal of Engineering Sciences/Vol.19/No.4/December 2012, (65-81).

[2] Mumtaz M.Ali AL-Mukhtar, Teeb Hussein Hadi, "Diagnosis of Failures in Zig-Bee Based Wireless Sensor Netwroks," IJCSET |March 2013 | Vol 3, Issue 3, 104-108.

[3] Amritpal Kaur, Jaswinder Kaur, Gurjeevan Singh, "Node Failure Investigation in Zig-Bee Sensor Network," I2CT, Vol. 2, Issue 1, 2014 ISSN (online):2321-7316 CT International Journal of Information & Communication Technology.

[4] JunWang, Min Chen, Victor C.M. Leung, "Forming priority based and energy balanced Zig-Bee networks—a pricing approach‖," Telecommun Syst, DOI 10.1007/s11235-011-9640-z.

[5] B. Meenakshi, P. Anandhakumar, "Optimization of energy consumption by fuzzy based routing in wireless sensor network." IOSR Journal of Electronics and Communication Engineering (IOSRJECE) ISSN : 2278-2834 Volume 2, Issue 1 (July-Aug 2012), PP 31-35.

[6] Jennic, Jennic's Zig-Bee e-learning Course. Available: http://www.jennic.com/elearning/Zig-Bee/index.htm

[7] Sukhvinder S. Bamber and Ajay K. Sharma, "Comparative Performance Investigations of different scenarios for 802.15.4 WPAN," IJCSI International Journal of Computer Science Issues, Vol. 7, Issue 2, No 4, March 2010 ISSN (Online): 1694-0784 ISSN (Print): 1694-0814

[8] http://www.nada.kth.se/kurser/kth/2D1490/05/lectures/feeney_mobile_adhoc_routing.pdf

[9] P. Anitha, Dr. C. Chandrasekar, "Energy Aware Routing Protocol For Zig-Bee Networks", Journal of Computer Applications (JCA) ISSN: 0974-1925, Volume IV, Issue 3, 2011

