Comparative Performance Evaluation of Routing Algorithms in IEEE 802.15.4 and IEEE 802.11 with Different Ad Hoc Routing Protocol

[1]P. Anitha and [2]C. Chandrasekar
[1]KSR College of Engineering, Tiruchengode, India
[2]Computer Science, Periyar University, Salem, Tamilnadu, India

Abstract: Problem statement: Wireless ADHOC networks are self organized dynamic networks can share wireless channel without any established central control standard for IEEE 802.11. **Approach:** The most common protocols are AODV, DSDV, DSR in ADHOC used to ensure the data transmission among themselves. To meet the need of low power and low cost IEEE 802.15.4 standard was developed for sensor networks. **Results:** Aim of the study is develop an Ad hoc routing protocol in IEEE 802.15.4 this will give more performance in the order of the low cost, low power, guarantee data transmission in routing than IEEE 802.11 Wireless LAN and also we address the comparison and performance analysis also measure the impact of these two standards how ADHOC routing protocols perform in sensor networks. **Conclusion/Recommendations:** At this point we address the comparison and performance analysis also measure the impact of these two standards in wireless technology.

Key words: ADHOC standard, low data rate, low power, performance analysis, wireless technology, Industrial Scientific Medical (ISM), routing protocols, Physical Layer (PHY), Request-To-Send (RTS), Clear-To-Send (CTS), energy consumption

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 study is to analyze the performance of these Sensor nodes working under ADHOC routing protocols. In section II, we give a brief description of 802.15.4. Next, in section III, we outline the NS2 simulator for 802.15.4. Then, in section IV, we define a set of performance metrics.

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

Corresponding Author: P. Anitha, Master of Computer Applications, KSR College of Engineering, Tiruchengode

communications are inherently susceptible to interception and interference. Some security research has been done for WLANs and wireless sensor networks (Karlof and Wagner, 2003; Perrig *et al.*, 2002; Hu *et al.*, 2002; Eschenauer and Gligor, 2002; Pietro *et al.*, 2003; Wood and Stankovic, 2002; Alfawaer *et al.*, 2007; Buratti and Verdone, 2009; Chen *et al.*, 2007; E1 Emary and A1-Rabia, 2005; Jayakumar and Gopinath, 2008; Lu *et al.*, 2004; Murad and Al-Mahadeen, 2007; Sapuan, 2005; Verdone *et al.*, 2008), but pursuing security in wireless networks remains a challenging task. 802.15.4 Employs a fully handshake protocol for data transfer reliability and embeds the Advanced Encryption Standard (AES) for secure data transfer. In the following subsections, we give a brief overview of the PHY layer, MAC sub layer and some general functions of 802.15.4.

MATERIALS AND METHODS

The main objective is to assess the adequateness of current standard and zigbee technology, for enabling large scale wireless sensor network applications with Qos requirements. The hypothesis is that this is possible by using the IEEE 802.15.4 and Zigbee protocols combined with commercial hardware/software platforms.This addresses the performance analysis of these protocols as well as to produced better performance compare with IEEE 802.15.4.

The 802.15.4 super frame is assumed to consist fully of the active period. Since our interest is in the CAP, there is no Contention-Free Period (CFP) in the super frame. There are assumed to be nodes connected to a PAN coordinator in a star topology and communicating with it directly. All the nodes are assumed to be within the carrier sensing range of each other. This assumption removes the possibility of hidden nodes and resulting collisions. There are no MAC level acknowledgements. The MAC layer does not have an interface queue. It accepts new packets from the upper layer only when it not attempting to transmit a previously received packet. Since we are analyzing the star topology, there is no need for a routing layer.

Ns2 simulator: The 802.15.4 NS2 (Hu *et al.*, 2002) simulator developed at the Joint Lab of Samsung and the City University of New York confirms to IEEE P802.15.4/D18 Draft. Figure 1 outlines the function modules in the simulator and a brief description is given below for each of the modules. Wireless Scenario Definition: It selects the routing protocol; defines the network topology; and schedules events such as initializations of PAN Coordinator, coordinators and devices and starting (stopping) applications.
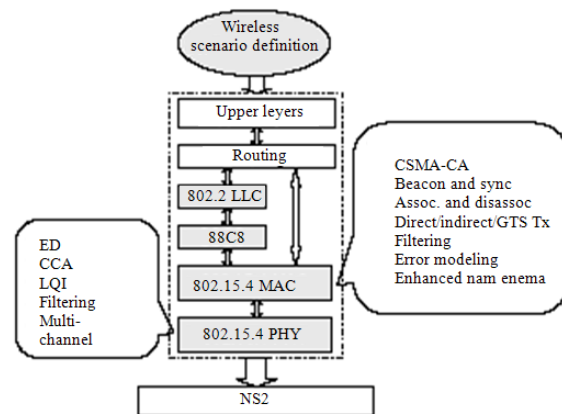

Fig 1: NS2 Simulator for IEEE 802.15

It defines radio-propagation model, antenna model, interface queue, traffic pattern, link error model, link and node failures, super frame structure in beacon enabled mode, radio transmission range and animation configuration:

- Service Specific Convergence Sub layer (SSCS): This is the interface between 802.15.4 MAC and upper layers. It provides a way to access all the MAC primitives, but it can also serve as a wrapper of those primitives for convenient operations. It is an implementation specific module and its function should be tailored to the requirements of specific applications
- 802.15.4 PHY: It implements all 14 PHY primitives
- 802.15.4 MAC: This is the main module. It implements all the 35 MAC sub layer primitives

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

RESULTS AND DISCUSSION

We have developed a set of performance metrics for comparing different routing algorithms including delay, load and energy and packet delivery ratio.

Here this graph it shows the delay performance with respect to load with AODV routing protocol by way of two different wireless MAC standards namely 802.11 used for adhoc and meant for 802.15.4 zigbee. Here load consider as packet interval, it illustrates if the load decreased the 802.15.4 delay time increased. 0.1 packet interval time of load sends packet at every 0.1 seconds. As well as if the load increased automatically the delay time decreased in 802.15.4 and during 802.11 its increased. As such the delay gives the results of packet transmission time between two nodes of source and destination end. Here we can classify the performance of two different protocols with load of packet interval and delay transmission time among two ends. The above graph shows zigbee standard takes less delay time though the load increased to deliver packets than ADHOC standard.

Figure 2A the forward route to the destination is updated on receiving a route reply packet. AODV uses sequence numbers to determine the timeliness of each packet delay vs. load. Figure 2B to relieve this problem, DSR requires each node to defer its reply for a period proportional to the length of route in its RREP. If during this delay, the node hears a data packet using a route shorter than the one it is deferring, then it may infer that the source already has a better path to the destination and may cancel its RREP for this route discovery. Figure 2C DSDV exhibits longer average end-to-end delay all the time regardless to node mobility rate compared to the other two protocols. I-DSDV uses a message exchange delay and to prevent loops.

The graph (Fig. 3 a-c) explains the comparison of Packet delivery ratio with load in routing protocol of AODV. Here we consider two protocol standard to get results. The ADHOC standard of 802.11 and the zigbee standard of 802.15.4 in mac layer standard. By using

zigbee standard AODV protocol provides 66 percentages to 100 percentage Packet delivery fraction while changing load. By default zigbee designed for low rate wireless network. Here load consider as packet interval time. Though increasing packet interval from 0.1 to 0.5 seconds its increase the no of packet transmission also. Consequently the packet delivery fractions also varied. During ADHOC standard 80 percentages to 100 percentage packet deliveries can be achieved by means of varying packets. This result shows the performance comparison study of reactive routing protocol in two different mac layer type protocols.

The graph shows the comparison of the energy consumption of two different MAC standards 802.15.4 and 802.11. Depends on the load, type of communication between mobile nodes and modulation techniques the overall network energy consumption varies as per different standards. Here graph shows 802.15.4 consumes more energy than 802.11 standards.
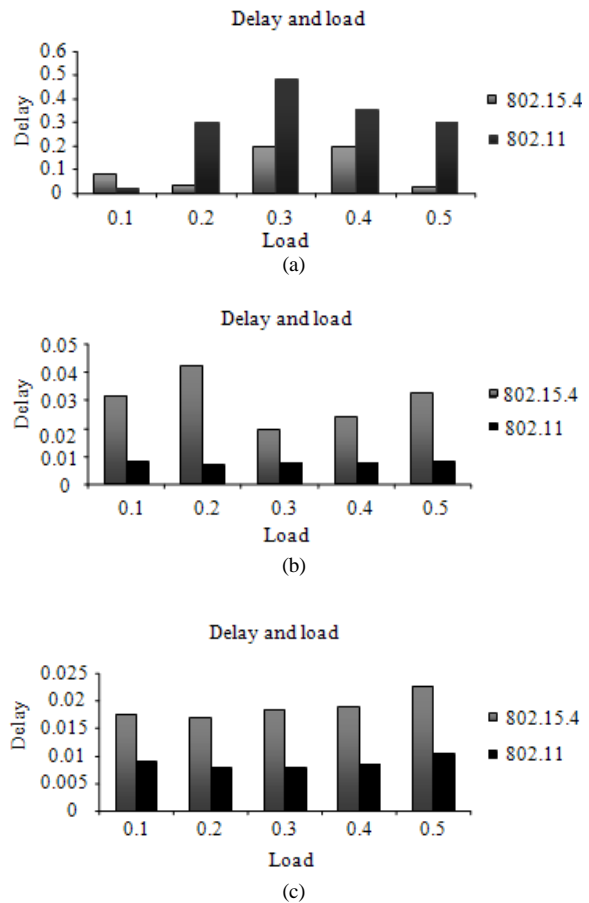

Fig. 2: (a) Average delay and load of AODV (b) Average delay and load of DSR (c) Average delay and load of DSDV
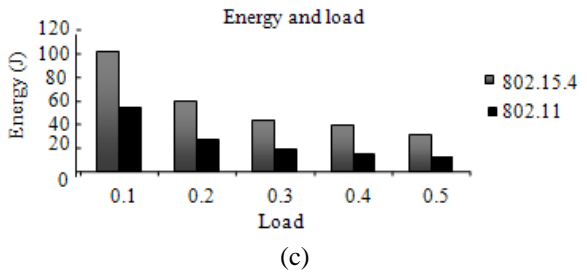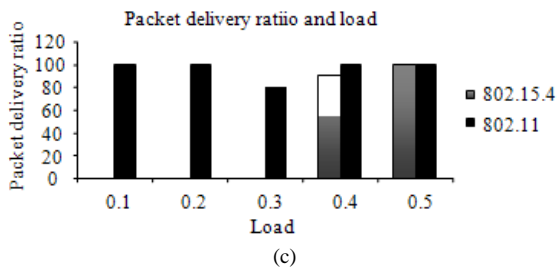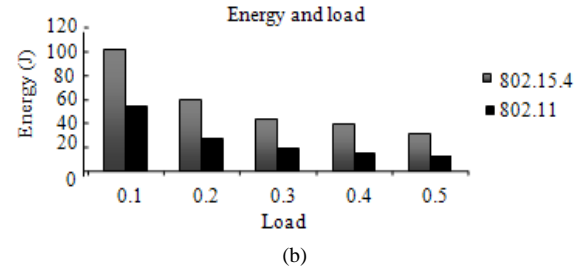
(a)

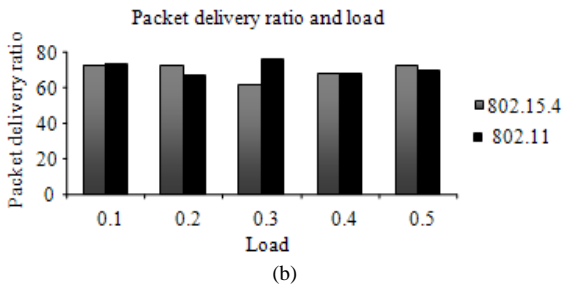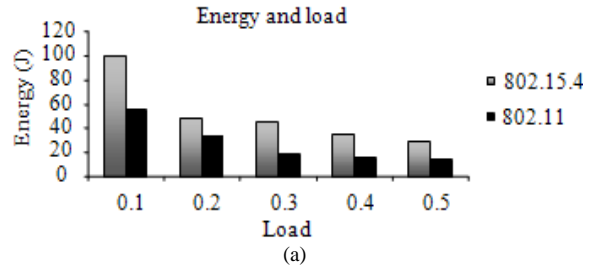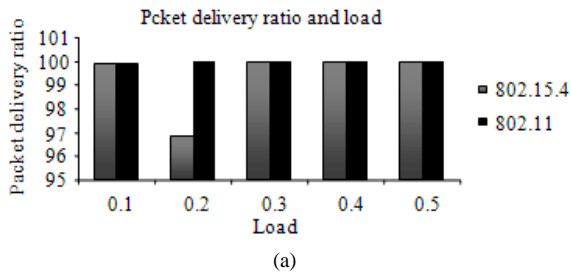(a)

(b)

(b)

(c)

(c)

Fig. 3: (a) Average PDR and load of AODV (b) average PDR and load of DSR (c) average PDR and load of DSDV

Fig. 4: (a) Average energy and load of AODV (b) average energy and load of DSR (c) average energy and load of DSDV

If the load increases energy consumption also increases. Figure 4A the protocol takes node remaining energy as routing control condition. By avoiding the low-energy nodes being involved in routing, generally 802.15.4 is low rate and low power device. 802.11 consume more energy than 802.15.4 MAC standard. The above graph represents zigbee give more performance than ADHOC standard. Figure 4B DSR is a source routing protocol and requires the sender to know the complete route to destination. It is based on route discovery and route maintenance process. Discovered routes will be cached in the relative nodes. Figure 4C Route discovery Route Request packets are propagated throughout the network thereby establishing multiple paths at destination node and at the intermediate nodes.

CONCLUSION

In this study the new IEEE 802.15.4 standard, which is designed for low rate wireless personal area networks (LR-WPANs), is an enabling standard. It brings to light a host of new applications as well as changes many other existing applications. It is the first standard to allow simple sensors and actuators to share a single standardized wireless platform. To evaluate the general performance of this new standard, we develop an NS2 simulator, which covers all the 802.15.4 PHY and MAC primitives and carry out comparing the performance between 802.15.4 and 802.11.But in this comparisons IEEE 802.11 produced better performance compare with IEEE 802.15.4.Our future work involve develop the new protocol for this that will give the better result than 802.11.

REFERENCES

Alfawaer, Z.M., G. Hua and N. Ahmed, 2007. A novel multicast routing protocol for mobile ad hoc networks. Am. J. Applied Sci., 4: 333-338. DOI: 10.3844/ajassp.2007.333.338

Buratti, C. and R.Verdone, 2009. Performance analysis of IEEE 802.15.4 non beacon-enabled mode. IEEE Trans. Veh. Technol., 58: 3480-3494. DOI: 10.1109/TVT.2009.2014956

Chen, Z., C. Lin, H. Wen and H. Yin, 2007. An analytical model for evaluating IEEE 802.15.4 CSMA/CA protocol in low-rate wireless application. Proceedings of the 21st International Conference on Advanced Information Networking and Applications Workshops, May 21-23, IEEE Xplore, Niagara Falls, Ont., pp: 899-904. DOI: 10.1109/AINAW.2007.77

E1 Emary, I.M.M. and A.I. A1-Rabia, 2005. Estimation techniques for monitoring and controlling the performance of the computer communication networks. Am. J. Applied Sci., 2: 1395-1400. DOI: 10.3844/ajassp.2005.1395.1400

Eschenauer, L. and V.D. Gligor, 2002. 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, (CCCS'02), ACM New York, NY, USA., pp: 41-47. DOI: 10.1145/586110.586117

Hu, Y.C., D.B. Johnson and A. Perrig, 2002. SEAD: Secure efficient distance vector routing for mobile wireless ad hoc networks. Ad Hoc Networks, 1: 175-192. DOI: 10.1016/S1570-8705(03)00019-2

Jayakumar, G. and G. Gopinath, 2008. Performance comparison of two on-demand routing protocols for ad-hoc networks based on random way point mobility model. Am. J. Applied Sci., 5: 659-664. DOI: 10.3844/ajassp.2008.659.664

Karlof, C. and D. Wagner, 2003. Secure routing in wireless sensor networks: Attacks and countermeasures. Ad Hoc Networks, 1: 293-315. DOI: 10.1016/S1570-8705(03)00008-8

Lu, G., B. Krishnamachari and C.S. Raghavendra, 2004. Performance evaluation of the IEEE 802.15.4 MAC for low-rate low-power wireless networks. Proceedings of the IEEE International Conference on Performance, Computing and Communications, (CPCC'04), Southern California Univ., USA., pp: 701-706. DOI: 10.1109/PCCC.2004.1395158

Murad, A.M. and B. Al-Mahadeen, 2007. Adding quality of service extensions to the enhanced associativity based routing protocol for Mobile Ad Hoc Networks (MANET). Am. J. Applied Sci., 4: 874-879. DOI: 10.3844/ajassp.2007.874.879

Perrig, A., R. Canetti, J.D. Tygar and D. Song, 2002. The TESLA Broadcast Authentication Protocol. The Pennsylvania State University. http://citeseerx.ist.psu.edu/viewdoc/summary?doi= 10.1.1.94.7500

Pietro, R.D., L.V. Mancini and A. Mei, 2003. Random key-assignment for secure wireless sensor networks. Proceedings of the 1st ACM Workshop on Security of Ad Hoc and Sensor Networks, (SASN'03), ACM New York, NY, USA., pp: 62-71. DOI: 10.1145/986858.986868

Sapuan, S.M., 2005. A conceptual design of the concurrent engineering design system for polymeric-based composite automotive pedals. Am. J. Applied Sci., 2: 514-525. DOI: 10.3844/ajassp.2005.514.525

Verdone, R., D. Dardari and G. Mazzini, 2008. Wireless Sensor and Actuator Networks: Technologies, Analysis and Design. 1st Edn., Elsevier/Academic Press, USA., ISBN-10: 0123725399, pp: 362.

Wood, A.D. and J.A. Stankovic, 2002. Denial of service in sensor networks. Computer, 35: 54-62. DOI: 10.1109/MC.2002.1039518