http://ansinet.com/itj

ITJ

ISSN 1812-5638

INFORMATION TECHNOLOGY JOURNAL

ANSInet
Asian Network for Scientific Information
308 Lasani Town, Sargodha Road, Faisalabad - Pakistan

Information Technology Journal 9 (3): 430-437, 2010
ISSN 1812-5638

Telecommunications Network using Electromagnetic Waves

M.S. Zahrani
College of Computer Sciences and Information Technology,
King Faisal University, Al-Ahsa, Saudi Arabia

Abstract: The present study identified wireless network as a type of computer network that is related to a telecommunication network where interconnections among its nodes are realized using electromagnetic waves without the use of wires. Additionally, it showed packet-switched network as a network where different packets of information each following a different path are individually sent and then reassembled as they arrive at intended destination. Furthermore, it is established that to make setup trouble-free, select a network adapter that was manufactured by the same vendor who manufactured the wireless router (Impact of Interference on Multi-Hop Wireless Network Performance). It is asserted that in wireless networking, switches are important components of a network since they speed up transmission of messages. Finally the study has pointed out that extending the scalability, lifetime and load balancing of the network are the foremost main requirements for countless informal sensor network applications.

Key words: Wireless network, electronic communication, telecommunications, internet, mobile, information

INTRODUCTION

The wireless network is a type of computer network that is related to a telecommunications network where interconnections among its nodes are realized by use of electromagnetic waves that does not involve the use of wires. Generally, wireless network is used by the public daily for following stock market analysis, communication, weather forecast, news update, business, travel plans, entertainments, learning and shopping (Davis, 2004). This has prompted the need for having a wireless internet connection in order to update their stock, receive text messages on the e-mail and get daily news. Presently the personal and the business life are expanding relying heavily on electronic communication than the Internet. The Wireless Application Protocol (WAP) has become a logical step for using mobile on the Internet. However, it is shown that surfing the Web using a phone is not fast in regard of getting the information required (Shaw, 2007).

The 21st century's greatest communication developments are marked by the internet (Gallo *et al*., 2001). Businessmen are accustomed of observing the various parts of Internet such as the downloaded files, e-mail messages and the web pages, which create the valuable and dynamic medium of internet in their offices (Shaw, 2007). The technological advancement in the transportation system's automation, industries, building, home, utilities and shipboard depends on the real world's sensory data. Emerging from various sensors of dissimilar modalities in distributed settings, sensory data in business environment requires information with reference to its surroundings in addition to its internal workings. Wireless network by using distributed wireless sensor networks provides solution to monitoring and collecting the data, detecting the relevant quantities, evaluation along with assessing the information, carry out decision-making functions and formulate meaningful user displays in business settings (Engst and Fleishman, 2002). In order to accomplish these functions, it is advisable to incorporate hybrid energy efficient distributed clustering approach which chooses cluster heads depending on a hybrid of their outstanding energy, node proximity and a secondary consideration. Extending the scalability, lifetime and load balancing of the network are the foremost main requirements for countless informal sensor network applications.

The protocol of hybrid energy efficient distributed clustering makes no assumptions with regards to the density of nodes, distribution or the node locality awareness. As the study shows, the process of hybrid energy efficient distributed clustering terminates in O (1) iterations not relying on size or topology of the network. It eventually results in low operating cost of messages exchanged together with processing cycles. Moreover, there will be a comparatively regular distribution of cluster head throughout the sensor network (Engst and Fleishman, 2002). The balancing of load among cluster heads is achieved by making a thoughtful selection of the secondary clustering parameter. The results of hybrid energy efficient distributed clustering model reveals that it surpasses weight-based clustering protocols based on a number of cluster characteristics like supporting data aggregation and effectual prolonged network lifetime.

A wireless communication network can be composed of nodes in a distinct network that comprises of numerous interlinked subnets of fully connected ring, star, bus, mesh and tree topologies (Cardei *et al*., 2005). In order to realize throughput associated with quality of service as well as quantity of service, an appropriate network topology must be used taking into consideration the message due dates, transmission power, bit error rates, economic cost of transmission, packet loss and message delay. One way of integrating wireless network is through use of wireless local area network where radio waves are used to broadcast data from side to side among networked computers in a small region particularly a school, an office or a home. Still it can be performed through use of wireless personal area network which interconnects computer devices that are in a fairly small neighborhood of an individual. The study showed a number of wireless networks in use (Gallo *et al*., 2001).

Kamal *et al*. (2005) addressed the following question: given a specific placement of wireless nodes in physical space and a specific traffic workload, what is the maximum throughput that can be supported by the resulting network? Unlike previous work that has focused on computing asymptotic performance bounds under assumptions of homogeneity or randomness in the network topology and/or workload, we work with any given network and workload specified as inputs. A key issue impacting performance is wireless interference between neighboring nodes. They model such interference using a conflict graph and present methods for computing upper and lower bounds on the optimal throughput for the given network and workload. To compute these bounds, they assume that packet transmissions at the individual nodes can be finely controlled and carefully scheduled by an omniscient and omnipotent central entity, which is unrealistic. Nevertheless, using ns-2 simulations, we show that the routes derived from our analysis often yield noticeably better throughput than the default shortest path routes even in the presence of uncoordinated packet transmissions and MAC contention. This suggests that there is opportunity for achieving throughput gains by employing an interference-aware routing protocol.

Balachandran *et al*. (2002) presented and analyzed user behavior and network performance in a public-area wireless network using a workload capture data a well-attended ACM conference. The goals of present study were (1) to extend our understanding of wireless user behavior and wireless network performance; (2) to characterize wireless users in terms of a parameterized model for use with analytic and simulation studies involving wireless LAN traffic and (3) to apply our workload analysis results to issues in wireless network deployment, such as capacity planning and potential network optimizations, such as algorithms for load balancing across multiple Access Points (APs) in a wireless network.

To begin with through Cellular phones, which are elements of massive wireless networking systems, communication takes place between people who happen to be miles and miles away quite reliably, easily and efficiently. The overseas information is sent through wireless network systems such as satellites (Kumar *et al*., 2008). The police departments and the emergency services make use of wireless network to get in touch with their colleagues who are far away but have important information that is needed quickly. Additionally, businessmen utilize wireless network to share and send data speedily in an office either across the world or within the same building (Rackley, 2007).

The wireless network, due to its nature, is a rapid and inexpensive way of getting connected via the Internet in the third world nations having poor telecom infrastructure. On the other hand, compatibility aspects crop up when coping with wireless networks. This implies that different computer components from different vendors are unlikely to work together, therefore extra work is needed to fix these aspects. Notably, wireless networks are characteristically slower than those networks that are interconnected directly via Ethernet cables (Engst and Fleishman, 2002). Similarly, wireless networking is more susceptible for the reason being that hackers can break into network disseminating information signal. Although, this is not a severe hitch as the security systems have used Wired Equivalent Privacy to block several intruders. Another form of wireless network security is Wi-Fi Protected Access that gives more security in wireless networking than a wired equivalent privacy security system. Also, firewalls are used to solve security problems in wireless networks (Cardei *et al*., 2005).

The research provides the basics required to fully understand the sensor nets. For communication to take place, the information sent must be subdivided into several sections. The header section of the message identifies its destination node, source node, length of the data field and such related information. The header information is utilized by the nodes in suitable transmission of the message. To improve the security of routed information, ciphered messages and parity bits are incorporated. During message transmission by the use of packet routing networks, each and every message is broken down into preset length packets. The transmission of packets is then carried out separately all the way through the network and finally reassembled at the

indented destination. The use of predetermined length of packet formulates an easier routing process that ensures quality of service satisfaction (Habraken, 2006). Usually, voice communications make use of circuit switching for packet transmission whereas data broadcasting employ packet routing (Cardei *et al*., 2005).

The FDDI protocol broadcasts the information section of content messages of the nodes with special frames that identifies and gives details of fault conditions in the transmitted information. The transmission of these special frames permits reconfiguration of the network for recovery of faults in the transmitted information. Extra special frames transmitted with message content comprise of route discovery packets which are sometimes referred to as ferrets (Briere *et al*., 2008). These ferrets flow from the beginning to the end of the network mainly to identify information on transmission cost, failed links and shortest paths. They also act as feedback mechanism in which they return to the starting place of the transmitted message and give the information on the best route for transmitting subsequent messages. As soon as a given node needs to send out a message, reliability is enhanced by the destination node and the handshaking protocols (Habraken, 2006). The destination plus the source nodes have to alternately transmit along these lines: the source gives a request to send, destination node issues a ready message to receive and the source node sends the message and then the source issues a feedback to signal that a message was received. The main purpose of ensuring handshaking is to guarantee both Quality of Service as well as quantity of service and enable retransmission of messages which were faultily received (Briere *et al*., 2008).

SWITCHING

It is well known that the transmission of packets from source node to destination node demands for switching. For the most part, a store and forward switching technique is used by the computer network to manage the information flow during transmission. Whenever, the packets arrive at the destination node, these are completely stored in restricted memory before being sent out as one piece. Other sophisticated technique of switching is wormhole that divides the message, which is to be transmitted, into miniature units recognized as flits or still flow control units. The route is established by the header flit. At the same time of routing the header, the residual flits go after the header flit in pipeline manner. Unfortunately, this switching method is observed of attaining the low latency of message receipt. A different trendy scheme of switching is virtual-cut-through where the header arriving at the temporary buffering node is switched devoid of waiting for the other packets those follow it. These packets are stored in memory in central buffers, software buffers, in the memory in edge buffers and hardware buffers (Gast, 2005).

For multiple access protocols in which multiple nodes need to be broadcasted, protocols are desired such as to evade lost data and collisions. The ALOHA scheme that was originally utilized at the University of Hawaii in 1970's, a message is transmitted by a node when the need arises. Acknowledgment can either be received or not. When acknowledgment is not received, the node keeps waiting for a random period of time and before the same message is re-transmitted. As for Frequency Division Multiple Access (FDMA) where different carrier frequencies resources are associated with different nodes, there is a drop off in the available bandwidth for each and every node. Furthermore, this scheme calls for extra intelligence and hardware at every node. A unique code is employed by every node to cipher its messages before transmission in Code Division Multiple Access (Rackley, 2007). This process leads to increased complications of the receiver together with the transmitter. As with Time Division Multiple Access, the link is separated on a time axis where every node is given a fixed time slot for utilization in communication. As it is observed that it reduces the sweep rate although it has an advantage of possessing the capability of being implemented in software. Each and every one node necessitates synchronized and accurate clock for Time Division Multiple Access (Gast, 2005).

The relationship that exists between the transmitted messages in a wireless communication network and applications programs run by the users is specified by The international standards organization architecture (Brodsky, 2007). The advancement of the open standard has promoted the adoption of uniform compatible arrangements interfaces by different vendor and developers. Error detection and correction is provided by the Transport Layer while the Network Layer carries out flow control and routing. The concrete hardware communication linkage interconnections are represented by the Physical Layer as the Applications Layer corresponds to programs users run (Gast, 2005).

ROUTING

For a distributed network with many nodes, routing is used to control transmission of messages at shared node. This is because; there are multiple pathways that do exist from the source to the destination. Unless routing is correctly done, the throughput which is measured in terms

Fig. 1: The diagram illustrates how one wireless router can be used to connect several devices to the internet

of quantity of service and the average packet delay that is measured in terms of quality of service are affected. Routing schemes does not only prevent deadlock but also livelock (Lowe, 2007). The wireless routing is explained in Fig. 1.

The main methods of routing used are adaptive, fixed, centralized, token ring, broadcast and distributed. In Token ring technique, a token is passed endlessly around a topology that takes the form of a ring. The node, that desires to send out, captures the circulating token and appends the message (Rackley, 2007). The intended node on the ring topology reads the header while the token passes and captures the send message. Sometimes, the destination attaches an acknowledgment message as a feedback mechanism. Thereafter, the token is let loose to accept more messages. Despite the fact that this method is reliable, it leads to wastage of network capability as the token has to go through the whole ring for every message (Gast, 2005).

Fixed routing methods make use of routing tables that specify the subsequent node for routing by using the present message locality and the node specified as the destination. It is shown that tables used for routing at times become so large for huge wireless networks and therefore lack the capability of taking into account the real-time effects like congested links, failed links and nodes with backed up queues. The adaptive routing schemes rely on the present status of the network and know how to take into consideration the various performance procedures that include congestion of a given link, transmission cost on a given link, transmission time and reliability of a path. The routing algorithms are based on a variety of network analysis and concepts of graph theories like minimum-span problems, maximal flow and shortest-route (Gallo *et al*., 2001). The shortest path routing methods locate the shortest path from a source node to the destination node and when cost is involved, it is correlated with every link (Cardei *et al*., 2005).

The routing is also aimed at livelock and deadlock avoidance. The wireless communication networks, those involve large-scale switching, have circular paths of nodes where node is a shared resource that takes into account many messages that flow along dissimilar paths in the circuit. This leads to deadlock as the entire nodes in a particular cycle have buffers that are already full and yet they are waiting for one another. Conversely livelock results when a message is recurrently broadcasted around the wireless network but it never arrives at its intended destination (Held, 2002). The livelock, a problem in routing, is a deficiency of a few routing methods that switch the message to be transmitted to alternate connections at a time when the preferred links are already congested not considering that the transmitted message ought to be routed nearer to its intended final destination (Engst and Fleishman, 2002).

DISCUSSION

The routing tries to improve flow control so as to shield the wireless network from speed mismatches and overload, increase network fairness and efficiency, maintains the quality of service of the network and protect it from deadlock (Steinke, 2008). The flow control in these queuing networks is provided using the associated buffer and queue that every node has to stack messages. Through the arrival of ad hoc networks of physically distributed sensors in inaccessible site environments, brings an increasing focus on the existences of sensor nodes throughout power conservation, power generation and power management (Rackley, 2007). The fair routing scheme routes all the messages fairly irrespective of their preference. In the case of buffer management, definite buffer portions are assigned for specific purposes. With the choke packet designs, whichever node that sense congestion has to send choke packets to the rest of the

Fig. 2: A typical ad hoc network

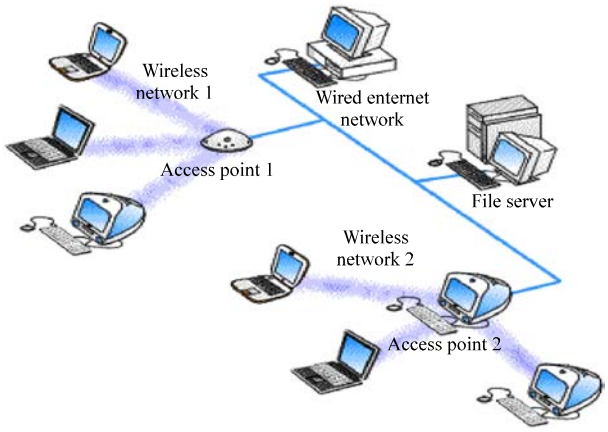

Fig. 3: The diagram shows multiple access points

nodes to inform them to decrease their transmissions (Gallo *et al*., 2001). A typical ad hoc network is shown in Fig. 2.

Designing of small micro-electromechanical systems Radio Frequency components like inductors and capacitors for transceivers contributed to wireless networking (Lowe, 2007). The current restrictive aspect is in the fabrication of micro-sized inductors. One more plunge is in devising and proposal of small micro-electromechanical systems power generators via electrostatic, thermal and electromagnetic technologies. For the time being, software power management methods are capable of significantly reducing the power used by Radio Frequency sensor nodes (Mueller, 2008). The Time Division Multiple Access (TDMA) is valuable in power conservation as every node can power down at its allocated time slots and then resuming for message transmission at the next time slot allocation (Gallo *et al*., 2001). This is shown in Fig. 3.

Since, the increase in the necessary transmission power is depended on the square of the distance between the destination and source, many short transmission message hops needs less power than long ones (Rackley, 2007).

If the truth is to be told, when this distance is R, the power necessary for single-hop transmission is equivalent to R^2. When the nodes between the destination and source seize, the benefits of transmitting n short hops as a substitute, the required power for every node becomes proportional to R^2/n^2 (Gallo *et al*., 2001). Therefore it becomes a good argument supportive of distributed networks that have multiple nodes like nets of the mesh topology (Engst and Fleishman, 2002). The research shows that congestion increases with too much use of power by any node. Nevertheless every node is required to select a big enough range of transmission that would maintain the network connection. When n nodes are arbitrarily dealt out in a disk, the network would be asymptotically linked with the possibility of one when the range of transmission is r for all nodes selected using the formula:

$$r \geq \sqrt{\frac{\log n + r(n)}{\pi n}}$$

where, the function r(n) goes to infinity as n becomes large. In distributed networks where use of routing tables is common, there is an exponential increase as more nodes are attached (Rackley, 2007).

For a network that has n mesh, it would have nm links and there would be several paths from every source to everyone of the destination. Routing is simplified in hierarchical network arrangements. Furthermore, they are agreeable to distributed signal decision-making and processing attributed to the fact that some processings are able to be made at every hierarchical layer. Earlier study reveals that a completely networked connection has NP-hard complexity, whilst striking routing protocols through restricting the permitted paths to achieve reentrant flow topology outcomes in polynomial complexity. These kinds of streamlined protocol are normal for hierarchical networks (Engst and Fleishman, 2002).

Multicast systems: The Multicast Systems (MS) within mesh networks utilize a hierarchical leader-based method for transmitting messages. Each one group of nodes contains allocated leader which is responsible for receipt of messages and broadcasting to nodes that are exterior to the group (Lowe, 2007). For hierarchical networks, a lot of work has been made on proper hierarchical structures designed for distributed networks. It is shown that a regular numbering method in hierarchical systems permits

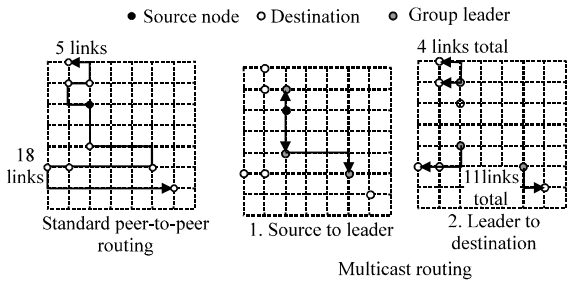

Fig. 4: Multicast routing improves efficiency and reduces message path length adopted from (Chin *et al*., 2000)

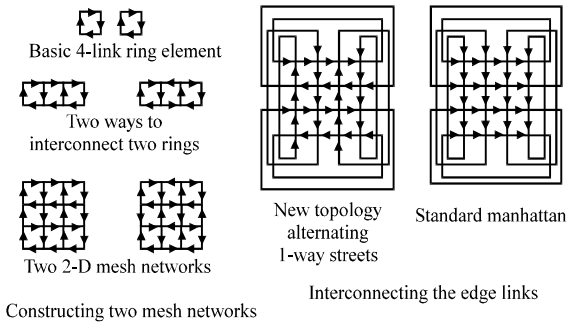

Fig. 5: Routing schemes of hierarchical network

use of a basic tree-based routing design (Brodsky, 2007). The edge binding in networks makes the routing power of marginal stations to be wasted since peripheral connections are unexploited. Accordingly, transmitted messages are inclined to replicate off the margin to shift in parallel to the margin. To evade this idea, the use of Manhattan geometry can connect the nodes on one edge of the network to those nodes that are at the opposite periphery (Heltzel, 2003). Since, the addition of nodes exponentially increases the number of connections, therefore, it heads for NP-complexity setbacks during failure of recovery and routing. The Multicast system, which improves routing efficiency and reduces message path length, is explained in Fig. 4.

It is simplified using hierarchical clustering procedures. The hierarchical arrangement used should be dependable by having a matching structure at every level (Brodsky, 2007).

Hierarchical network: In order to carry out routing in hierarchical network, a number of things has to be accomplished. Selection of a consistent numbering format such as numbering the groups as 1, 2, 3, 4 starting in the top left and moving clockwise is the first thing and must be done at every level. By means of this numbering format it is easy to construct routing scheme because the equivalent basic routing algorithm is reiterated at every hierarchical level. Unlike quad tree routing employed in mobile robot path arrangement, failure recovery is clear-cut. Apart from having an easy code to write, failing of one link only necessitates for switching in the disabled connections (Briere *et al*., 2008). The routing schemes of Hierarchical network are shown in Fig. 5.

It is a good idea in failure recovery as well as routing system to assign the entry node for hierarchical networks for every group as a group leader. The group leader node is required to make extra decisions than other nodes like disabled link activation for failure recovery and accessibility of resource for deadlock avoidance (Gast, 2005). The process would lay an accepted framework for digital signal processing and dispersed decision-making in which the group leader would have to process the group's data before sending it out. This way, the group leader for this wireless communications must be every group's entry node whereas the group leader for digital signal processing ought to be every group's exit node (Kotz and Essien, 2005).

Ethernet: The development of Ethernet was done in 1970's by Xerox, DEC and Intel. The Ethernet standard IEEE 802.3 was released in 1983 by the Institute of Electrical and Electronics Engineers (Rabaey *et al*., 2000). This type of Ethernet was a bit faster as it is operated at ten times higher speed than the regular Ethernet's speed. Its adoption was officially done in the year 1995 (Cardei *et al*., 2005). This brought into being new features like auto-negotiation together with full-duplex operation. The 4 Mbit/s Token ring network was initiated in the year 1984 IBM. In spite of the fact that this system was robust and of high quality than Ethernet, but the Ethernet was more popular owing to cost considerations. The token ring was standardized by the Institute of Electrical and Electronics Engineers with the specification of IEEE 802.5. The fiber distributed data interface stipulates a 100 Mbit/s token-passing which is a dual-ring Local Area Network that makes use of fiber optic cable. In the mid 1980s, the American National Standards Institute developed it. It was much faster than the competence of IEEE 802.5 and Ethernet that existed during that period (Briere *et al*., 2008).

Gigabit ethernet alliance: The establishment of gigabit ethernet alliance took place in 1996 and then the ratification of Gigabit Ethernet standards occurred in 1999, indicating a physical layer that makes use of a combination of original Ethernet technologies and technologies of fiber optic cable from fiber distributed

data interface (Kotz and Essien, 2005; Rabaey *et al*., 2000). The Client-Server networking turned out to be popular during the late 1980's through the substitution of large mainframe computers by systems of personal computers. Application programs designed for distributed computing backgrounds are fundamentally divided into the server or back end and the client or front end parts (Briere *et al*., 2008).

The personal computer's user is the client and more dominant server machines interface toward the network. The Peer-to-Peer architectural networks have machines with the same responsibilities along with capabilities. Here, computers are interconnected to one another by use of a bus topology in order to share printers, files and Internet access. However, the server is missing in client server technologies. From client server technology, the trend moved to Peer-to-Peer computing which was a major next inventory step over P2P networking. The tasks of computing were split among multiple computers, with the upshot being brought together for further utilization. The P2P computing ignited a revolution for the age of Internet and it acquired considerable achievement within a short period. By mid 2000, The Napster MP3 music file sharing application became live in late 1999 as it caught the attention of more than twenty million users (Kotz and Essien, 2005).

The ratification of IEEE 802.11 by the Institute of Electrical and Electronics Engineers was done in the year 1997 as a standard for Wireless Local Area Network. The current versions of IEEE 802.11b support message broadcasting up to a maximum of 11 Mbit/s (Characterizing user behavior and network performance in a public wireless LAN). Currently, it is known as WiFi and is helpful for easy and fast networking of Personal Computers and printers in a local environment like home. The hardware of present laptops and Personal Computers supports WiFi technology.

The costs associated with installation and purchasing a WiFi receivers and router is not beyond reach of home users of Personal Computers (Briere *et al*., 2008). Then in 1998, the initiation of Bluetooth was made and its standardization was done by the Institute of Electrical and Electronics Engineers as Wireless Personal Area Network specification IEEE 802.15 (Rackley, 2007). The Bluetooth is not only a short range Radio Frequency technology that is intended for assisting electronic devices communication between one another along with the Internet but also allows for synchronization of data to facilitate transparency to the user (Mueller, 2008). It supports many devices such as laptops, personal computers, joysticks, printers, keyboards, PDA, mice and cell phones. The inventory protocols permit latest and new devices to be fastened to the wireless network. This device makes use of the unauthorized 2.4 GHz band and has the capability of broadcasting data to a maximum of 1 Mbit/s. It is able to penetrate solid non-metal obstacles and encompasses a nominal range of between ten meters to a hundred meters (Briere *et al*., 2008).

The study showed that a master station is able to service up to seven concurrent slave connections. At the moment, development kits of Bluetooth can be bought from assorted suppliers except that the systems commonly involve lot of effort, time, knowledge for debugging and programming. The initiation of Home Radio Frequency was made in 1998 and is considered to have comparable goals to those of bluetooth for wireless PAN to transmit shared data/voice (Mueller, 2008). The Home Radio Frequency interfaces with the public switched telephone network and the internet. It employs the 2.4 GHz band in addition to having a range of 50 m that makes it appropriate for yard and home. It can accommodate maximum of one hundred nodes in one network. The Wireless PAN Technology, encompassed in IrDA, has a narrow-transmission-angle and a short-range beam that is appropriate for selective and aiming signals reception (Briere *et al*., 2008).

Wireless sensor networks: The information required by smart environments is collected by wireless sensor networks in utilities, buildings, industrial, shipboard, transportation and home systems automation (Cardei *et al*., 2005). The Wireless sensor nodes are expected to carry out different functions such as self-identification, reliability, self-diagnosis, ease of installation and time awareness for synchronization with some software functions, other nodes and standard control network interfaces and protocols (Brodsky, 2007). Even if there are lots of networks as well as sensor manufacturers on the market today, it is still very expensive for these manufacturers to come up with unique transducers for all networks that are on the market. The compatibility of all these different components from different vendors has to be maintained. A smart sensor came up after a study that was carried out by the Institute of Electrical and Electronics Engineers in the year 1451 (Brodsky, 2007). The IEEE 1451 Standard for Smart Sensor Networks is presented in Fig. 6.

This device offers extra functionalities outside the ones required for creating a correct symbol of the quantity that was sensed. The functions included are signal processing, signal conditioning, alarm functions and decision-making. The Smart sensors are used in moving the intelligence nearer to the point of measurement which makes it lucrative to maintain and incorporate dealt out sensor systems (Briere *et al*., 2008).

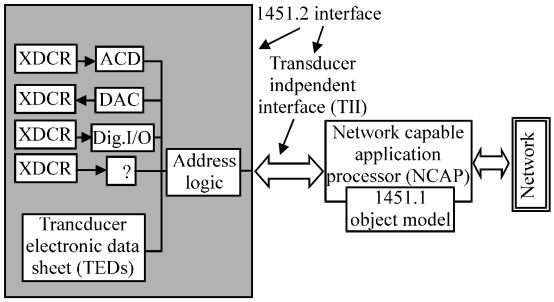

Fig. 6: The IEEE 1451 standard for smart sensor networks

CONCLUSION

This study identified wireless network as a type of computer network that is related to a telecommunication network where interconnections among its nodes are realized using electromagnetic waves without the use of wires. Additionally, it showed packet-switched network as a network where different packets of information each following a different path are individually sent and then reassembled as they arrive at intended destination. Furthermore it is established that to make setup trouble-free, select a network adapter that was manufactured by the same vendor who manufactured the wireless router (Impact of Interference on Multi-Hop Wireless Network Performance). It is asserted that in wireless networking, switches are important components of a network since they speed up transmission of messages. Finally the study has pointed out that extending the scalability, lifetime and load balancing of the network are the foremost main requirements for countless informal sensor network applications.

REFERENCES

Balachandran, A., G.M. Voelker, P. Bahl and P.V. Rangan, 2002. Characterizing user behavior and network performance in a public wireless LAN. ACM SIGMETRICS Performance Evaluat. Rev., 30: 195-205.

Briere, D., H. Pat and F. Edward, 2008. Wireless Home Networking. Dummies, Chicago, USA.

Brodsky, I., 2007. Wireless Computing: A Managers Guide to Wireless Networking. John Wiley and Sons, USA.

Cardei, M., C. Ionut and D. Dingzhu, 2005. Resource Management in Wireless Networking. Artech House, New Jersey.

Chin, T.S., C.Y. Chang and J.P. Sheu, 2000. Efficient path-based multicast in wormhole-routed mesh networks. J. Syst. Architecture, 46: 919-930.

Davis, H., 2004. Absolute Beginners Guide to Wi-Fi Wireless Networking. Que Publishing Company, China.

Engst, A. and G. Fleishman, 2002. The Wireless Networking Starter Kit: The Practical Guide to Wi-Fi Networks for Windows and Macintosh. Springer, New Jersey.

Gallo, M., H. William and H. Bill, 2001. Networking Explained. Digital Press, New Jersey.

Gast, M.S., 2005. 802.11 Wireless Networks: The Definitive Guide. 2nd Edn., O'Reilly Media Inc., USA., ISBN: 978-0-596-10052-0.

Habraken, J., 2006. Home Wireless Networking in a Snap. Indianapolis IN Sams Publishing, USA.

Held, G., 2002. Building a Wireless Network. CRC Press, Boca Raton.

Heltzel, P., 2003. Complete Wireless Home Networking. Prentice Hall PTR, New York.

Kamal, J., P. Jitendra, P. Venkata and Q. Lili, 2005. Impact of interference on multi-hop wireless network performance. J. Wireless Networks, 11: 471-487.

Kotz, D. and K. Essien, 2005. Analysis of a campus-wide wireless network. J. Wireless Networks, 11: 115-133.

Kumar, A., M. Joy and D. Kuri, 2008. Wireless Networking. Morgan Kaufmann, California.

Lowe, D., 2007. Networking for Dummies. 8th Edn., For Dummies, Chicago, ISBN-13: 978-0-470-05620-2.

Mueller, S., 2008. Upgrading and Repairing Laptops. Que Publishing, Bomodong.

Rabaey, J.M., M.J. Ammer, J.L. de-Silva, D. Patel and S. Roundy, 2000. Pico radio supports ad hoc ultra-low power wireless networking. J. Dept. Electrical Eng. Comput. Sci., 33: 42-48.

Rackley, S., 2007. Wireless Networking Technology: From Principles to Successful. Elsevier, Amsterdam.

Shaw, R., 2007. Wireless Networking Made Easy: Everything You Need to Know to Build Your Own PANs, LANs and WANs. AMACOM Books, New York.

Steinke, S., 2008. Network Tutorial: A Complete Introduction to Networks. Focal Press, Boston, MA.