

IoT based Wireless Sensor Network Improvement Against Jammers Using Ad-Hoc Routing Protocols

<https://doi.org/10.3991/ijim.v17i07.38587>

Shayma Wail Nourildean^(✉), Yousra Abd Mohammed
Communication Engineering Department, University of Technology, Baghdad, Iraq
Shayma.w.nourildean@uotechnology.edu.iq

Abstract—The Internet of Things (IoT) is an interconnected network of electronic objects, machines, and physical items in our environment. Wireless Sensor Network is the key component of Internet of Things. Wi-Fi is used by IoT to link home appliances to the internet so that they may be managed and controlled remotely. Sensors were used in WSN technology to sense and gather data from various smart home components, then send it to a gateway. In this paper, the performance of IoT based WSN had been examined when the Jammers interfered with the normal operation of the network and caused deficiency in network from the delay, throughput and data dropped points of view which they are important parameters to examine the performance of any network. The aim of this paper is to improve the degradation in performance caused by Jammers using three Ad-hoc routing protocols (AODV, GRP and OLSR) in number of different Riverbed Modeler Simulation scenarios for different audio and video applications. The results showed that these routing protocols had a significant role in network performance. AODV had been investigated a better delay and data dropped improvement with acceptable throughput improvement while OLSR had the best throughput among other routing protocols with acceptable improvement in delay and data dropped. According to the research, an intelligent system should be used to decide whether a route is used for applications with a high throughput requirement or low delay and data loss.

Keywords—WSN, IoT, Ad-Hoc, Riverbed, QoS, Jammers

1 Introduction

A rapidly emerging combination of technologies known as the "Internet of Things" enables everyday things to collect, process, and exchange data across networks with digital intelligence. IoT, which links the physical and digital worlds, has the potential to enhance environmental perception and proactive decision-making without human intervention. IoT is an interconnected network of machines, electronic and physical items in our environment [1][2]. Wireless sensor networks (WSNs) and cloud computing have been developed quickly and have a wide range of applications, turning the Internet of Things (IoT) from a theoretical notion into a practical reality [3][4]. Wi-Fi is used by IoT to link home appliances to the internet so that they may be managed and

controlled remotely. Clusters, sensors, and actuators used in WSN technology to sense and gather data from various smart home components, then send it to a gateway [5]. This study consists of number of sensor nodes forming a Wireless sensor Network with each sensor node was represented by ZigBee end device. The data had been collected by these sensors to be sent the data to the controller. ZigBee served for low cost and low power Wireless sensor network. In this study, ZigBee coordinator performed the controller that sent the data to the gateway so that it could be monitored and controlled by the user. A number of jammers (jamming attacks) had interfered with the normal operation of the network which caused the degradation of the network efficiency. This paper's aim is to improve IoT based WSN performance degradation because of the Jammers in number of video and file transfer of data applications. The improvement was done using AD-HOC routing protocols which evaluates the best communication pathways for the network data transmission between nodes of the network using software and routing algorithms in terms of (delay, throughput and data dropped).

2 Literature review

The Two key components of home automation technology are IoT and WSN. In the past few years, a large number of publications and research that used IoT technology for various goals were published. Routing is one of the important challenges in WSN [5]. Three topologies were used to examine the effectiveness of the network by Hazha S. Yahia et al (star, tree, and mesh). This has been accomplished by improving the latency, throughput and packet dropped [6]. Madhupreetha Rajaram. et al. created a MATLAB platform for WSN simulation which could be used with a hardware platform to monitor the safety of the structure of spans, huge structures, and monuments [7]. Mohammed-Alamine El Houssaini et al. propose an approach for detecting predicted jamming attacks by utilizing statistical process control on the packet drop ratio (PDR). It had been concluded that the PDR control chart based helped to detect the jammer assault in real time via a visual graph as the performance had been evaluated [8]. Shayma W. N. et al, assesses the Ad-Hoc Routing protocols' effect in Virtual Area Network using Riverbed Modeler modeled scenarios. The outcomes showed that the performance of WSN had been improved using these ad hoc protocols in terms of delay and throughput [9]. Shayma W. N. et al, determined the throughput and delay QoS parameters to improve the MANET's performance deficiency caused by the interference of jamming attacks. This improvement had been done using Point coordination function (PCF) [10]. Padmapriya T. et al, examined a comparison of these two effective routing protocols (AODV and OLSR) for video streaming applications [11].

3 Basic theoretical concepts

3.1 IoT-WSN

Due to the advancement of IoT technology which enable the communication between billions of items, applications, data and people. Since most IoT devices communicate wirelessly with one another and/or the base station (BS) [12][13]. The WSN serves as a bridge to the Internet of Things. A wireless sensor network is a collection of sensor nodes with a restricted power source and limited computing and transmission capabilities. It is simpler to monitor the challenging environments that are difficult to monitor normally because sensor nodes perceive, analyze, and transmit the observed data to the destination. Routing algorithms can assist to preserve resources and prolong the life of a node by making intelligent decisions based on a realistic lifespan prediction. [14][15].

IoT and WSN are going toward edge technologies. IoT-based Wireless sensor networks include a wide range of considerations, including communication delay, throughput, security, cost and power consumption. Low-cost sensor nodes for transmission, data collection and remote monitoring are being performed with the rapid rise of IoT-based WSNs [16][17].

Due to an IEEE 802.15.4 standard, the maximum WSN-IoT data rate for end nodes is just 250 kbps. In WSN-IoT, the gateway is connected to the main power source. The cloud server receives the sensor data from the IoT device so that the user could manage and control the program using a desktop PC, laptop, or a mobile device from the IoT cloud. Currently, several well-known cloud service providers offer free with restricted sensor data storage in their cloud storage [18] [19].

3.2 Jamming attack

Any network security is severely threatened by jamming. A jammer attack uses radio waves to reduce the signal to noise ratio and obstruct all conversations. To distinguish it from interference, which includes unintentional jamming, the term jamming is employed [20]. A jammer is a device that obstructs data transmission and reception over wireless communications in a network. In order to block authorized wireless communication, the jammer continuously produces RF waves. The usage of MAC protocols for communication is one of many traits shared by jamming assaults. Instead of relying on a single source, this approach makes use of multiple sources. These sources send the scrambled packets to the transmission channels and jam the channels, which results in packet loss and lowers the system's dependability and efficiency [21]. This paper examined the impact on number of jammers to a WSN which reduce the efficiency of the network by affecting the QoS parameters of the network. Jamming attack is shown in Figure 1.

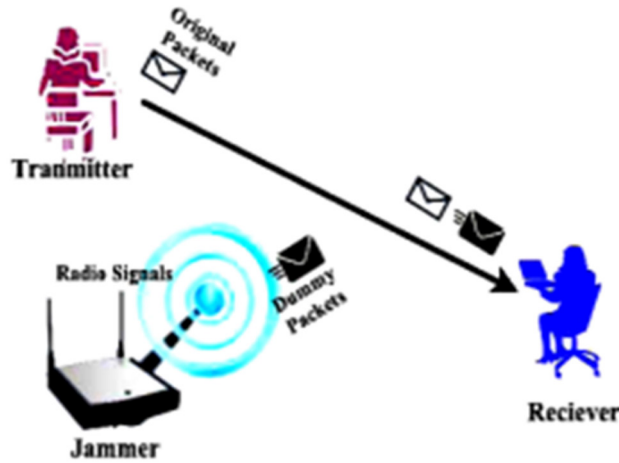


Fig. 1. Jamming Attack [20]

3.3 AD-HOC routing protocols

Evaluates the best communication pathways for the network data transmission between nodes of the network using software and routing algorithms [22]. These protocols can be further divided into reactive (on demand), proactive (table driven), and hybrid approaches [23]. Optimized link state routing protocol (OLSR) [24], DV (distance-vector) [21] and Destination Sequenced Distance Vector (DSDV) [25] protocols are the examples of Proactive protocol. Ad Hoc On-Demand Distance Vector (AODV), Dynamic Source Routing (DSR) [25], and Temporally Ordered Routing Algorithm (TORA) [26] are examples of on-demand routing protocols. ZRP [26] is an example of hybrid routing protocols.

ZigBee and IEEE 802.15.4 are two of the most widely utilized protocols for WSN. Among the numerous advantages of ZigBee technology are its ability to conserve battery power, its ability to handle a large number of nodes in a network, and its ability to communicate over long distances. As a result, expanding the network is simple, and it offers high levels of security for its users [27].

3.4 ZigBee

it is a low in cost and low in power with a 2.4GHz frequency band with 10-100 meters that is frequently used to control and monitor applications. To preserve battery life, Zigbee supports a range of network topologies that support master to slave and master to master communication with a variety of parameters. Zigbee networks can be expanded by connecting to many nodes via routers to create a wider area network [28]. ZigBee topologies were shown in Figure 2.

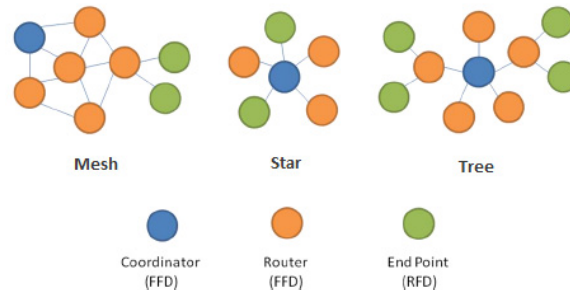


Fig. 2. ZigBee Routing Topologies

The most popular WiFi versions are 802.11n and 802.11g. ZigBee and WiFi share the same frequency spectrum, as well as the power of WiFi is more than the power of ZigBee [29]. A ZigBee device's output power is as low as 0 dBm, while a WLAN standard device's output power is 15 dBm or higher [30].

The ZigBee protocol supports 3 node types: Coordinator, Router and End Device [31][32].

ZigBee Coordinator (ZC): it sets up the network, creates the necessary control algorithms and secures it. ZC is the device that stored network information and responsible of network configuration.

ZigBee Router (ZR): it is used in tree and mesh topologies to enhance the coverage area for wireless communication network.

ZigBee End Device (ZED): They are typically low-power and battery-powered devices. They send their information to the parent (ZC), which might be another router node or the coordinator. The data from the nodes in various locations is sent to a central coordinator through the Internet.

4 Research method

The conventional method of system behavior analysis has proven to be increasingly challenging as communication networks have become more complex. It is vital to assess a system's functionality and performance using a computer simulation before implementing a model or approach in hardware. Wireless sensor network modeling and simulation frameworks are utilized to test and validate the system in a variety of operational environments [33][34]. This study made use of Riverbed (OPNET) Modeler Academic Edition 17.5 because it offers in-depth performance analysis of ZigBee networks in terms of quality service standards. Multiple system models are established in this simulation application to enable communication between end devices, the routers, coordinator and the administrator [32]. The simulation steps were as follows:

- The WSN consists of 20 sensor nodes performed by ZED with number of ZigBee routers with a single coordinator as shown in Figure 3 in the first scenario named (WSN without Jammers).

- The coordinator sent the collected data from the sensors to the gateway to be monitored by the user.
- Wifi acts as a gateway which included three wireless workstations (PCs) and one server.
- Applications and profiles had been configured for a number of video and audio applications, File transfer, Email, HTTP, Mobile Instant messaging applications.
- The application and profile configuration had been assigned to each workstation and server.
- Two Jammers with the transmission power of 0.01 Watt had interfered with the normal operation of the network which caused the efficiency degradation of the network because they increased the delay and packet drop and reduced the throughput and as shown in Figure 4 in the second scenario named (WSN with Jammers).
- Three selected routing protocols (AODV: reactive protocols), (OLSR: Proactive protocols) and (GRP: Hybrid protocols) were applied to improve the network performance in three scenarios named (WSN with Jammers AODV, WSN with Jammers OLSR and WSN with Jammers GRP).

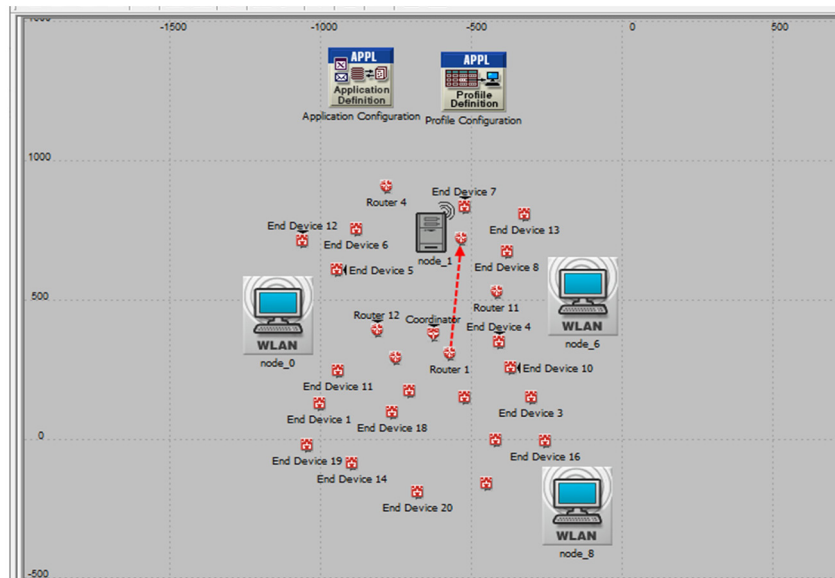


Fig. 3. WSN without Jammers

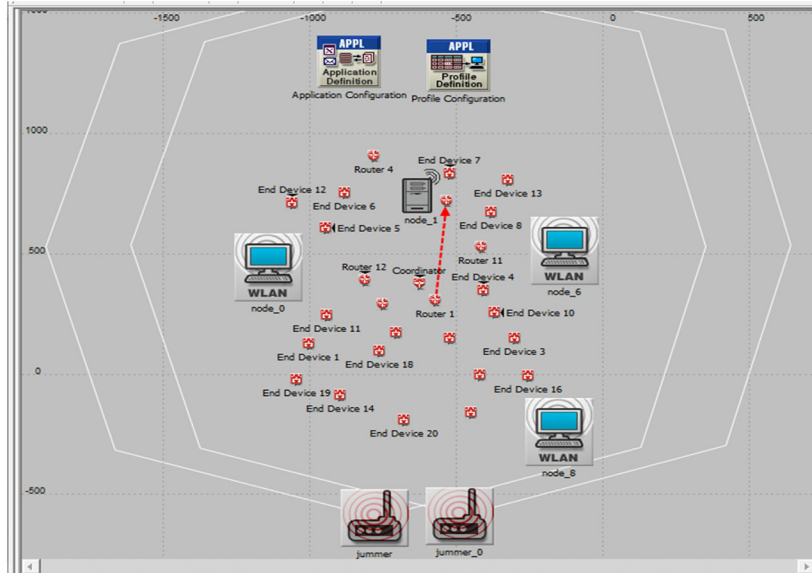


Fig. 4. WSN with Jammers

- Individual statistics had been collected for each scenario to examine the QoS parameters and how it would improve the degradation in network efficiency caused by the Jammers.
- Run the simulation for 1 hour (3600 seconds).

The Network objects had been summarized in Table 1.

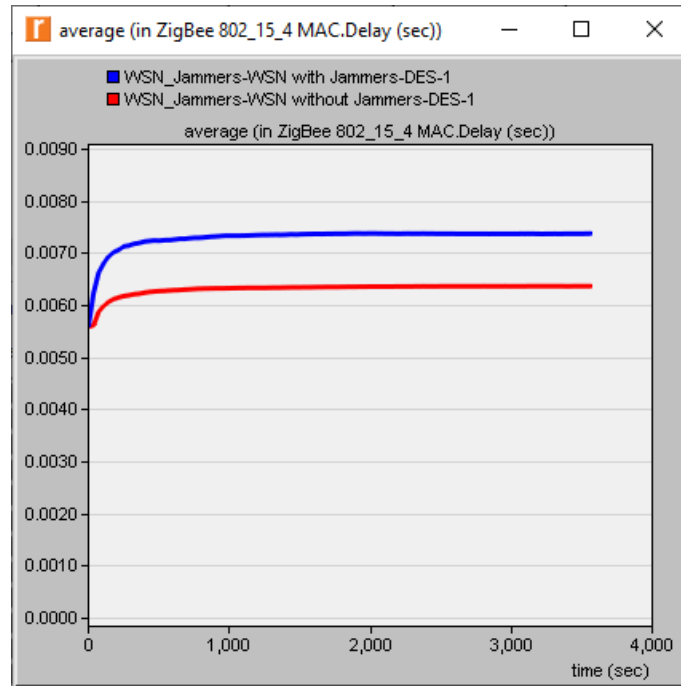
Table 1. IoT based WSN objects

| Parameter | Value |
|----------------------------------|---|
| Sensor Nodes | (1 ZigBee coordinator, 6 ZigBee Routers, 20 ZigBee end devices) |
| Number of wireless clients | Three |
| Number of wireless server | One |
| Data transfer | 24 Mbps |
| Wifi and ZigBeeTransmission Band | 2.4 GHz |
| Transmit Power | 0.03 Watt |
| Repeatability | unlimited |
| Mode of operation | Serial (ordered) |
| Jammers | Two |
| Jammer transmission power | 0.01 Watt |
| Simulation Duration | 3600 sec |
| Applications of the profile | video and audio applications, File transfer, Email, HTTP, Mobile Instant messaging applications |

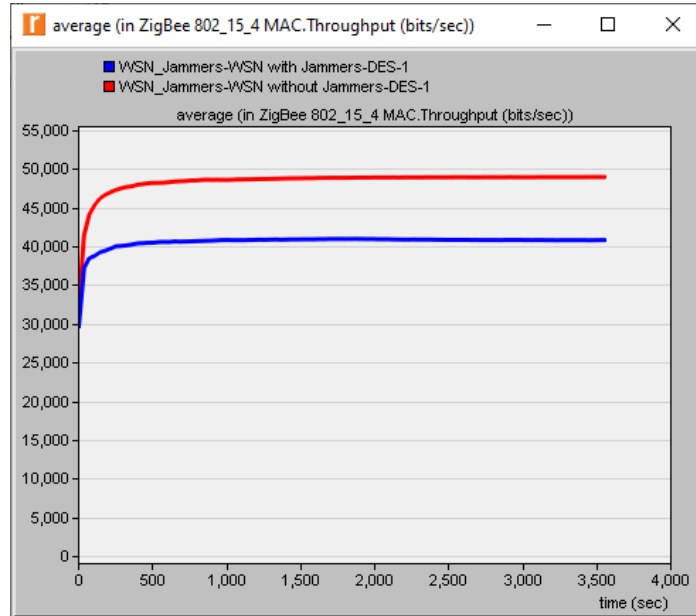
The Results were as follows:

5 Results and discussion

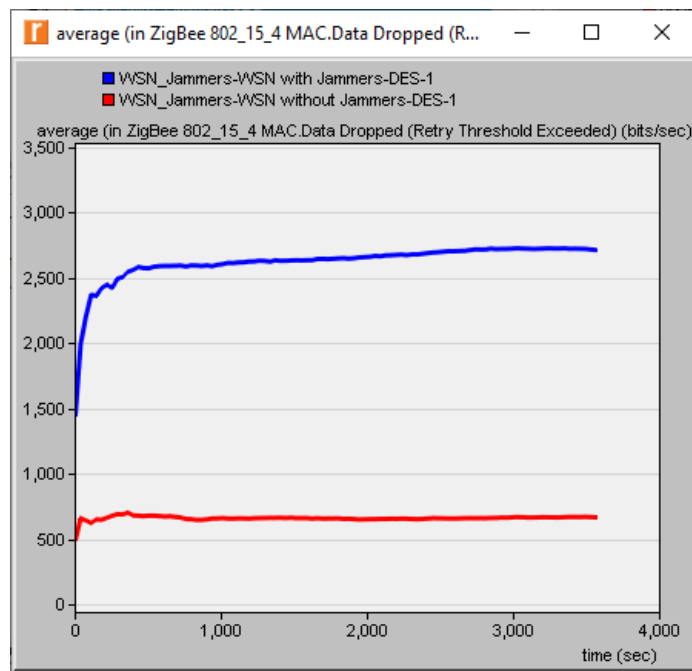
- Delay, throughput and packet dropped had been examined for the WSN with Jammers and without Jammers to study the impact of the jammers on these parameters as shown in Figure 5.



(a) Delay



(b) Throughput

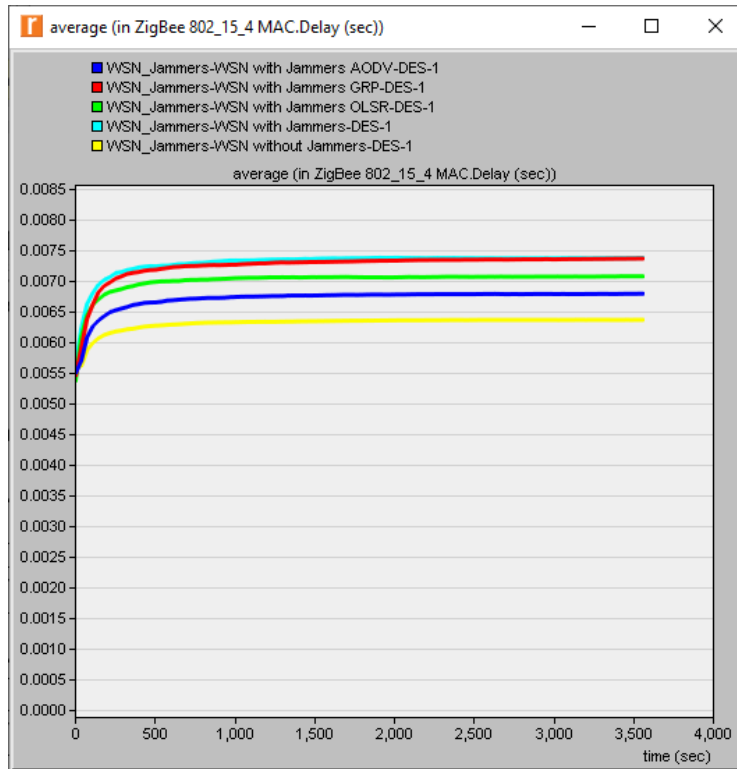


(c) Data Dropped

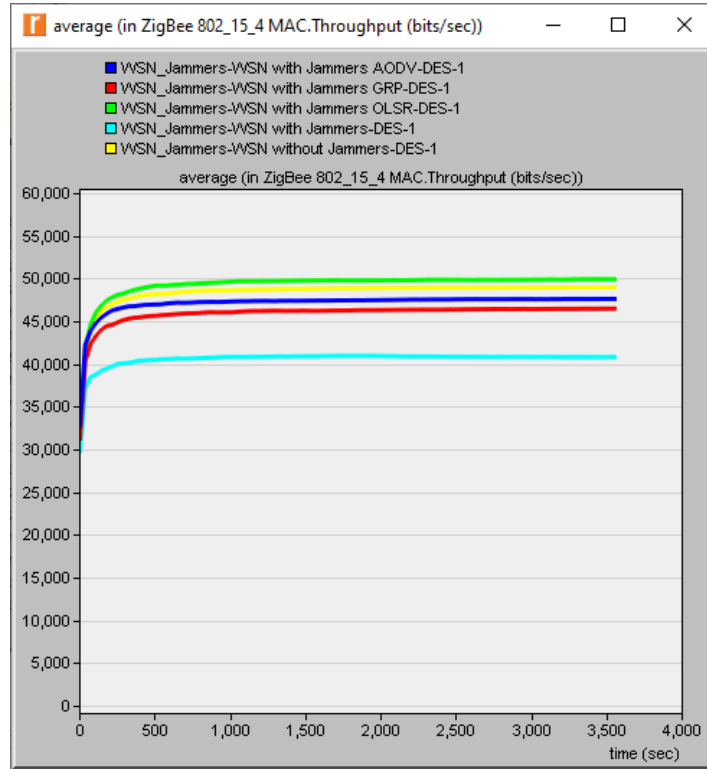
Fig. 5. QoS parameters for WSN with and without Jammers

As shown above, the Jammers degraded the network performance. They reduced throughput and increased the delay and data dropped.

- Delay, throughput and data dropped had been measured for the WSN with Jammers and without Jammers and the utilization of three routing protocols (AODV, OLSR and GRP) as shown in Figure 6.

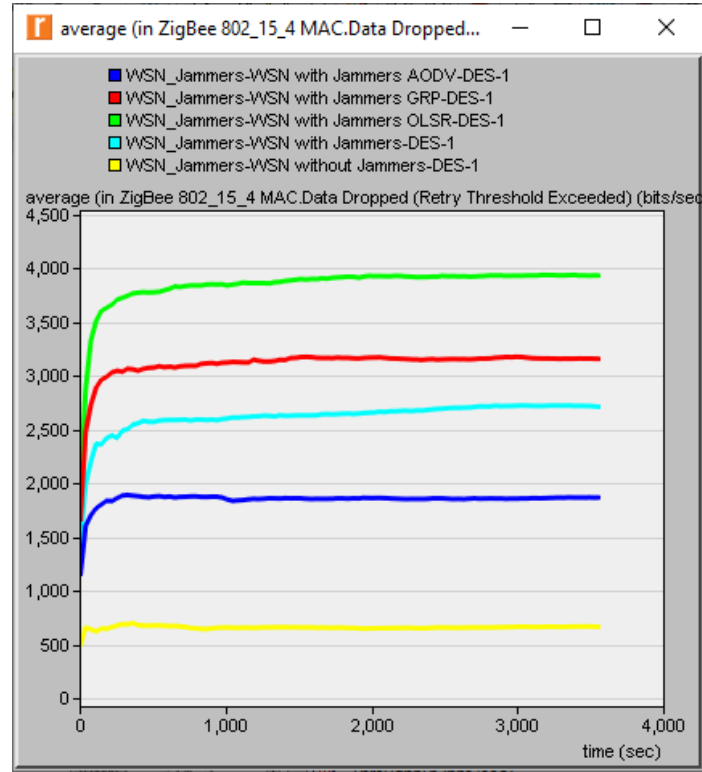


(a) Delay



(b) Throughput

As seen, the performance of WSN had been improved using these Ad Hoc routing protocols. They reduced the delay and data dropped caused by the Jammers and improved the throughput. AODV increased throughput and decreased delay and data dropped. GRP had no effect on the delay improvement but it increased the throughput and. OLSR increased the throughput and decreased the delay but it also increased the data dropped. Table 2 showed the simulation results.



(c) Data Dropped

Fig. 6. QoS parameters for WSN with (AODV, OLSR and GRP) Routing protocols

Table 2. Simulation Results

| Parameter | Network Scenario | WSN without Jammers | WSN with Jammers | WSN with Jammers AODV | WSN with Jammers OLSR | WSN with Jammers GRP |
|-----------|------------------|---------------------|------------------|-----------------------|-----------------------|----------------------|
| | 20 Sensors | Throughput | 49050.50444 | 40916.16 | 47699.90444 | 50015.66444 |
| | Data Dropped | 672.1022222 | 2720.151111 | 1875.764444 | 3942.337778 | 3167.995556 |
| | Delay | 0.006375741 | 0.007385132 | 0.006800377 | 0.007085427 | 0.007375608 |

6 Conclusion

Wireless sensor networks (WSNs) and cloud computing have been developed quickly and have a wide range of applications, turning the Internet of Things (IoT) from a theoretical notion into a practical reality. This study proposed an IoT-based WSN platform in number of different Riverbed’s Modeler simulation scenarios. The modeled platform consisted of number of ZigBee nodes because it is suitable for low cost and

low power wireless sensor network. These sensors sensed the environmental parameters and sent the data to the ZigBee controller. The controller sent the data to the gateway which it is performed by three wireless PC with wireless server so that the user can monitor and control the collected data via the gateway. The aim of this paper was to examine the degradation efficiency caused by the two Jammers with 0.01Watt transmission power. The improvement had been investigated by using three routing protocols which determine the best paths between communication nodes (AODV, OLSR and GRP) for different video and audio applications. The outcomes presented that these routing protocols had a significant role in the throughput, data dropped and delay improvement of this IoT- based WSN. AODV routing protocol achieved the best delay and data dropped improvement since they achieved the least dropping and delay of data among the other routing protocols with acceptable improvement in throughput. If the requirement is throughput improvement, then OLSR had the best throughput among other routing protocols with acceptable improvement in delay and data dropped. GRP had a slightly improvement in delay, throughput and data dropped. The selection of ad hoc routing protocols was crucial in the performance improvement of IoT based WSN.




7 References




- [1] M. L. Zhang, "Intelligent Scheduling for IoT Applications at the Network Edge," 2021.
- [2] A. Elsaadany and M. Soliman, "Experimental Evaluation of Internet of Things in the Educational Environment," *Int. J. Eng. Pedagog.*, vol. 7, no. 3, p. 50, 2017. <https://doi.org/10.3991/ijep.v7i3.7187>
- [3] H. F. Atlam, R. J. Walters, and G. B. Wills, "Intelligence of things: Opportunities challenges," in *3rd Cloudification of the Internet of Things Conference, CIoT 2018*, 2019, pp. 1–6. <https://doi.org/10.1109/CIOT.2018.8627114>
- [4] B. Rahmadya, Zaini, and M. Muharam, "IoT: A mobile application and multi-hop communication in wireless sensor network for water monitoring," *Int. J. Interact. Mob. Technol.*, vol. 14, no. 11, pp. 288–296, 2020. <https://doi.org/10.3991/ijim.v14i11.13681>
- [5] M. Assim and A. Al-Omary, "Design and Implementation of Smart Home using WSN and IoT Technologies," in *2020 International Conference on Innovation and Intelligence for Informatics, Computing and Technologies, 3ICT 2020*, 2020, no. December, pp. 1–7. <https://doi.org/10.1109/3ICT51146.2020.9311966>
- [6] H. Yahia and W. Monnet, "Performance of ZigBee Wireless Body Sensor Networks for ECG Signal Transmission under Maximum Payload Size," *UKH J. Sci. Eng.*, vol. 1, no. 1, pp. 19–25, 2017. <https://doi.org/10.25079/ukhjse.v1n1y2017.pp19-25>
- [7] M. L. Rajaram, E. Kougianos, S. P. Mohanty, and P. Sundaravadivel, "A wireless sensor network simulation framework for structural health monitoring in smart cities," *IEEE Int. Conf. Consum. Electron. - Berlin, ICCE-Berlin*, vol. 2016-Octob, pp. 78–82, 2016. <https://doi.org/10.1109/ICCE-Berlin.2016.7684722>
- [8] M. El Houssaini, A. Aaroud, A. El, and J. Ben-, "Detection of Jamming Attacks in Mobile Ad Hoc Networks using Statistical Process Control," in *Procedia - Procedia Computer Science*, 2016, vol. 83, no. Ant, pp. 26–33. <https://doi.org/10.1016/j.procs.2016.04.095>
- [9] S. W. Nourildean, Y. A. Mohammed, and H. A. Attallah, "Ad Hoc Routing Protocols in a Wireless Network," *Computers*, vol. 12, no. 2, pp. 1–18, 2023. <https://doi.org/10.3390/computers12020028>

- [10] S. W. Nourildean, S. I. Jasim, M. T. Abdulhadi, and M. M. Jaber, "Point coordination mechanism based mobile ad hoc network investigation against jammers," *Eastern-European J. Enterp. Technol.*, vol. 5, no. 9(119), pp. 45–53, 2022. <https://doi.org/10.15587/1729-4061.2022.265779>
- [11] T. Padmapriya and S. V. Manikathan, "Investigation of Video Streaming over MANETS Routing Protocols," *Int. J. Interact. Mob. Technol.*, vol. 16, no. 12, pp. 103–113, 2022. <https://doi.org/10.3991/ijim.v16i12.30805>
- [12] A. Salim, A. I. Id, W. Osamy, and A. M. Khedr, "Compressive sensing based secure data aggregation scheme for IoT based WSN applications," *PLoS One*, no. December, pp. 1–27, 2021. <https://doi.org/10.1371/journal.pone.0260634>
- [13] A. Cardoso and P. Gil, "Teaching and online learning activities in engineering courses using Wireless Sensor and Actuator Networks," *2012 15th Int. Conf. Interact. Collab. Learn. ICL 2012*, pp. 76–80, 2012. <https://doi.org/10.1109/ICL.2012.6402126>
- [14] H. H. El-sayed and H. Al Bayatti, "Improving Network Lifetime in WSN for the application of IoT," *Appl. Math. Inf. Sci.*, vol. 15, no. 4, pp. 453–458, 2021. <https://doi.org/10.18576/amis/150407>
- [15] V. K. V. Saurabh Sharma, "An Integrated Exploration on Internet of Things and Wireless Sensor Networks," *SPRINGER Wirel. Pers. Commun.*, no. Jan, 2022. <https://doi.org/10.1007/s11277-022-09487-3>
- [16] A. Anandhavalli and A. Bhuvaneshwari, "IoT Based Wireless Sensor Networks – A Survey," *Int. J. Comput. Trends Technol.*, vol. 65, no. 1, pp. 21–28, 2018. <https://doi.org/10.14445/22312803/IJCTT-V65P104>
- [17] M. Shafiq *et al.*, "Robust Cluster-Based Routing Protocol for IoT-Assisted Smart Devices in WSN," *Comput. Mater. Contin.*, vol. 67, no. 3, pp. 3505–3521, 2021. <https://doi.org/10.32604/cmc.2021.015533>
- [18] H. Sharma, A. Haque, and F. Blaabjerg, "Machine learning in wireless sensor networks for smart cities: A survey," *Electron.*, vol. 10, no. 9, pp. 1–22, 2021. <https://doi.org/10.3390/electronics10091012>
- [19] P. J. Sousa, R. Tavares, P. Abreu, and M. T. Restivo, "NSensor - Wireless sensor network for environmental monitoring," *Int. J. Interact. Mob. Technol.*, vol. 11, no. 5, pp. 25–36, 2017. <https://doi.org/10.3991/ijim.v11i5.7067>
- [20] J. Singh and S. Gupta, "Impact of Jamming Attack in Performance of Mobile Ad hoc Networks," *Int. J. Comput. Sci. Trends Technol.*, vol. 5, no. 3, pp. 184–190, 2017.
- [21] D. Fernandes and R. K. B, "Survey on jamming attack in manet," *Int. J. Latest Trends Eng. Technol.*, no. SACAIM, pp. 410–414, 2017.
- [22] A. Sharma and D. Kaur, "Behavior of Jamming Attack in OLSR , GRP , TORA and improvement with PCF in TORA using OPNET tool," *Int. Res. J. Eng. Technol.*, vol. 3, no. 3, pp. 191–194, 2016.
- [23] R. Arnous, E. M. T. El-kenawy, and M. Saber, "A Proposed Routing Protocol for Mobile Ad Hoc Networks," *Int. J. Comput. Appl.*, no. June 2020, 2019. <https://doi.org/10.5120/ijca2019919305>
- [24] A. H. Wheeb and N. A. Al-jamali, "Performance Analysis of OLSR Protocol in Mobile Ad Hoc Networks P," *Int. J. Interact. Mob. Technol.*, vol. 16, no. 1, pp. 106–119, 2022. <https://doi.org/10.3991/ijim.v16i01.26663>
- [25] F. T. Al-dhief, N. Sabri, M. S. Salim, S. Fouad, and S. A. Aljunid, "MANET Routing Protocols Evaluation: AODV , DSR and DSDV Perspective," in *MATEC Web of Conferences*, 2018, vol. 150, pp. 1–6. <https://doi.org/10.1051/mateconf/201815006024>

- [26] I. Ahmad, "Performance Assessment of QoS Using AODV, TORA and ZRP Routing Protocol in MANET," *Mehran Univ. Res. J. Eng. Technol.*, vol. 39, no. 4, pp. 744–750, 2020. <https://doi.org/10.22581/muet1982.2004.06>
- [27] A. E. Coboi, V. Nguyen, M. Nguyen, and N. T. Duy, "An Analysis of ZigBee Technologies for Data Routing in," *ICSES Trans. Comput. Networks Commun. (ITCNC)*, vol. X, no. August, pp. 1–10, 2021.
- [28] S. Hindinamani and A. B. Bodas, "Implementation of Zigbee Technology for Patient HealthCare Monitoring System," *Ijarcce*, vol. 6, no. 3, pp. 400–402, 2017. <https://doi.org/10.17148/IJARCCCE.2017.6391>
- [29] S. Jacob and P. Ravi, "Enabling Coexistence of ZigBee and WiFi," *Commun. Appl. Electron.*, vol. 2, no. 6, pp. 28–34, 2015. <https://doi.org/10.5120/cae2015651788>
- [30] S. S. Wagh, A. More, and P. R. Kharote, "Performance Evaluation of IEEE 802.15.4 Protocol under Coexistence of WiFi 802.11b," *Procedia Comput. Sci.*, vol. 57, pp. 745–751, 2015. <https://doi.org/10.1016/j.procs.2015.07.467>
- [31] H. Ghayvat, S. Mukhopadhyay, X. Gui, and N. Suryadevara, "WSN- and IOT-Based Smart Homes and Their Extension to Smart Buildings," *sensors*, vol. 15, pp. 10350–10379, 2015. <https://doi.org/10.3390/s150510350>
- [32] S. Vançın, "Design and Simulation of Wireless Sensor Network Topologies Using the ZigBee Standard," *Int. J. Comput. Networks Appl.*, vol. 2, no. 3, pp. 135–143, 2015.
- [33] R. Sharma, V. Vashisht, and U. Singh, "Modelling and simulation frameworks for wireless sensor networks : a comparative study," *IET Wirel. Sens. Syst.*, vol. 10, no. 5, pp. 181–197, 2020. <https://doi.org/10.1049/iet-wss.2020.0046>
- [34] Y. Khlifi, "Hybrid Authentication Combining Student Behavior and Knowledge for E-Evaluation Transparency and Equity Over E-Learning Platform," *Int. J. Emerg. Technol. Learn.*, vol. 17, no. 21, pp. 17–37, 2022. <https://doi.org/10.3991/ijet.v17i21.32825>

8 Authors

Shayma Wail Nourildean    is a lecturer (a member of an academic staff) in Communication Engineering department in University of Technology (UOT), Baghdad – Iraq. She published a number of papers in national and international journals and participated in multiple national and international conferences (Shayma.w.nourildean@uotechnology.edu.iq).

Yousra Abd Mohammed    is a lecturer at the Communication Engineering Department, Technology University, Baghdad, Iraq since 2005 (yousra.a.mohammed@uotechnology.edu.iq).

Article submitted 2023-01-04. Resubmitted 2023-02-27. Final acceptance 2023-02-27. Final version published as submitted by the authors.