I2CT, Vol. 2, Issue 1, 2014

ISSN (online) :2321-7316

CT International Journal of Information & Communication Technology

www.ctgroup.co.in

Node Failure Investigation in Zigbee Sensor Network

Amritpal Kaur [1,] Jaswinder Kaur [2,] Gurjeevan Singh [3]

[1,2]Deptt of ECE SBSSTC, [3]Deptt of ECE SBSSTC (Polywing), Ferozepur, Punjab, India

gurdevgill2123@gmail.com[1], jaswinder.ece@gmail.com[2], gurjeevansandhu@gmail[3]

ARTICLE INFO:

Article history:
Received 3 June, 2014
Revised 31 August, 2014
Available online 12 Sept., 2014

Keywords:
Hybrid Network Topology, Zigbee Wireless Sensor Network, Router and End Device Failure.

ABSTRACT

This research work is implemented in ZigBee 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 ZigBee 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.

I. INTRODUCTION

Wireless sensor networks (WSN) are regularly used for real-time applications, such as environment examination, therapeutic care, and automobile traffic control. The sensor 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 [1]. Zigbee is a wireless personal area network based on IEEE 802.15.4 wireless protocol. Zigbee network defined first in 2004 and released in 2006. The second stack of the Zigbee network was defined as Zigbee 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) [2]. Furthermore, it has several advantages such as self organization, smaller size of protocol stacks, and larger addressing space. Most commonly Zigbee 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 [3]. The main aim of this technology is remote control and sensor applications, which is appropriate to operate in ruthless radio environments and isolated locations. IEEE 802.15.4 based WSN defines the physical and MAC layers. It use CSMA / CA mechanism and solves the problem of channel access [4]. The MAC layer of IEEE 802.15.4 standards operates in two modes, they are beacon enabled and non-beacon enabled mode. In beacon enabled mode, beacon messages are transmitted periodically for network organization and management. Beacon enabled are synchronized and allows the mode to operate on slotted Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) mechanism. In non-beacon mode nodes are not synchronized, because periodic beacon transmissions are absent. Therefore, this mode supported to unslotted CSMA/CA mechanism [5]. Zigbee protocol stack consists of three layers. The upper layer is application layer (APL), which provide interface between the Zigbee system to its end users and also defines the device functionality. The basic function of this layer is to convert the input into digital data, and/or converts digital data into output. The middle layer known as the network layer (NWK) is responsible for network structure, routing, and security such as encryption, key management, and authentication. The lower layer is the physical layer and functionality of this layer is to transmit or receive data using certain radio channels with specified modulation and spreading techniques [6, 7].

In [8] the author only analyzes the performance of tree topology in case of node failure. This paper investigate the performance of hybrid network which is implemented by the possible combinations of ZigBee routing schemes and then analyze the affect of router and end device failure on the performance parameter of networks.

II. SYSTEM MODEL

There are four Zigbee releases, which are ZigBee 2004 (released in December 2004), ZigBee 2006 (released in December 2006), and finally ZigBee 2007 and ZigBee Pro (released in October 2007). On each new release there is an improvement according to the previous releases and new releases have backward compatibility with the old releases. The Zigbee standard is based, at the first two layers of the ISO/OSI stack, on the IEEE 802.15.4 standard. IEEE 802.15.4 is a standard for wireless Personal Area Networks (PANs), which provide low data rate at short communication range with low cost. It also uses a non-persistent Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) Medium Access Control (MAC) protocol. An optional acknowledgement (ACK) message is required to confirm the successful delivery of a data packet. In case of ACK messages, the access mechanism of the non-persistent CSMA/CA MAC protocol is modified to some extent [9, 10]. The ZigBee protocol stack consists of four main layers: the application (APL) layer, the network (NWK) layer, the medium access control (MAC) layer, and the physical (PHY) layer. While the NWK and APL layers of the ZigBee protocol are defined by the ZigBee specification, the PHY and MAC layers are defined by the IEEE 802.15.4 standard. The application layer provide effective interface between the system and the end user. A framework for communication and applications in the network are provided by the application layer. The functionalities of network layer include maintenance, providing and organizing routing over a multihop network, route discovery. The medium access control (MAC) enables the transmission of MAC frames through the use of the physical channel. Besides the data service, it offers a management interface and itself manages access to the physical channel and network beaconing. It also controls frame validation, guarantees time slots and handles node associations. Finally, it offers hook points for secure services. The physical layer (PHY) ultimately provides the data transmission service, as well as the interface to the physical layer management entity, which offers access to every layer management function and maintains a database of information on related personal area networks [11]. The security mechanism of Zigbee includes Data Encryption, Sequential Freshness, Frame Integrity Checking Function, and Entity Authentication Service. Data Encryption is implemented with a symmetric cipher to protect data from being read by the parties without cryptographic key. ZigBee adopts AES-128 key for security [12]. The Frame Integrity Checking function use Message Integrity Code (MIC) in the each data frame to protect data from hackers or by those parties, which do not have cryptography key. Entity Authentication Service provides a secure means for a device to synchronize information with another device simultaneously based on a shared key [13]. There are three different devices supported by ZigBee, which are ZigBee Routers (ZR), ZigBee Coordinator (ZC), and ZigBee End Devices (ZED). ZRs are responsible from performing the IEEE 802.15.4's tasks for routing the packets. ZCs coordinate and manage all devices in the network. ZEDs are simple devices and do not have any routing capabilities [9]. According to their functionality, these devices can be categorized into full function devices (FFDs) and reduced function devices (RFDs). FFDs are able to forward frames for other devices and start up the network as the coordinator of the PAN. A coordinator can periodically broadcast beacon frames by using slotted CSMA/CA, so that nearby RFDs can discover it and join the PAN. The default addressing method for ZigBee networks is Distributed Address Assignment Mechanism (DAAM). DAAM reserves a unique address for each possible location with a given setting of the topological parameters. In DAAM the ZC/ ZR can locally allocate addresses to its children with global setting of the topological parameter and the knowledge of its own depth value [14]. In ZigBee, a device can obtain a network address from the coordinator or a router and join a network successfully. In case of network formation, the coordinator determines the maximum number of children of a router (*Cm*), the maximum number of child routers of a router (*Rm*), and the depth of the network (*Lm*). Note that a child of a router can be a router or an end device, so *Cm* ¸ *Rm*. Cm, Rm, and Lm parameters are used to calculate nodes' network addresses. While these parameters facilitate address assignment, they also prohibit a node from joining a network [15]. Three main types of network topology are considered in IEEE 802.15.4, namely, the star, generic mesh and cluster tree topology. In the star topology, a FFD takes up the role of the PAN coordinator; the other nodes communicate with the PAN coordinator. In generic mesh topology, a FFD can communicate with other nodes within its radio range and outside of its radio coverage through an intermediate device by forming a multi-hop network. In the tree-topology nodes associated to a single PAN coordinator are arranged in parent–child relationships by establishing a tree [16].

III. SIMULATION SCENARIO

Zigbee has been define the three routing schemes i.e. star, tree and mesh but in this paper the performance is analyzed by making three hybrid topologies by using possible combinations of the different routing schemes. So the hybrid topologies used to analyze under different network configurations are star-tree (ST), star-mesh (SM) and mesh-tree (MT). The hybrid topologies are designed by using two PAN coordinators in office scale network and two different topologies are assigned to these coordinators. The affect of device failure has been analyzed for these new hybrid networks using different network parameters. The main intention of this work is to quantify the performance of hybrid topologies better than the network containing single coordinator.

The simulation of Zigbee network has been done using OPNET 14.5 and presents the preliminary simulation result to illustrate the attributes of hybrid network in case of node failure. The devised system distributes different Zigbee devices in an area (an office network scale) of (100m x 100m). The performance of these networks has been examined under different network configuration as shown in Table 1.

TABLE I. SIMULATION PARAMETERS

Network Scale	100 m*100m
Number Of Nodes	50
Network Type	Mixed
Mobility Model	Random Waypoint (Record Trajectory)
Speed of Mobile Nodes	2 m/s
Pause Time	150 s
Simulation Duration	300 s

There are three networks, in each network there are two ZC. In case of MT network, tree topology assign to one coordinator and mesh topology assigned to another one. In case of ST network, star topology assign to one coordinator and tree topology assigned to second. In case of SM network, mesh topology assign to one coordinator and star topology assigned to another coordinator. Using Table1. nine scenarios has been designed. First, second and third scenarios analyze the performance of hybrid topologies under ZR failure. Fourth, fifth and sixth scenarios analyze the performance of hybrid topologies under ZED and ZR failure at same instant of time. Seventh, eighth and ninth scenarios analyze the performance of hybrid topologies under ZED failure.

IV. RESULTS and DISCUSSIONS

Following results are used to enumerate the performance of network.

A. *Throughput*

Throughput is the ratio of the total amount of data that a receiver receives from a sender to a time it takes for receiver to get the last packet. Throughput is the data quantity transmitted correctly starting from the source to the destination within a specified time (seconds). A low delay in the network translates into higher throughput. Throughput is quantified with varied factors including packet collisions, obstructions between nodes and the type of used topology. The results shown in fig. 1,2 and 3 discovered that maximum throughput achieved by ST network and minimum by MT network in all cases of failure. But throughput of ST and MT network degrades when ZED and ZR fail at similar time, whereas SM network mostly affected by the failure of ZR. As the MT network contain more number of routers and less number of end devices than SM and ST networks.

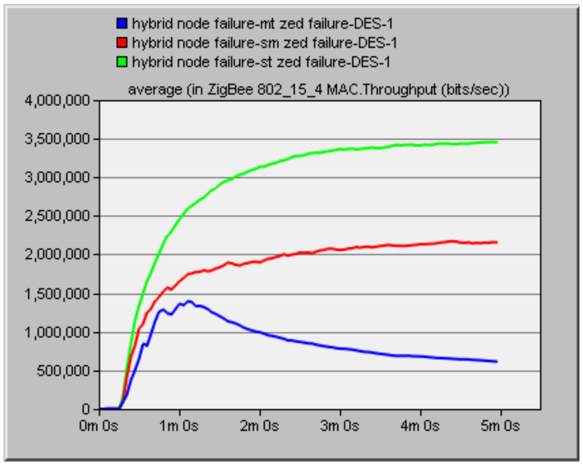

Figure1. Throughput in MT, SM and ST Topologies in Case of ZED Failure

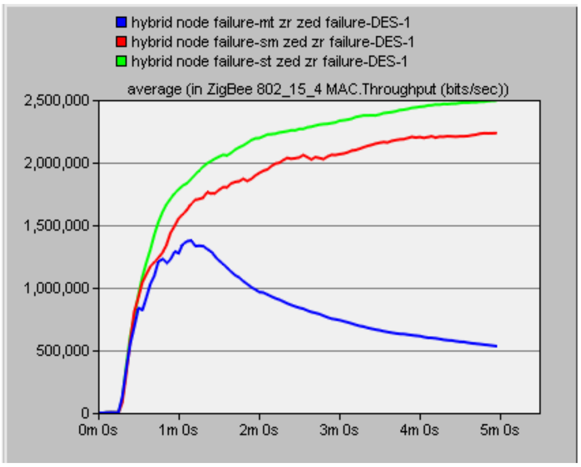

Figure2. Throughput in MT, SM and ST Topologies in Case of ZED and ZR Failure

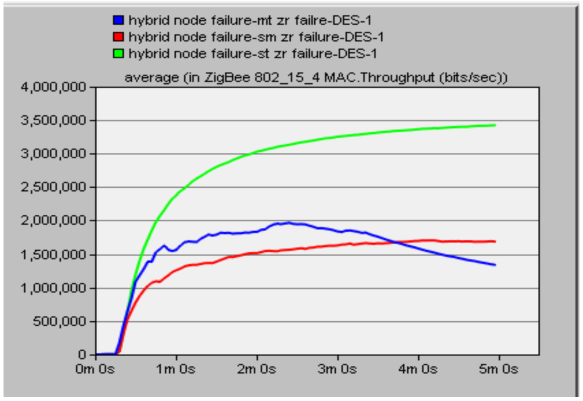

Figure3. Throughput in MT, SM and ST Topologies in Case of ZR Failure

B. *Data Dropped*

This statistic records the total amount of data that was received from the upper layer and then dropped by all nodes in the network due to repeatedly failed retransmissions (i.e., exceeded the corresponding short retry or long retry threshold value). Maximum data dropped by MT network and minimum by SM. The ZED individual failure and ZED, ZR both failure affect the network in similar manner (referred to fig. 4 and 5), whereas ZR individual failure show less affect then other case as shown in fig 6.

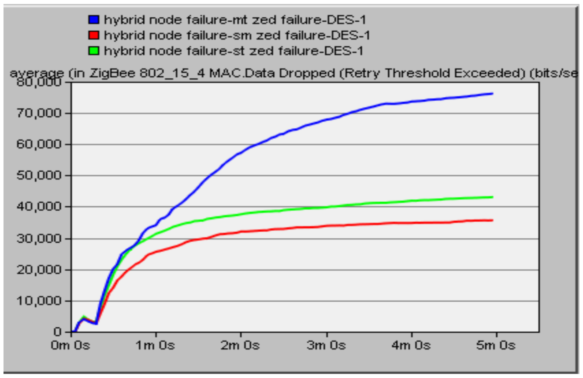

Figure4. Data Dropped in MT, SM and ST Topologies in Case of ZED Failure

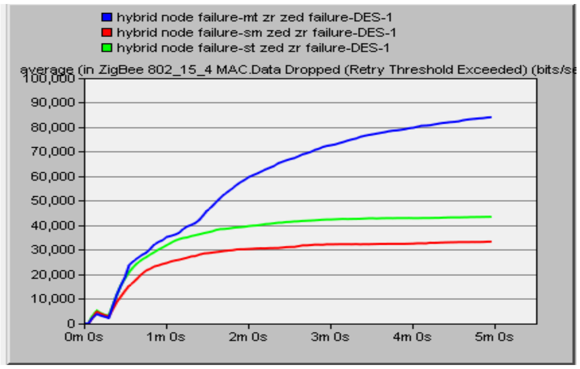

Figure5. Data dropped in MT, SM and ST Topologies in Case of ZED and ZR Failure

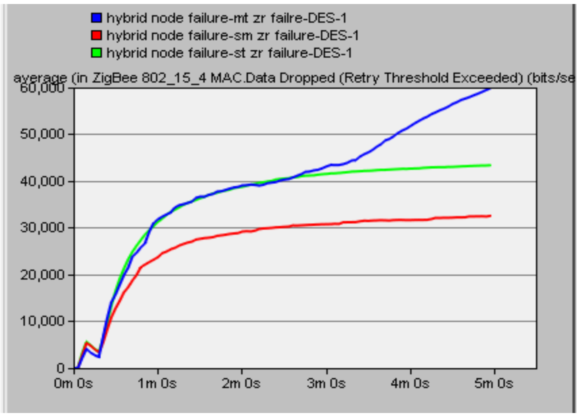

Figure6. Data Dropped in MT, SM and ST Topologies in Case of ZR Failure

C. *Delay*

This statistic records the medium access delay experienced by the packets submitted for transmission on all interfaces in the network. This value is computed as the interval from the time the packet was inserted into the transmission queue until the time when the packet was sent to the physical layer for the first time. In case of ZED failure and ZED, ZR failure maximum delay shown by MT and SM network and minimum by ST network as referred to fig. 7 and 8.

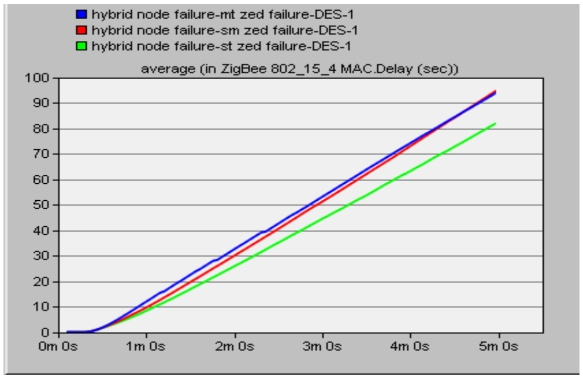

Figure7. Delay in MT, SM and ST Topologies in Case of ZED Failure

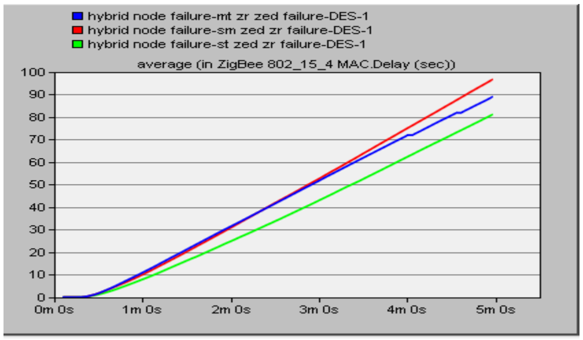

Figure8. Delay in MT, SM and ST Topologies in Case of ZED and ZR Failure

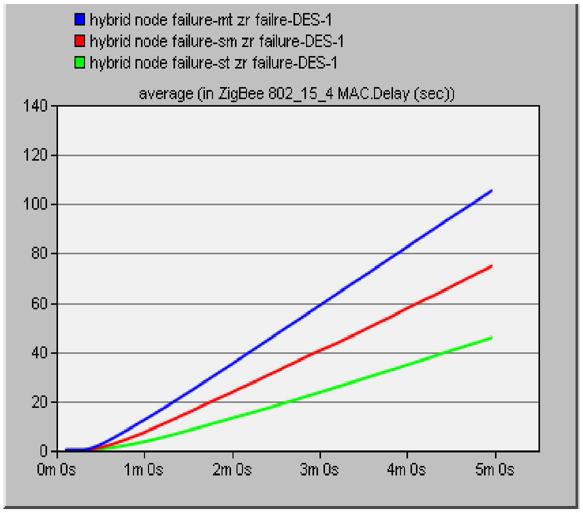

Figure 9. Delay in MT, SM and ST Topologies in Case of ZR Failure

Here the result shown in figure 9 shows that maximum delay achieve by MT network and minimum by ST network in case of ZR failure.

D. Data Traffic Received

These statistics record successfully received data traffic on this network interface from the physical layer. When these statistics are reported in units of bits/second, the physical and the MAC header sizes are included in the computation of the total amount of traffic received. These statistics record all the data received on the network interface regardless of the destination address. The given figure 10, 11 and 12 results conclude that maximum DTR observed in case of SM network and minimum in MT network.

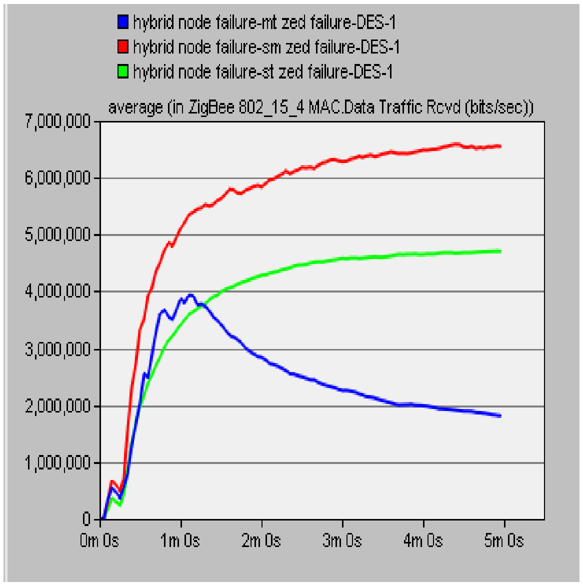

Figure10. DTR in MT, SM and ST Topologies in Case of ZED Failure

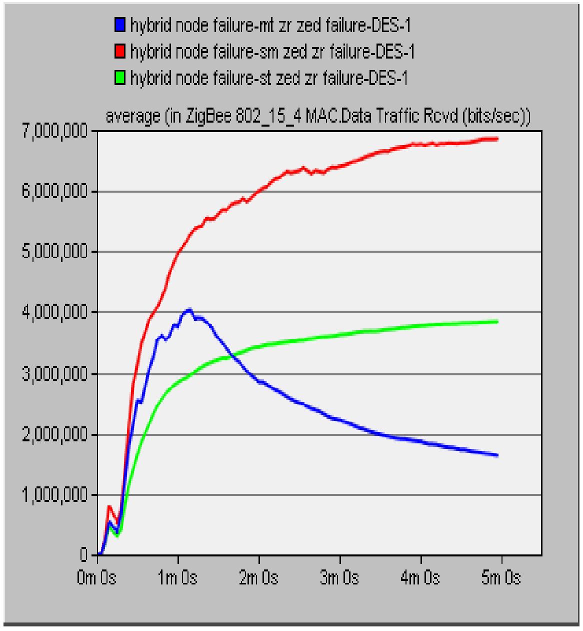

Figure11. DTR in MT, SM and ST Topologies in Case of ZED and ZR Failure

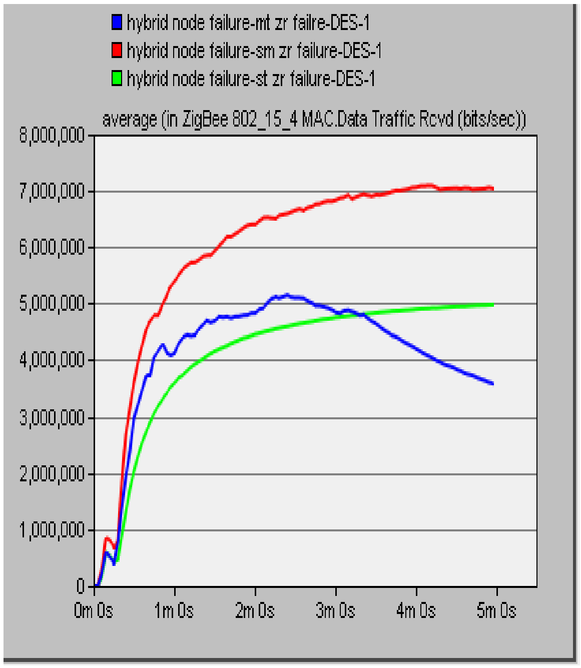

Figure12. DTR in MT, SM and ST Topologies in Case of ZR Failure

E. Data Traffic Sent

These statistics record the amount of data transmitted by the network interface onto the physical layer. When these statistics are reported in units of bits/second, the physical and the MAC header sizes are included in the computation of the total amount of traffic sent.

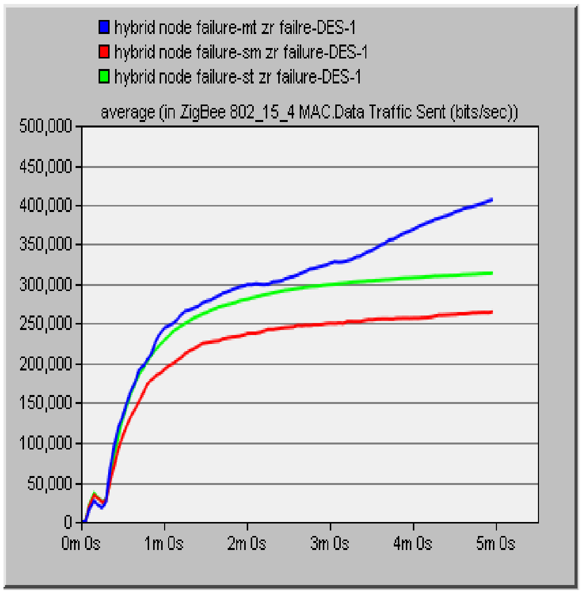

Figure13. DTS in MT, SM and ST Topologies in Case of ZR Failure

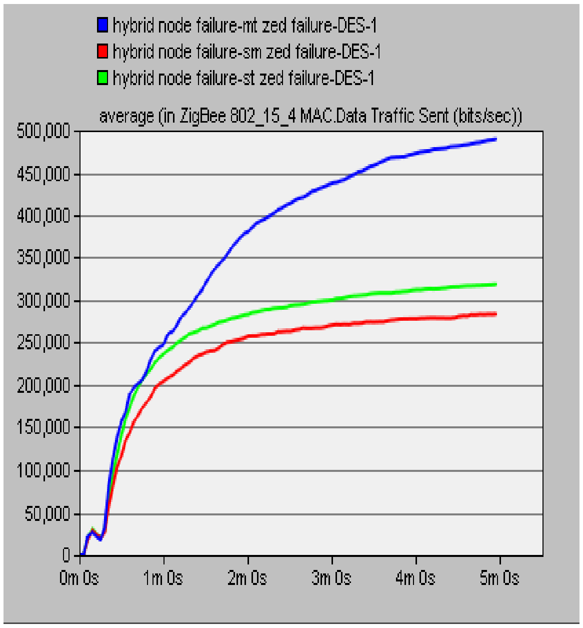

Figure14. DTS in MT, SM and ST Topologies in Case of ZED Failure

The maximum DTS observed by MT network And minimum by SM network as referred to fig. 13, 14 and 15. According to these results MT send maximum data but receive minimum so it lost of data during communication, whereas SM sent minimum data and receive maximum that means it include duplicate packets during transmission and in case of ST average transmission and reception of data occurred which concludes that it loss minimum data packets and also the duplicate packet transmission is less.

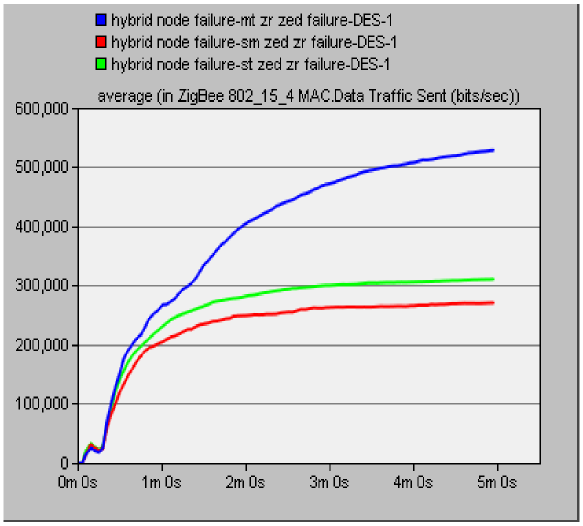

Figure15. DTS in MT, SM and ST Topologies in Case of ZED and ZR Failure

V. CONCLUSION

The overall results conclude that maximum throughput achieved by ST network and minimum by MT network But throughput of ST and MT network degrades when ZED and ZR fail at same time instant, whereas SM network mostly affected by the failure of ZR. In case of DTS and DTR, the maximum DTS observed by MT network but receive minimum and minimum DTS observed by SM network and receive maximum. In case of ST average transmission and reception of data occurred which concludes that it loss minimum data packets. Due to failure of devices maximum delay achieve by MT network and minimum by ST network in case of ZR failure. According to these results ST hybrid network gives better performance than other topologies in case of node failure.

REFERENCES

1. Marco Gribaudo, Daniele Manini, Alessandro Nordio, “Transient Analysis of IEEE 802.15.4 Sensor Networks”,IEEE Transaction On Wireless Communications, VOL.10, NO. 4, APRIL 2011.
2. Zavosh Abdollahzadeh Davani, Azizah Abdu Manaf, “A Survey on Key Management of ZigBee Network”, The International Conference on E-Technologies and Business on the Web (EBW2013).
3. Rozeha A. Rashid , Hamdan Sayuti, Nurul Mu'azzah Abdul Latiff, Norsheila Fisal, Mohd Adib Sarijari, Abdul Hadi Fikri Abdul Hamid, Rozaini Abd Rahim, “Simple Scheduling Scheme for Smart Home and Ambient Assisted Living”, The Second International Conference on Informatics Engineering & Information Science (ICIEIS2013) – Malaysia.
4. Shi Longlonga, Qiu Chunlinga, Gao Penga, Jia Zhengsena, “The Research and Simulation of CSMA/CA Mechanism of Zigbee Protocol”, 2012 International Workshop on Information and Electronics Engineering (IWIEE), Procedia Engineering 29 (2012) 3466 – 3471

5. Surender.R, P. Samundiswary, “Performance Analysis of Node Mobility in Beacon and Non-Beacon enabled IEEE 802.15.4 based Wireless Sensor Network”, IJCA (0975 – 8887), Volume 76– No.12, August 2013.
6. J. Pedro Amaro, Fernando J.T.E. Ferreira,RuiCortesão, Jorge Landeck, “Powering Wireless Sensor Networks Nodes for Complex Protocols on Harvested Energy”, CENTERIS 2012 – Conference on ENTERprise Information Systems HCIST 2012 - International Conference on Health and Social Care Information Systems and Technologies, 2012
7. Yuan-Yao Shih, Wei-Ho Chung,Pi-Cheng Hsiu, Ai- Chun Pang, “A Mobility-Aware Node Deployment and Tree Construction Framework for ZigBee Wireless Networks”, IEEE transaction on vehicular technology, vol. 62, no. 6, july 2013.
8. Mumtaj M.Ali Al-Mukthar, Teeb Hussain Hadi, “Modeling the Performance of Zigbee Cluster Tree Wireless Sensor Network in Presence of Failure”, Journal of Advanced Computer Science and Technology Research,Vol.3 No.3, September 2013, 116-126.
9. P. Medagliani, M. Martalò, G. Ferrari, “Clustered Zigbee networks with data fusion: Characterization and performance analysis” Ad Hoc Networks 9 (2011) 1083–1103.
10. B.E. Bilgin, V.C. Gungor, “Performance evaluations of ZigBee in different smart grid environments”, ELSEVIER, Computer Networks 56(2012) 2196–2205.
11. http://en.wikipedia.org/wiki/ZigBee.
12. E. Yüksel, H. R. Nielson, and F. Nielson, "Zigbee-2007 security essentials," in Proc. 13th Nordic Workshop on Secure IT-systems, 2008, pp. 65-82.
13. Zavosh Abdollahzadeh Davani, Azizah Abdul Manaf “A Survey on Key Management of ZigBee Network” The International Conference on E-Technologies and Business on the Web (EBW), (SDIWC).
14. Li-Hsing Yen, Wei-Ting Tsai, “The room shortage problem of tree-based ZigBee/IEEE 802.15.4 wireless networks”, ELSEVIER, Computer Communications 33 (2010) 454–462.
15. Meng-Shiuan Pan, Yu-Chee Tseng “The Orphan Problem in ZigBee-based Wireless Sensor Networks” MSWiM, page 95-98. ACM, (2007).
16. Francesca Cuomo, Emanuele Cipollone, Anna Abbagnale “Performance analysis of IEEE 802.15.4 wireless sensor networks: An insight into the topology formation process” Computer Networks 53 (2009) 3057–3075.