International Journal of Enhanced Research in Science, Technology & Engineering
ISSN: 2319-7463, Vol. 11 Issue 10, October-2022, Impact Factor: 7.957

Modeling and Simulation of Wireless Sensor Network Using OPNET and Effect of Transport Protocols on Simulation

Pravin V. Thakare[1], Amit S. Kakad[2], Manjusha M. Patil[3], Renuka S. Shinde[4], Swati A. Yadgire[5]

[1,4,5]Assistant Professor, Department of Computer Science and Engineering, MGICOET Shegaon, Maharashtra, India
[2]Head of Department, Department of Computer Science and Engineering, MGICOET Shegaon, Maharashtra, India
[3]Senior Training and Placement Officer, G. H. Raisoni Institute of Engineering and Technology, Wagholi, Pune Maharashtra, India

ABSTRACT

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. It is intended for a general application and should be able to collect data from many nodes, every node connected to several sensors. One possible application for such a network is in the medical area. At first the network will be used to display the evolution of blood pressure; the body temperature, the ambient temperature and pressure and the level of the transfusion liquid can be collected as well. The network coordinator will transmit the data to a local server for further processing. The simulation will be used to evaluate the general parameters of the wireless network and to optimize it. In this paper, we aim to evaluate the performance of a ZigBee wireless sensor network using OPNET and also study the effects of TCP and UDP on the performance of the application based on OPNET simulation software.

Keywords- Sensor, wireless sensor network, ZigBee, OPNET, TCP, UDP

INTRODUCTION

Wireless sensor networks can be defined as a self-configured and infrastructure-less wireless networks to monitor physical or environmental conditions, such as temperature, sound, vibration, pressure, motion or pollutants and to cooperatively pass their data through the network to a main location or sink where the data can be observed and analyzed. A sink or base station acts like an interface between users and the network. One can retrieve required information from the network by injecting queries and gathering results from the sink. Typically a wireless sensor network contains hundreds of thousands of sensor nodes. The sensor nodes can communicate among themselves using radio signals. A wireless sensor node is equipped with sensing and computing devices, radio transceivers and power components. The individual nodes in a wireless sensor network (wsn) are inherently resource constrained: they have limited processing speed, storage capacity, and communication bandwidth. After the sensor nodes are deployed, they are responsible for self-organizing an appropriate network infrastructure often with multi-hop communication with them. Then the onboard sensors start collecting information of interest. Wireless sensor devices also respond to queries sent from a "control site" to perform specific instructions or provide sensing samples.

Wireless sensor networks (WSNs) enable new applications and require non-conventional paradigms for protocol design due to several constraints. Owing to the requirement for low device complexity together with low energy consumption (i.e. long network lifetime), a proper balance between communication and signal/data processing capabilities must be found. This motivates a huge effort in research activities, standardization process, and industrial investments on this field since the last decade. At present time, most of the research on WSNs has concentrated on the design of energy and computationally efficient algorithms and protocols, and the application domain has been restricted to simple data-oriented monitoring and reporting applications. A Cable Mode Transition (CMT) algorithm, which determines the minimal number of active sensors to maintain K-coverage of a terrain as well as K-connectivity of the network. Specifically, it allocates periods of inactivity for cable sensors without affecting the coverage and connectivity requirements of the network based only on local information. In delay-aware data collection network structure for wireless sensor networks is proposed. The objective of the proposed network structure is to minimize delays in the data collection processes of wireless sensor networks which extends the lifetime of the network. Relay nodes to mitigate the

network geometric deficiencies and used Particle Swarm Optimization (PSO) based algorithms to locate the optimal sink location with respect to those relay nodes to overcome the lifetime challenge. Energy efficient communication a geometrical solution for locating the optimum sink placement for maximizing the network lifetime. Most of the time, the research on wireless sensor networks have considered homogeneous sensor nodes. But nowadays researchers have focused on heterogeneous sensor networks where the sensor nodes are unlike to each other in terms of their energy. New network architectures with heterogeneous devices and the recent advancement in this technology eliminate the current limitations and expand the spectrum of possible applications for WSNs considerably and all these are changing very rapidly.

A. ZigBee Architecture

Zigbee system structure consists of three different types of devices such as Zigbee coordinator, Router and End device. Every Zigbee network must consist of at least one coordinator which acts as a root and bridge of the network. The coordinator is responsible for handling and storing the information while performing receiving and transmitting data operations. Zigbee routers act as intermediary devices that permit data to pass to and fro through them to other devices. End devices have limited functionality to communicate with the parent nodes such that the battery power is saved as shown in the figure. The number of routers, coordinators and end devices depends on the type of network such as star, tree and mesh networks.

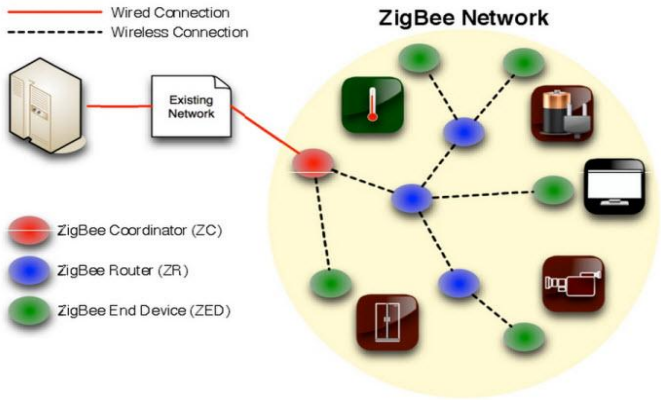

Figure 1*: ZigBee System Structure*

ZigBee is a technology based on a standard (IEEE 802.15.4) that defines a set of communication protocols for small coverage, low data rate wireless networks. The transfer rate can reach a maximum of 250 kbit/s in the case of the 2.4 GHz frequency band. This transfer rate is quite small when compared with the 1 Mbps that Bluetooth can reach or the 54 Mbps that Wi-Fi can reach. The applications where ZigBee can be employed use mainly batteries and some of their main requirements concern small costs and long battery life. In order to maximize battery life in many ZigBee applications transceivers are active only for a short period and for the remaining time they enter a low energy consuming state. Because of this it is possible for ZigBee wireless nodes to be active for up to several years without maintenance and that is why this technology is preferred in many sensor networks.

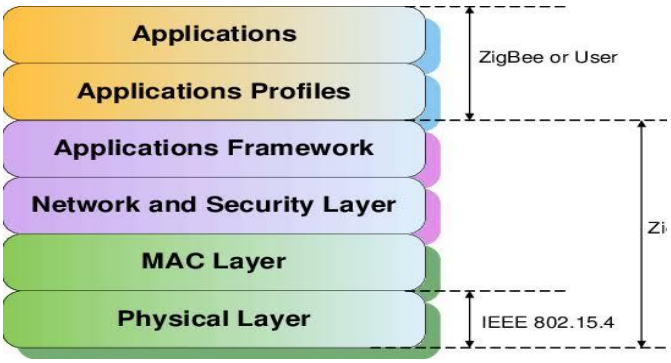

Figure 2: ZigBee Reference Model

The IEEE 802.15.4 standard is a standard developed for Wireless Personal Networks (WPANs). Since the standard only defines the Physical and MAC layers the ZigBee Alliance it defines the Network (NWK) and Application (APL) layers. The IEEE 802.15.4 standard specifies the use of three modulation types: Binary Phase Shift Keying - BPSK, Amplitude Shift Keying – ASK and Offset Quadrature Phase Shift Keying - O-QPSK. For BPSK and O-QPSK the digital data modulates the phase of the signal. For ASK the data modulates the signal amplitude. The same standard

specifies the use of Direct Sequence Spread Spectrum (DSSS) or of Parallel Sequence Spread Spectrum (PSSS).These energy spreading techniques improve the performances of the system in a multipath environment. These specifications make ZigBee a robust and versatile technology.

ZigBee can operate in the following frequency bands:

- 868–868.6 MHz (the 868 MHz frequency band).
- 902–928 MHz (the 915 MHz frequency band).
- 2400–2483.5 MHz (the 2.4 GHz frequency band).

The 868 MHz frequency band is used mainly in Europe for wireless networks with low coverage radius. The 915 MHz and the 2.4 GHz bands are part of the so called industrial, scientific and medical frequency bands (ISM). The 915 MHz band is used mainly in North America while the 2.4 GHz is used worldwide.

B. TCP and UDP

TCP (Transport Control Protocol) and UDP (User Datagram Protocol) are two most important transport protocols in TCP/IP network architecture, which guarantee the transmission of network layer data.TCP is a reliable connection-oriented transport layer protocol. This means that prior to the transmission of data; the two sides should establish a connection to send and receive the data before the completion of the transmission and then disconnect the connection. UDP is a connectionless transport layer protocol, regardless of the state of the other side, you can send data directly. In different network environments, different transport protocols have different effects on application performance, and we can choose different transport protocols according to different requirements.

➢ TCP

TCP is a connection-oriented protocol provides reliable data transmission. TCP packet format is shown in fig

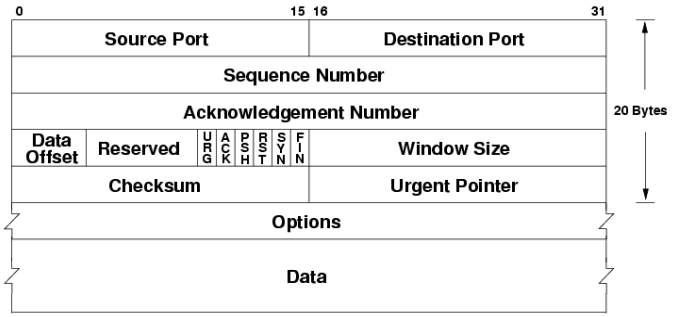

Figure 3: TCP Datagram Format

The term connection-oriented means the two applications using TCP must establish a TCP connection with each other before they can exchange data. While it must follow the principle of Three-way Handshaking to establish a connection and terminate a connection by Four-way Handshaking.

Functions provided by TCP to ensure its reliability are given below:

- The application data is divided into data blocks, called segment, according to the most suitable size for transmission. Since the TCP protocol is byte-oriented and each byte is numbered according to the sequence of byte streams. The first data byte in each segment is called sequence number.
- Upon sending a TCP segment, the sending end starts a timer, and then re-sending the segment if it has not received the confirmation from the receiving end in time.
- Upon receiving a TCP segment, the receiving end replies a confirmation through the so-called acknowledgment number (ACK for abbr.) to the sending end.
- TCP maintains a checksum on its header and data. This is an end-to-end checksum whose purpose is to detect any modification of the data in transit. If a segment arrives with an invalid checksum, TCP discards it without sending the acknowledgment packet.
- TCP provides flow control mechanism. Each end of a TCP connection has a limited buffer space, the receiving end can only allow the sending end to send as much as the receiving end can buffer. To limit the transmission rate of the sending end with the propose to prevent the receiver from being flooded. TCP flow control mechanism is provided by the field of window size at each end of the connection.
- TCP also provides congestion control mechanism. TCP congestion control algorithm can make the sending rate of the sender to adapt the network capacity and prevent network from being flooded.

- **UDP**

UCP packet format is shown in Fig4 and we can see that compared with TCP, UDP is a simple communication protocol and it provides connectionless unreliable transport services.

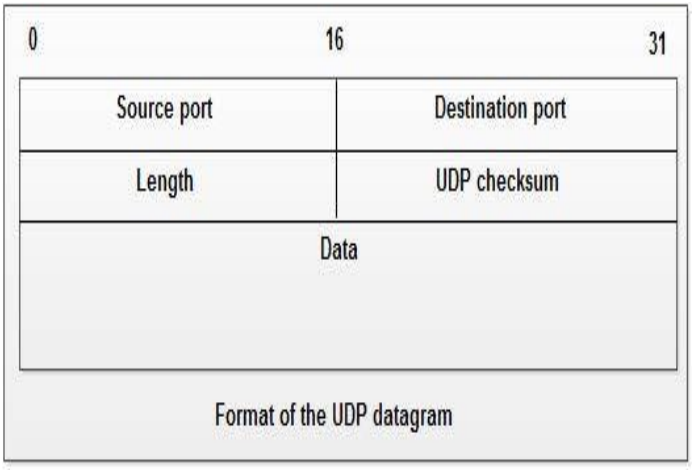

Figure 4: UDP Datagram Format

Between the sending and receiving ends, UDP doesn't provide a point-to-point connection and it can transmit data immediately.UDP is a packet-oriented, and the length of the datagram will remain unchanged. UDP does not provide a guaranteed transmission, flow control mechanism, congestion control mechanism and error control mechanism and other functions but forwards the data of IP layer without ensuring that they reach the destination successfully .UDP is a good choice for applications that can tolerate data errors.

SIMULATION OF WIRELESS SENSOR NETWORK USING OPNET

OPNET is an Optimized Network Engineering Tools used for network simulation and modeling. It is powerful computational software used to model and simulate data networks. The present version can simulate heterogeneous networks that use various communications protocols. OPNET simulates the network at packet-level and was conceived initially to analyze fixed networks. It was later extended to encompass mobile and satellite networks. In order to allow this the software encompasses libraries including the models for the equipments and protocols for many of the best known communication technologies.

The OPNET simulation environment facilitates the simulation of ZigBee based networks by providing several components of a ZigBee network (ZigBee coordinator, ZigBee router, ZigBee end device – these components can be fixed or mobile). The objects are defined according to the standard. The possibilities offered by OPNET for modeling ZigBee wireless networks were studied from different perspectives. Using these components we can build a network that represents a close enough model of a real network and can analyze this network and configure component attributes. After these initial steps are performed (define the network topology, set the attributes, and choose the statistic that should be collected) the simulation can be run. After the simulation process is completed, we can analyze the statistics collected. These statistics can be defined at a global or network level or at a local or node level. The simulation that we developed was aimed to evaluate several network parameters: maximum number of nodes that can be employed using one coordinator, best network structure for data integrity, reliability and costs. In order to achieve these aims three projects were designed. These projects are introduced below.

In fig5, we considered a network consisting of one coordinator and one mobile station. The maximum area covered by one ZigBee station in specific OPNET conditions should be determined. A mobile station was used and a trajectory for this station was defined in order to evaluate the impact of distance on the signal received by the coordinator. The distance at which a signal can be received is influenced by several factors:

- Transmitter power
- Receiver sensitivity
- Antennas gain
- Power loss between transmitter and antenna and between receiver and antenna
- Relative antennas position (distance between the two antennas, obstacles between them, etc.);

Figure 5: Scenario used to determine the impact of distance on received signal level

After running the simulation for this project a coupled statistic concerning received power at the coordinator from the mobile station was collected (fig6). By analyzing this statistic it was possible to conclude that using the free space propagation model with a transmitter power of -3dBm and a sensibility of -85 dBm, the coordinator can receive signals from a station that is at maximum 100 m. The version of OPNET simulation environment uses several propagation models but the one that is closest to propagation on small distances inside is the free space model. This version can not include the effect of obstacles but some experiments shown that the real coverage range is smaller, somewhere around 30 to 40 m [9, 10].

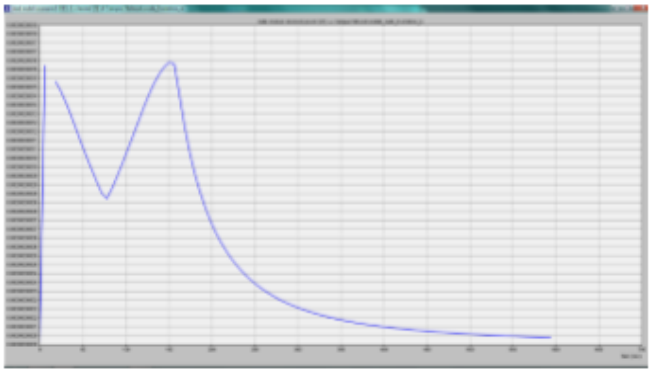

Figure 6: **Signal level as a function of distance**

In fig7(Project 2), the variable is the ZigBee mobile stations number. We simulated a network where the stations (the number of stations was varied between 25 to 225 stations) are located around the coordinator, inside its coverage area (as evaluated d in project 1).

By changing the station number and monitoring network performances it was possible to determine the maximum number of stations that can be used with one network coordinator considering a given performance parameter.

The global statistics monitored were: delay, traffic sent (packets and bps), traffic received (packets and bps) and load. In fig8 a synthetic diagram is given.

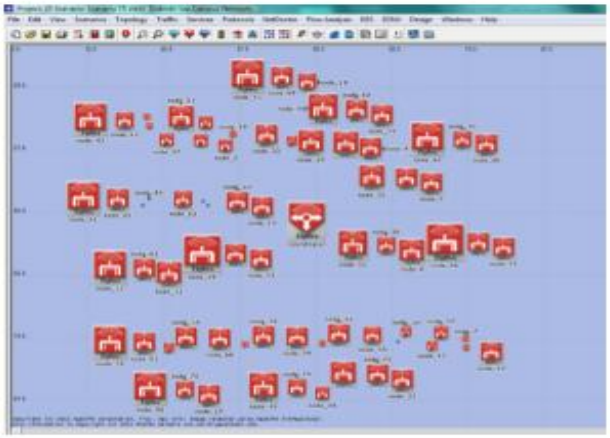

Figure 7: One of the scenarios used to determine network capacity. In this case n=75 where n is the number of stations

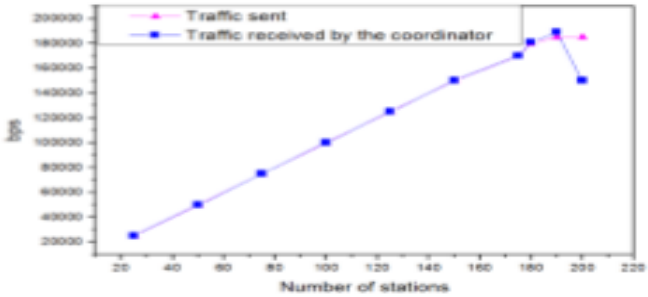

Figure 8: Variation of the sent traffic (network level) and of the traffic received by the coordinator at the application level as a function of the station number

It was possible to remark that without considering interferences and operating without acknowledgements the node number should be limited below 175. This was to be expected knowing that overhead traffic can be around 30 % of total traffic and that the traffic generated by each station is one packet per second (1kbit). Since the security data and acknowledgments will increase the overhead it is recommended to use them only when necessary. When used the number of nodes and the number of measurement stations will be reduced accordingly. If the noise and interference levels increase the number of children should be limited and acknowledgements should be used. In this simulation a relatively large number of children was used (220) – such a number can be implemented only if the network is a star network working without routers.

In fig9 (Project 3) with four scenarios. Project 3 is a study of a network distributed on a volume with 24 supervised areas each containing one to four stations. If some of these areas are outside the area covered by the coordinator routers are added.

In the case of project 3 an L configuration of the supervised area was considered. In order to take into account the presence of walls the power of the transmitters was changed taking into account how many walls there are between the node and the receiver.

Figure 9: One of the scenarios developed for project 3 (n=2)

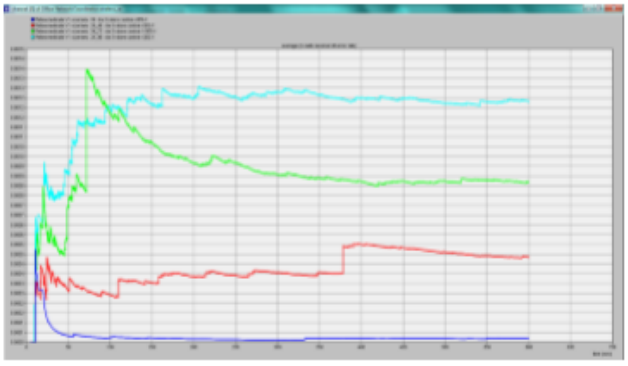

Figure 10: Bit error rate variation as a function of time as a parameter the number of stations in the supervised area vas varied from 1-turquoise to 4-blue

EFFECTS OF TRANSPORT PROTOCOLS ON SIMULATION

Simulation software is to study the effects of TCP and UDP on the performance of FTP under different network environments. The simulation content is the client requests files to the FTP server. The client node sends file download requests to the FTP server periodically in LAN (Local Area Network) and the Internet through different transport protocols and the files are returned to the client after the FTP server received requests.

Following experiment involves four scenes and the application configuration of scenes is shown in TABLE I. The network topology is made up by 1 client node, 2 FTP server nodes, 1 gateway node and 1 IP cloud nodes, as shown in Fig.3. The average download response time of the application and the throughput of the link connecting to the server node are used as the statistics.

Scene	Property	
	Transport protocol	*Data loss*
Scenario 1	TCP	No
Scenario 2	UDP	No
Scenario 3	TCP	Yes
Scenario 4	UDP	Yes

Table1: Application Configuration

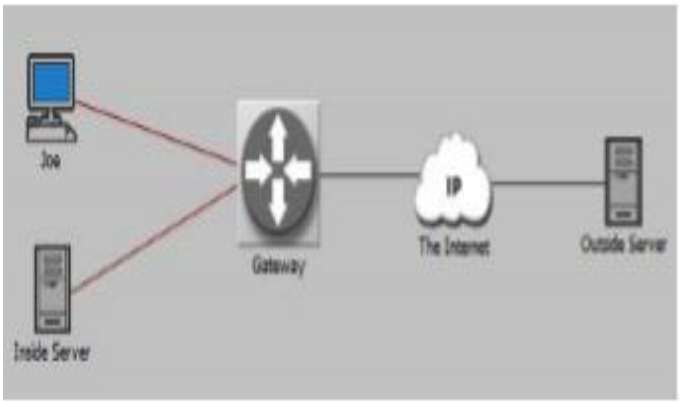

Figure 11: The Network Topology

SIMULATION RESULT AND ANALYSIS

- **Simulation of WSN**

By analyzing the results obtained after running the first project (fig5) it was established that, in the conditions specified in OPNET, the maximum distance nodes can connect is 100 m. In a real environment this distance is smaller [9, 10]. It is possible to increase this distance if routers are used.

By analyzing the scenarios included in project 3(fig7) the importance of implementing routers in order to cover a larger area became clear. In the studied case using three routers proved to be an adequate solution. In this case the number of stations that can be used decreases, by comparison with the second project, since some packets are sent using one or more hops. In this case the global traffic increases, the interference level increases and the packet loss probability also increases.

- **Effect of Transport Protocols on Simulation**

  - **Under the environment without data loss**

Scenario 1 and scenario 2 test average download response time of the application and throughput of the link connecting to the server in the case of no data loss based on different transport protocols in different networks.

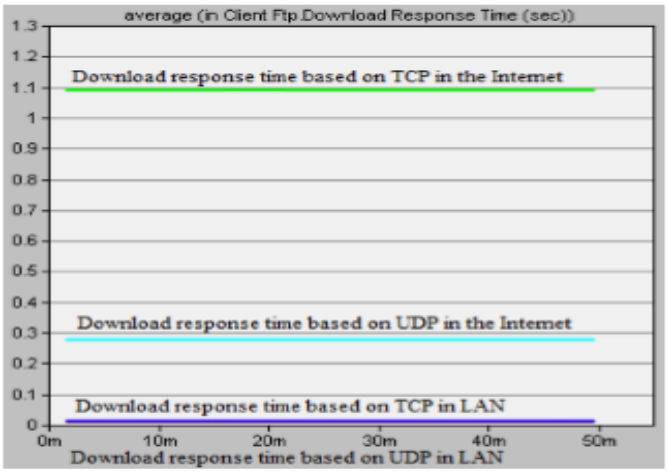

Figure 12: Download response time based on different transport protocols in different networks

In TCP based applications ,download response time is affected by the protocol of Three-way Handshaking, data fragment, confirmation, timeout re-transmission, sorting, traffic control mechanism and congestion control mechanism. UDP is a simple transport layer protocol and it can transmit data directly to avoid the expenditure of establishing a connection. UDP is a packet-oriented transport protocol without data slicing and does not provide confirmation, timeout re-transmission, sorting, flow control mechanism and congestion control mechanism. Therefore, as shown in Fig.4, download response time of TCP-based application is longer than UDP-based application.

The coverage of LAN is relatively small, usually a few thousand meters. It has high stability and the data appears no loss normally. But the Internet is a huge network, covering a wide range and in the process of data transmission, the data need to be forwarded by routers. And the stability of the Internet is poor; therefore, it is easy to produce delay of the data. So in the Internet, download response time of the application is longer

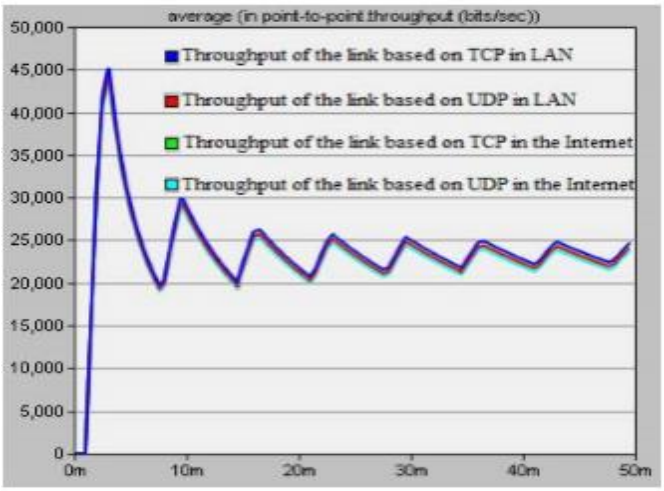

Figure 13: Throughput of the link based on different transport protocols in different networks

The results of throughput of the link in a network environment without data loss are shown in Fig13. Because of the stability of network situation, the data can arrive at the receiving end successfully. Therefore, throughput of the link is basically same in different networks based on different transport protocols. But using UDP transport protocol will get a shorter download response time. Therefore, in the network environment without data loss, it is recommended to use UDP transport protocol.

- **Under the environment with data loss**

Due to the Internet can reflect the impacts of TCP and UDP on the application performance in the case of data loss more clearly. So in scenario 3 and scenario 4 we mainly study the effects of different transport protocols on download response time of the application and throughput of the link connecting to the server in the environment that data loss rate is 0%, 0.5%, 1%, 5% in the Internet.

In the environment with loss of data, the results of download response time of the application based on TCP are shown in Fig14.When the data loss rate is increased, the increasing number of TCP retransmission makes download response time of the application longer. Therefore, with the increase of data loss rate, the download response time of the application becomes longer.

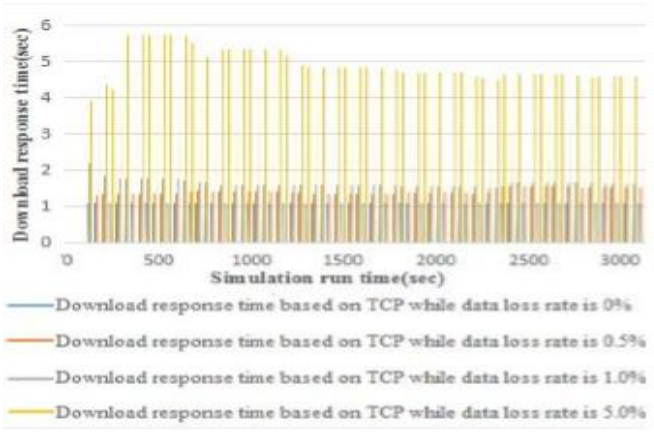

Figure 14: Download response time based on TCP in the environment of different data loss rates

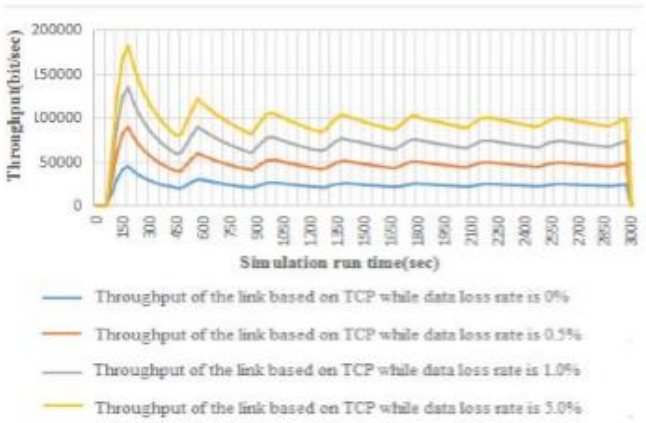

Figure 15: Throughput of the link based on TCP in the environment of different data loss rates

In the environment with data loss, the results of throughput of the link connecting to the server based on TCP are shown in Fig15 When data loss rate is increased, more and more data need to be re-transmitted. Thus, as data loss rate increases, throughput of the link connecting to the server becomes larger.

In the environment with data loss, the results of download response time of the application based on UDP are shown in Fig.8. With lost data increases, the data that need to be sent are getting less. Therefore, download response time of the application becomes shorter with the increase of data loss rate.

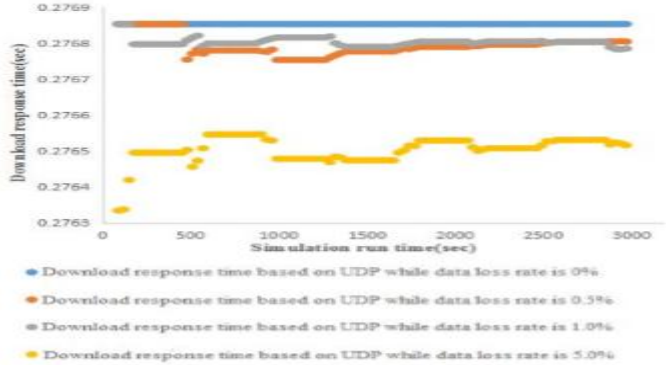

Figure 16: Download response time based on UDP in the environment of different data loss rates

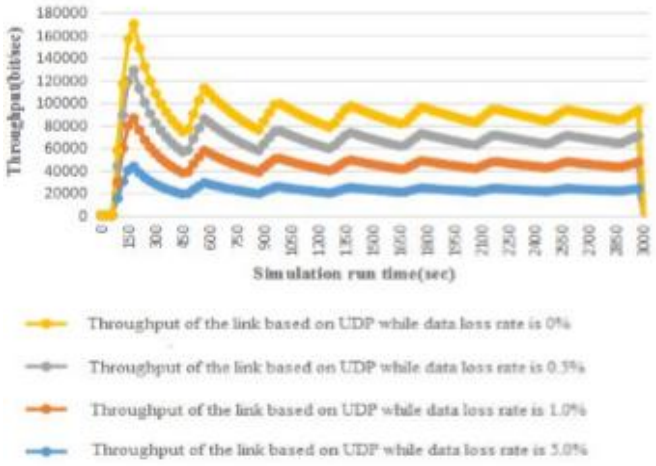

Figure 17: Throughput of the link based on UDP in the environment of different data loss rates

In the environment with data loss, the results of throughput of the link connecting to the server based on UDP are shown in fig17.When lost data are increasing; the data that need to be transmitted are reduced. Therefore, throughput of the link connected to the server becomes smaller with the increase of data loss rate. When data are lost, TCP can ensure the correctness of the data through the confirmation and retransmission mechanism. But UDP does not provide reliable data transmission and loses a lot of data. Therefore, in the environment with data loss, it is recommended to use TCP transport protocol.

CONCLUSION

In simulation of wsn, the number of stations is limited by the fact that next to the useful traffic there is also network related traffic. By increasing the data traffic the node number should be decreased accordingly. For worst working conditions, in order to assure good communication, the number of stations should also be decreased. In this case acknowledgments and retransmissions should be used which leads to increased traffic. If the network is one that requires that transmission form certain nodes should not be interrupted then the corresponding router should be doubled or even all routers could be doubled. In a normal situation the nodes will randomly join one of the routers and in case of failure of one of the two routers the remaining router shall take the remaining traffic.

This paper also implemented the study of the effects of different transport protocols on FTP application performance in the different network environments based on OPNET. Through different scenarios, the impacts of TCP and UDP on download response time of application and throughput of the link connecting to the server in different network environments are compared and we can learn that different transport protocols will have different impacts on the performance of applications in different environments and the simulation results are analyzed based on the characteristics of TCP and UDP.We find that UDP is able to use less time to transmit data in the case of no data loss and can avoid the overhead of establishing a connection.TCP is able to provide better transport services in order to ensure the correct transmission of data in the environment with data loss.

REFERENCES

[1] L. Xu, Z. D. Chen and C. Huang, “The Application of Game Theory in Wireless Sensor Network,” Science Press, 2012.
[2] J.-S. Lee, Y.-W. Su and C.-C. Shen, „A Comparative Study of Wireless Protocols: Bluetooth, UWB, ZigBee and Wi-Fi, The 33rd Annual Conference of the IEEE Industrial Electronics Society (IECON) Nov. 58, 2007,Taipei, Taiwan.
[3] A. Timm-Giel, K. Murray, M. Becker, C. Lynch, C. Görg, D. Pesch, “Comparative Simulations of WSN”, ICT-MobileSummit 2008.
[4] Molina, G., Alba, E.: Location discovery in Wireles Sensor Networks using metaheuristics. Applied Soft Computing 11,1223–1240 (2011).
[5] R. Vigneri, “Radio Physics for Wireless Devices and Networking”.
[6] C. Marghescu,”Study and Optimization of a Wireles Sensor Network”.
[7] Wireless Sensor Networks - An Introduction, Wireless Sensor Networks: Application-Centric Design, Yen Kheng Tan (Ed.),ISBN: 978-953-307-321-7.
[8] Vats, k. and Dalal, M. (2012) “OPNET based Simulation and performance analysis of GRP Routing protocol”, International Journal of Advance Research in Computer Science and Software engineering, vol. 2, (3), pp.118-122.

[9] W.R Stevens. TCP/IP Illustrated Volume1: The Protocols [M]. Post and Telecom Press, 2010, pp. 223-227.
[10] A darshpal S.Sethi, Vasil Y.Hnatyshin. The Practical OPNET User Guide for Computer Network Simulation [M]. CHINA MACHINE PRESS, 2014, PP. 1
[11] J. Shi, L. J. Zhong. Study of OPNET Network Simulation Mechanism and Modeling Method [J]. Science and Technology Information, 2009.
[12] Y. B. Zhang, Z. B. Zhang, Y. Zhao, L. Guo. Analysis and Research on TCP and UDP Network Traffic [J].Application Research of Computer, 2010.
[13] J. S. Kong, P. Y. Ren. Research on TCP Network Congestion Control [J]. Computer Technology and Development, 2013.