Nat. Volatiles & Essent. Oils, 2021; 8(6): 5723-5735

NVEO
Natural Volatiles & Essential Oils

An 5g Environment Based Clb-Aodv Multicast Routing For The Zigbee On Wireless Sensor Hetrogenous Network

R.SRINIVASAN [1], P.MALATHI [2], ASWIN KUMAR R [3]

[1]Assistant Professor, Department of ECE, Dhanalakshmi Sirinvasan College of Engineering and Technology, Chennai.

[2]Assistant Professor, Department of CSE, Dhanalakshmi Sirinvasan College of Engineering and Technology, Chennai

[3] Student, Department of ECE, Dhanalakshmi Sirinvasan College of Engineering and Technology, Chennai.

ABSTRACT

A communication load balanced dynamic topology management algorithm (CLB-AODV) is proposed to extend the wireless sensor network (WSN) lifetime via managing the participation in communication process among all nodes in the network. The idea is that, each time there is a failure in the network topology; the topology is adjusted only on-demand by choosing the best path according to paths weights between source and destination nodes. Simulation results show that CLB-AODV can prolong the lifetime of the network, increase the number of alive nodes and reduce the average routing load when compared with some of the most powerful recent algorithms the integration of Wireless Sensor Networks (WSN), new generation networks or 5G, TCP / IP (IPv6) protocols with the Internet of Things (IoT) that aims to exchange information, applying security, QoS (Quality of Service) and configuration, these three aspects are the problems in the construction of a network in which confidentiality, integrity, availability, authentication, reconfiguration of topology, improvement, high quality of service, addressing, infrastructure, Network and node construction, for M2M (Machine to Machine) communication or end to end. Because 5G cellular networks, in particular, are attractive technologies to provide Internet connectivity to equipment (UE). Moreover, an additional routing information collecting method is developed to further improve the routing performance.

Index Terms: Energy and Power Efficient Synchronous Sensor Network (Eph ESOS), Routing Algorithm, Energy optimization.

I.INTRODUCTION

A Wireless sensor network can be defined as a network of devices that can communicate the information gathered from a monitored field through wireless links. The data is forwarded through multiple nodes, and with a gateway, the data is connected to other networks like wireless Ethernet. Terrestrial WSNs are capable of communicating base stations efficiently, and consist of hundreds to thousands of wireless

sensor nodes deployed either in unstructured (ad hoc) or structured (Preplanned) manner. In an unstructured mode, the sensor nodes are randomly distributed within the target area that is dropped from a fixed plane. The preplanned or structured mode considers optimal placement, grid placement, and 2D, 3D placement models.

The AODV protocol builds routes between nodes only if they are requested by source nodes. AODV is therefore considered an on-demand algorithm and does not create any extra traffic for communication along links. The routes are maintained as long as they are required by the sources. They also form trees to connect multicast group members. AODV makes use of sequence numbers to ensure route freshness. They are self-starting and loop-free besides scaling to numerous mobile nodes. In AODV, networks are silent until connections are established. Network nodes that need connections broadcast a request for connection. The remaining AODV nodes forward the message and record the node that requested a connection. Thus, they create a series of temporary routes back to the requesting node.

II.RELATED WORK

Octavio J. Salcedo et al,2013.[1] proposed the existing multi-hop effective capacity model from the continuous-time domain into the discrete-time domain. Mathematical formulae including tail probabilities of delay, delay mean and jitter over multi-hop wireless paths were derived. Furthermore, we used these formulae to develop a simple algorithm for predicting end to-end delay based on the sampling method. End-to-end delay performance is an important Quality of Service (QoS) metric in 5G communication systems and wireless sensor networks (WSNs). Recently, a multi-hop effective capacity model was proposed to provide accurate characterization of end-to-end delay performance in wireless multi-hop environments. However, this model was developed in the continuous-time domain, which accounts for a discrepancy in digital/discrete-time systems.

In this work, we extend such a model into the discrete-time domain and derive new mathematical formulae for tail probabilities of delay, delay mean and jitter in multi-hop cases. Furthermore, propose a simple algorithm for end-to-end delay performance prediction based on the sampling method. By using publicly-available real traces from a wireless sensor network, we recreate these field experiments in a simulation platform to validate the algorithm. The results show that the algorithm gives satisfactory prediction**.** In this work, Data move from source to destination in shortest path in dynamic networks compared to static ones. As future work, more investigation on extra factors can be evaluated in the WSN of 5G area

Brayan Steven Reyes Daza et. Al,2015 [2] contributed to provide a simulation-based analysis of the energy efficiency, accuracy and path length of static and dynamic wireless sensor networks for 5G environment. Results are analyzed and discussed to show the difference between these two types of sensor networks. The tasks of WSNs are functionally influenced by the power source constrains. Minimizing power consumption is very important issue in these networks. In this study, the antecedents that integrate new technologies that integrated with the IoT has a good development, next step is to understand the logic of the architectures and finally based on the network traffic model Gauss-Markov

studied the variables as S (Speed), D (address), (length) L, (width) W, (certainty) d_c (uncertainty) due to obtain an error approaching zero in a 4G network that improves for 5G in budget packet delays in Very small times.

Sergio Huertas Martínez et.al,2013[3] Proposed a design for implementing network-based virtual Ethernet switches (NVESs) on top of a physical substrate consisting of a software-defined networking (SDN) network. An NVES has the same capability as a real Ethernet switch. A user makes a request to provision an NVES by specifying the number of ports and the maximum bandwidth for each port. The substrate network considered in this study is an Open Flow network. The entire network is controlled by an Open Flow controller. The controller is responsible for performing admission control, resource allocation, routing, address learning, and spanning tree protocol. QoS (Quality of Service) and configuration, these three aspects are the problems in the construction of a network in which confidentiality, integrity, availability, authentication, reconfiguration of topology, improvement, high quality of service, addressing, infrastructure, Network and node construction, for M2M (Machine to Machine) communication or end to end. Because 5G cellular networks, in particular, are attractive technologies to provide Internet connectivity to equipment (UE).It is intended to shed some light on the possible problems of integration that are imposed by the integration of wireless sensor networks and 5G that are manifested in the difference in traffic characteristics. For the development we studied the antecedents that integrate new technologies that integrated with the IoT has a good development, next step is to understand the logic of the architectures and finally based on the network traffic model Gauss-Markov we studied the variables as S (Speed), D (address), (length) L, (width) W, (certainty) d_c (uncertainty) d_u to obtain an error approaching zero in a 4G network that improves for 5G in budget packet delays in Very small times The possibility of integrating WSN with IoT through the use of LTE / 5G capabilities.

M. T. Kurniawan et.al,2017[4] In this paper, The ZigBee network is widely studied and deployed recently because of its low cost and simplicity features. However, the power consumption issue needs a further improvement since the application requirements are not fully satisfied. The emerging 5G communication technology is characterized by the smarter devices and the native support for the M2M communication.

On that basis, the 5G terminals are capable of joining the existing ZigBee networks and have the potential to improve the data transmission. In this paper, we investigate the performance of the ZigBee networks in the 5G environment for different scenarios. Then a nearest access routing (NAR) algorithm based on the physical depth is proposed for different communication types. To reduce the loads in ZigBee networks, the data flow in the neighborhood of 5G terminals is gathered and transmitted via the IP networks. The simulation results showed that NAR effectively share the communication in ZigBee networks. It leads to better performances with higher packet delivery ratio, less hop counts from ZigBee devices, lower latency, fewer packets sent by ZigBee nodes and zero routing overheads. comparison between static and dynamic WSNs conducted for 5G environment. Results prove that dynamic networks are consumes less energy than static networks. However, static networks more accurate than dynamic networks. There are several methods of detection and mitigation for sinkhole attacks, there are Delphi method and Multipath routing protocol AODV. But there has been no detailed discussion of the security

strategy for both methods. This study discusses the security strategy to achieve a balance between security and usability in WSN applications for both methods.

Jemimah Ebenezer et.al,2015 [5] In this work, Machine-type communication (MTC) is endorsed in the fifth-generation (5G) networks to realize innovative IoT based applications, such as smart city and intelligent manufacturing. MTC devices with sensing and communication capabilities can monitor the surrounding environment and transmit the collected information back to Base Station (BS) for further data analysis. The dense deployment of sensing devices calls for a clustering structure to preprocess the redundant data to avoid traffic overload. Moreover, due to limited battery capacity, the energy cost remains a critical concern in such IoT systems. In this work, proposed an energy-efficient clustering routing algorithm. Considering the non-uniform traffic distribution, we propose an uneven cluster formation scheme for load balancing and energy efficiency. Moreover, we propose a distributed cluster head (CH) rotation mechanism to balance energy consumption within each cluster. To improve energy efficiency and network lifetime, this paper presented an energy-efficient clustering routing algorithm which can be applied in multi-hop largescale IoT network appropriately. The uneven cluster structure in our routing algorithm balanced the different traffic load in different layers to improve the energy efficiency. The CH node is rotating periodically to balance the energy consumption among nodes in a same cluster.

Fang Ju et.al,2014 [6] In this work, WSNs are restricted by storage capacity, energy and computing power. So it is necessary to design effective and energy aware protocol in order to increase the network lifetime. A review on routing protocol in WSNs is carried out which are classified as data centric, hybrid and geo location based depending on the network. Then some of the multipath routing protocols which are widely used in WSNs to improve performance are also checked and compared with the performances of protocols. Routing protocols are discussed based on three categories: Flat based routing, hybrid-routing and geo Location-based routing on the basis of network structure and trying to increase the lifetime of the wireless sensor network. Most of the routing protocols require information of location for sensor nodes in wireless sensor networks to calculate the distance between two nodes on the basis of signal so that energy consumption can be calculated. Single-path routing approach is unable to provide effective data rate transmission in wireless sensor networks due to the limited capacity of a multi-hop path and the dynamics of wireless links.

This problem can be removed by using multipath routing. To evaluate the trustworthiness of a sensor node, multiple points of its nature can be monitored. Each of them aims at finding a specific type of attack. For example, each time node s1 selects node s3 for forwarding its data it enters the promiscuous in order to check whether node s3 successfully forwarded it. After a number of comparing the successfully sent packets to the number of packet s1 sent to s3, the source node (node s1) can assess the sincere running of the routing protocol while a failure reveals a selfish and/or malicious node acting as a black hole. Similarly, measuring the packets correctly sent without being modified, nodes issuing modification attacks can be detected.

Setiadi Yazid et.al,2013 [7] Energy consumption is one of the constraints in wireless sensor networks (WSNs). The routing protocols are the hot areas to address quality-of-service (QoS) related issues, viz.,

energy consumption, network lifetime, network scalability, and packet overhead. In WSN, there are several routing protocols, which are used to enhance the performance of the network. Out of those protocols, dynamic source routing (DSR) protocol is more suitable in terms of small energy density, but sometimes when the mode of a node changes from active to sleep, the efficiency decreases as the data packets need to wait at the initial point, where the packet has been sent and this increases the waiting time and end-to-end delay of the packets, which leads to increase in energy consumption.

Our problem is to identify the dead nodes and to choose another suitable path so that the data transmission becomes smoother and less energy gets conserved. In order to resolve these issues, we propose directional transmission-based energy aware routing protocol named PDORP. The proposed protocol PDORP has the characteristics of both power efficient gathering sensor information system and DSR routing protocols. In addition, hybridization of genetic algorithm and bacterial foraging optimization is applied to proposed routing protocol to identify energy efficient optimal paths. The performance analysis, comparison through a hybridization approach of the proposed routing protocol, gives better result comprising less bit error rate, less delay, less energy consumption, and better throughput, which leads to better QoS and prolong the lifetime of the network. Moreover, the computation model is adopted to evaluate and compare the performance of the both routing protocols using soft computing techniques. should address application security issues such as reliability, authentication, confidentiality etc.

III. AODV ROUTING PROTOCOL

The AODV routing protocol is designed for the ad hoc networks, it has a trustworthy performance in various environments. The on demand routing discovery may bring the global shortest path in any time, but the routing overheads and the bandwidth occupation caused by the flooding are the disadvantages. A feasibility analysis of the ZigBee protocol for the wireless dynamic sensor networks (WDSN) applications feasibility of adopting ZigBee in the WDSN is proved and the advantages and limitations are well discussed. It is shown that as the node mobility increases, the Z-AODV routing plays a more and more important role in the data transmission design a multiple feedback policy by processing key messages during route discovery for the AODV routing protocol in the ZigBee specification. Instead of reducing the routing overhead, this work tends to increase the flexibility in the Z-AODV routing. Different from the original algorithm in which the link is decided by the destination node, the sending device would choose the best link based on the multiple replies from each potential path

IV. ZIGBEE NETWORKS

Zigbee wireless technology is specially designed for sensors and control devices that employ low cost connectivity and widely used for several applications. Zigbee is an IEEE 802.15.4-based specification for a suite of high-level communication protocols used to create personal area networks with small, low-power digital radios, such as for home automation, medical device data collection, and other low-power low-bandwidth needs, designed for small scale projects which need wireless connection. Hence, Zigbee is a low power, low data rate, and close proximity (i.e., personal area) wireless ad hoc network.

The technology defined by the Zigbee specification is intended to be simpler and less expensive than other wireless personal area networks (WPANs), such as Bluetooth or more general wireless networking such as Wi-Fi. Applications include wireless light switches, home energy monitors, traffic

management systems, and other consumer and industrial equipment that requires short-range low-rate wireless data transfer.

Its low power consumption limits transmission distances to 10–100 meters line-of-sight, depending on power output and environmental characteristics. Zigbee is typically used in low data rate applications that require long battery life and secure networking (Zigbee networks are secured by 128 bit symmetric encryption keys.) Zigbee has a defined rate of 250 kbit/s, best suited for intermittent data transmissions from a sensor or input device.

V.WIRELESS SENSOR NODE APPLICATION

These networks are used in environmental tracking, such as forest detection, animal tracking, flood detection, forecasting and weather prediction, and also in commercial applications like seismic activities prediction and monitoring. Military applications, such as tracking and environment monitoring surveillance applications use these networks. The sensor nodes from sensor networks are dropped to the field of interest and are remotely controlled by a user. Enemy tracking, security detections are also performed by using these networks.

Health applications, such as Tracking and monitoring of patients and doctors use these networks. The most frequently used wireless sensor networks applications in the field of Transport systems such as monitoring of traffic, dynamic routing management and monitoring of parking lots, etc., use these networks.

Rapid emergency response, industrial process monitoring, automated building climate control, ecosystem and habitat monitoring, civil structural health monitoring, etc., use these networks. This is all about the wireless sensors networks and their applications. We believe that the information about all the different types of networks will help you to know them better for your practical requirements. Apart from this, for additional information about wireless SCADA, queries, and doubts regarding this topic or electrical and electronic projects, and for any suggestions, please comment or write to us in the comment section below. Dense Node Deployment. Sensor nodes are usually densely deployed in a field of interest. The number of sensor nodes in a sensor network can be several orders of magnitude higher than that in a MANET.

Battery - Powered Sensor Nodes. Sensor nodes are usually powered by battery. In most situations, they are deployed in a harsh or hostile environment, where it is very difficult or even impossible to change or recharge the batteries. Severe Energy, Computation, and Storage Constraints. Sensor nodes are highly limited in energy, computation, and storage capacities. Self - Configurable. Sensor nodes are usually randomly deployed without careful planning and engineering. Once deployed, sensor nodes have to autonomously configure themselves into a communication network. Application Specific. Sensor networks are application specific. A network is usually designed and deployed for a specific application. The design requirements of a network change with its application.

Unreliable Sensor Nodes. Sensor nodes are usually deployed in harsh or hostile environments and operate without attendance. They are prone to physical damages or failures. Frequent Topology Change. Network topology changes frequently due to node failure, damage, addition, energy depletion, or channel

fading. No Global Identification. Due to the large number of sensor nodes, it is usually not possible to build a global addressing scheme for a sensor network because it would introduce a high overhead for the identification maintenance. Many - to - One Traffic Pattern. In most sensor network applications, the data sensed by sensor nodes flow from multiple source sensor nodes to a particular sink, exhibiting a many - to - one traffic pattern.

In most sensor network applications, sensor nodes are densely deployed in a region of interest and collaborate to accomplish a common sensing task. Thus, the data sensed by multiple sensor nodes typically have a certain level of correlation or redundancy.

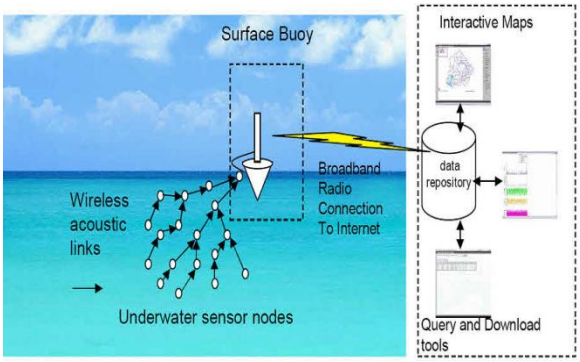


Fig 1.1 : Multimedia WSNs

A. SECURITY

Infrastructure-less architecture (i.e. no gateways are included, etc.) and inherent requirements (i.e. unattended working environment, etc.) of WSNs might pose several weak points that attract adversaries. Therefore, security is a big concern when WSNs are deployed for special applications such as military and healthcare. Owing to their unique characteristics, traditional security methods of computer networks would be useless (or less effective) for WSNs. Hence, lack of security mechanisms would cause intrusions towards those networks. These intrusions need to be detected and mitigation methods should be applied. More interested readers would refer to Butun et al.'s paper regarding intrusion detection systems devised for WSNs.

B. SECURE DATA AGGREGATION

This is a form of in-network processing where sensor nodes are assumed to be unsecured with limited available energy, while the base station is assumed to be secure with unlimited available energy. Aggregation complicates the already existing security challenges for wireless sensor networks and requires new security techniques tailored specifically for this scenario. Providing security to aggregate data in wireless sensor networks is known as secure data aggregation in WSN. were the first few works discussing techniques for secure data aggregation in wireless sensor networks.

C. SIMULATION TOOL

NS2(Network Simulator 2) is an open-source event-driven simulator designed specifically for research in computer communication networks. NS2 has continuously gained tremendous interest from industry, academia, and government. Having been under constant investigation and enhancement for years, NS2 now contains modules for numerous network components such as routing, transport layer protocol, application, etc. To investigate network performance, researchers can simply use an easy-to-use scripting language to configure a network, and observe results generated by NS2. Undoubtedly, NS2 has become the most widely used open source network simulator, and one of the most widely used network simulators.

On the other hand, a large part of network research involves slightly varying parameters or configurations, or quickly exploring a number of scenarios. In these cases, iteration time (change the model and re-run) is more important. Since configuration runs once (at the beginning of the simulation), run-time of this part of the task is less important. Ns meets both of these needs with two languages, C++ and OTcl. C++ is fast to run but slower to change, making it suitable for detailed protocol implementation. OTcl runs much slower but can be changed very quickly (and interactively), making it ideal for simulation configuration. NS(via tclcl) provides glue to make objects and variables appear on both languages.

NS (from **network simulator**) is a name for series of discrete event network simulators, specifically **ns-1**, **ns-2** and **ns-3**. All of them are discrete-event network simulator, primarily used in research and teaching. NS-3 is free software, publicly available under the GNU GPLv2 license for research, development, and use. NS (version 2) is an object-oriented, discrete event driven network simulator developed at UC Berkely written in C++ and OTcl. NS is primarily useful for simulating local and wide area networks. Although NS is fairly easy to use once you get to know the simulator, it is quite difficult for a first time user, because there are few user-friendly manuals. Even though there is a lot of documentation written by the developers which has in depth explanation of the simulator, it is written with the depth of a skilled NS user. The purpose of this project is to give a new user some basic idea of how the simulator works, how to setup simulation networks, where to look for further information about network components in simulator codes, how to create new network components, etc., mainly by giving simple examples and brief explanations based on our experiences. Although all the usage of the simulator or possible network simulation setups may not be covered in this project, the project should help a new user to get started quickly.

The goal of the ns-3 project is to create an open simulation environment for networking research that will be preferred inside the research community:

- It should be aligned with the simulation needs of modern networking research.
- It should encourage community contribution, peer review, and validation of the software.

Since the process of creation of a network simulator that contains a sufficient number of high-quality validated, tested and actively maintained models requires a lot of work, ns-3 project spreads this workload over a large community of users and developers. The core of ns-2 is also written in C++, but the C++ simulation objects are linked to shadow objects in OT cl and variables can be linked between both language realms. Simulation scripts are written in the OT cl language, an extension of the Tcl scripting

language. Presently, ns-2 consists of over 300,000 lines of source code, and there is probably a comparable amount of contributed code that is not integrated directly into the main distribution (many forks of ns-2 exist, both maintained and unmaintained). It runs on GNU/Linux, FreeBSD, Solaris, Mac OS X and Windows 95/98/NT/2000/XP. It is licensed for use under version 2 of the GNU General Public License.

VI.RESULT AND DISCUSSION

1. **NAM (NETWORK ANIMATOR)**

NAM provides a visual interpretation of the network topology created. The application was developed as part of the VINT project. Its feature is as follows.

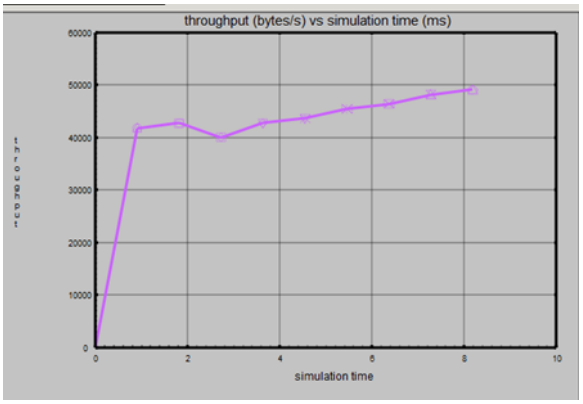
- Provides a visual interpretation of the network created
- Can be executed directly from a Tcl script
- Controls include play; stop fast forward, rewind, pause, a display speed controller button and a packet monitor facility.
- Presented information such as throughput, number packets on each link.

2. X GRAPH

X- Graph is an X-Window application that includes**:**

Interactive plotting and graphing Animated and derivatives To use Graph in NS-2 the executable can be called within a TCL script. This will then load a graph displaying the information visually displaying the information of the file produced from the simulation. The output is a graph of size 800 x 400 displaying information on the traffic flow and time.

3. THROUGHPUT

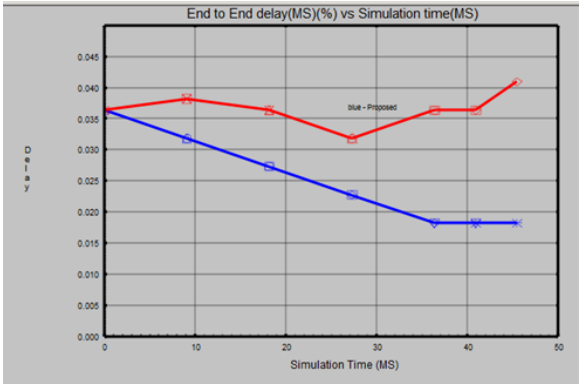


The system throughput or aggregate throughput is the sum of the data rates that are delivered to all terminals in a network.[1] Throughput is essentially synonymous to digital bandwidth consumption; it can be analyzed mathematically by applying the queueing theory, where the load in packets per time unit is

denoted as the arrival rate (λ), and the throughput, where the drop in packets per time unit, is denoted as the departure rate (μ).

The throughput of a communication system may be affected by various factors, including the limitations of underlying analog physical medium, available processing power of the system components, and end-user behavior. When various protocol overheads are taken into account, useful rate of the transferred data can be significantly lower than the maximum achievable throughput; the useful part is usually referred to as goodput.

4. DELAY VS SIMULATION TIME



In a network based on packet switching, transmission delay (or store-and-forward delay, also known as packetization delay) is the amount of time required to push all the packet's bits into the wire. In other words, this is the delay caused by the data-rate of the link. Transmission delay is a function of the packet's length and has nothing to do with the distance between the two nodes. This delay is proportional to the packet's length in bits,

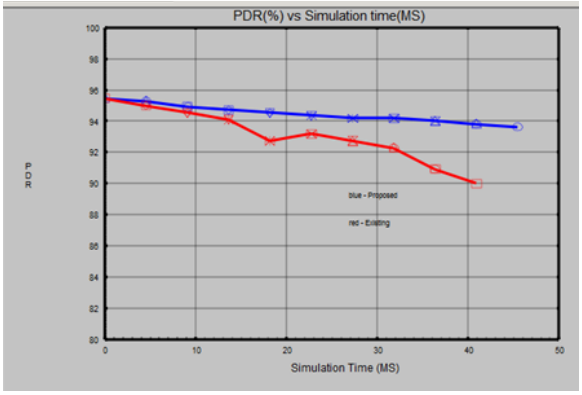
It is given by the following formula:

D_T=N/R Seconds

where

D_T is the transmission delay in seconds
N is the number of bits, and
R is the rate of transmission (say in bits per second)

Most packet switched networks use store-and-forward transmission at the input of the link. A switch using store-and-forward transmission will receive (save) the entire packet to the buffer and check it for CRC errors or other problems before sending the first bit of the packet into the outbound link. Thus, store-and-forward packet switches introduce a store-and-forward delay at the input to each link along the packet's route.



5. PDR VS SIMULATION TIME

In some networks, routing is complicated by the fact that no single entity is responsible for selecting paths; instead, multiple entities are involved in selecting paths or even parts of a single path. Complications or inefficiency can result if these entities choose paths to optimize their own objectives, which may conflict with the objectives of other participants.

A classic example involves traffic in a road system, in which each driver picks a path that minimizes their travel time. With such routing, the equilibrium routes can be longer than optimal for all drivers. In particular, Braess' paradox shows that adding a new road can lengthen travel times for all drivers.

In another model, for example, used for routing automated guided vehicles (AGVs) on a terminal, reservations are made for each vehicle to prevent simultaneous use of the same part of an infrastructure. This approach is also referred to as context-aware routing.[6]

The Internet is partitioned into autonomous systems (ASs) such as internet service providers (ISPs), each of which controls routes involving its network, at multiple levels. First, AS-level paths are selected via the BGP protocol, which produces a sequence of ASs through which packets flow. Each AS may have multiple paths, offered by neighboring ASs, from which to choose. Its decision often involves business relationships with these neighboring ASs,[7] which may be unrelated to path quality or latency. Second, once an AS-level path has been selected, there are often multiple corresponding router-level paths, in part because two ISPs may be connected in multiple locations. In choosing the single router-level path, it is common practice for each ISP to employ hot-potato routing: sending traffic along the path that minimizes the distance through the ISP's own network—even if that path lengthens the total distance to the destination.

VII.CONCLUSION

The simulations show that ZAG achieves better performances with higher packet delivery ratio, less hop counts from ZigBee devices and lower end-to-end delay. Moreover, its overheads are reduced as well, each ZigBee device sends less packet and the normalized routing overheads are also decreased. the on demand routing improvement for ZigBee networks in 5G environments in WSN. The core idea of our work is to utilize the communication and storage resources on 5G nodes as much as possible to share the loads in ZigBee devices. Thus a ZigBee AODV routing method using associated gateways is proposed. At first, we improve the flooding mechanism in the routing discovery by the RREQ teleporting. Afterwards, we make

the source node determine the optimum path To make our algorithm compatible with the ZigBee specification, the optimum ZigBee path and a routing validation command is designed and introduced. Finally, Besides, the effect of 5G nodes mobility is also investigated. The results indicate that SAR is less sensitive to the mobility because of the AGs share the routing information and the additional routing mining mechanism. The improvements both on the network performances and overheads imply that the 5G devices effectively share the communication in ZigBee networks by ZAG. The hop counts as the only metric considered in path costs in this paper. We plan to extend the metric to the residual energy, network congestion and other parameters which need to be paid attention to in the real world. In network layer so many attacks but introduce only collaborative black hole attack a group of black hole node easily employed against routing in mobile ad-hock networks called collaborative black hole attack. In this paper we introduce trusted AODV routing protocol which trust value calculate using tangent hyperbolic function. The result shows performance improvement as compared to standard AODV protocol.

REFERENCES

[1] E. Kalantari, M. Z. Shakir, H. Yanikomeroglu, and A.Yongacoglu, “Backhaul-aware robust 3d drone placement in 5g+ wireless networks,” IEEE Pimrac. 2018.

[2] B. Hu, G. Ren, T. Ding, T. Shang, W. Chen, and Y. Yang, “Topology control algorithm and dynamic management scheme for mobile fso networks.” IEEE/OSA J. Opt. Commun.Net., vol. 7, no.9, pp. 906-917, Sep. 2018.

3] S. A. W. Shah, T. Khattab, M. Z. Shakir, and M. O. Hasna, “Association of Networked Flying Platforms with Small Cells for Network Centric 5G+

C-RAN.” Submitted to IEEE Pimrc. 2017.

[4] A. A. Farid, and S. Hranilovic, “Outage capacity optimization for freespace optical links with pointing errors.” IEEE /OSA J. Lightw. Technol., vol. 25, no. 7, pp. 1702-1710, Jul. 2017.

[5] M. Tekkalmaz,I Korpeoglu, PSAR: power-source-aware routing in ZigBee networks, Wirel. Netw. 18 (6) (2012) 635–651.

[6] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci, Wireless sensor networks: a survey, Comput. Netw. 38 (4) (2002) 393–422.

[7] Ren Qingchun, Q. Liang, An energy-efficient MAC protocol for wireless sensor networks, IEEE Global Telecommunications Conference 1 (10) (2001) 1567–1576, vol. 3.

[8] Chakeres Ian D., L. Klein-Berndt, Aodvjr, aodv simplified, Acm Sigmobile Mobile Comput. Commun. Rev. 6 (3) (2002) 100–101.

[9] P. Charles E., E.M. Royer, Ad-hoc on-demand distance vector routing, in: The Workshop on Mobile Computing Systems & Applications, 1999, pp. 90–100.

[10] F Cuomo, S Della Luna, U Monaco, F Melodia, Routing in ZigBee: benefits from exploiting the IEEE

802.15.4 association tree, in: IEEE International Conference on Communications, 2017, pp. 3271–3276.

[11] F Boccardi, R.W. Heath, A. Lozano, T.L. Marzetta, Five disruptive technology directions for 5G, IEEE Commun. Mag. 52 (2) (2014) 74–80.

[12] Maria Palattella, et al., Internet of things in the 5G Era: enablers, architecture and business models, IEEE J. Select. Areas Commun. 34 (3) (2016)

[13] J.G. Andrews, S. Buzzi, W. Choi, S.V. Hanly, A.C.K. Soong, J.C. Zhang, What will 5G be? IEEE J. Select. Areas Commun. 32 (6) (2014) 1065–1082 June.

[14] A. Gohil, H. Modi, S.K. Patel, 5G technology of mobile communication: a survey, in: International Conference on Intelligent Systems and Signal Processing, 2013, pp. 288–292.

[15] Oliveira Thiago, De Almeida, E.P. Godoy, ZigBee wireless dynamic sensor networks: feasibility analysis and implementation guide, IEEE Sens. J. 16 (11) (2018).