ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

Challenges in Wireless Sensor Networks

[I]Alaa Eisa Mohammed, Samir M. Abd Elrazik, Hazem M. El-Bakry,
[II]Sajjad Q. hasan, Asaad Q. Hasan, [III]Samir Zaid
[I]Information Systems Dept., Faculty of Computer and Information Sciences,
Mansoura University, Al-Mansoura, EYGPT
[II]University of Baghdad, IRAQ
[III]Dept. of Geology, Faculty of Sciences, Zagazig University, EGYPT

Abstract

Wireless sensor networking is an emerging technology that promises a wide range of potential applications in both civilian and military areas. These sensor nodes are not only sensing, but also data processing and communicating capabilities. Distinguished from traditional wireless communication networks, for example, cellular systems and mobile ad hoc networks (MANET), WSNs have unique characteristics, for example, denser level of node deployment, higher unreliability of sensor nodes, and severe energy, computation, and storage constraints, which present many new challenges in the development and application of WSNs as large scale, energy constraints, amount of data that can be stored and unreliable environment. These hardware constraints present many challenges in software development and network protocol design for sensor networks. The main aim of most research in WSN is how to provide maximum lifetime to network and how to provide secure communication to network which must consider not only the energy constraint in sensor nodes, but also the processing and storage capacities of sensor nodes.

I. Introduction

WSNs are the breakthrough approach based on networks of devices that can be densely deployed in human aggressive and inaccessible environments, to sense and instrument the environment and monitor with high accuracy physical phenomena. Each one of these devices is called a sensor node. Each node should not be larger than a few square millimeters and its target cost is less than US$1.00, including radio, microcontroller, power supply and sensor (capable of sensing temperature, light, vibration, sound, etc.) [1-3]. The individual nodes in a WSN are inherently resource constrained: They have limited processing speed, storage capacity, and communication bandwidth.

Wireless Sensor Networks (WSN)s are highly distributed self-organized systems. They rely on significant numbers of scattered low-cost tiny devices featuring strong limitations in terms of processing, memory, communications and energy capabilities. Sensor nodes collect measurements of interest over a given space, making them available to external systems and networks at special nodes designated sink nodes [1-12].

II. Sensing and Sensors

Sensing is a technique used to gather information about a physical object or process, including the occurrence of events (i.e., changes in state such as a drop in temperature or pressure). An object performing such a sensing task is called a ***sensor***.

From a technical perspective, a sensor is a device that translates parameters or events in the physical world into signals that can be measured and analyzed. Many wireless sensor networks also include actuators which allow them to directly control the physical world. That is called a wireless sensor and actuator network (WSAN) [8-21].

III. Wireless Sensor Networks

Wireless sensor networks are potentially one of the most important technologies of this century. Recent advancement in wireless communications and electronics has enabled the development of low-cost, low-power, multifunctional miniature devices for use in remote sensing applications. The combination of these factors has improved the viability of utilizing a sensor network consisting of a large number of intelligent sensors, enabling the collection, processing analysis and dissemination of valuable information gathered in a variety of environments. A sensor network is composed of a large number of sensor nodes which consist of sensing, data processing and communication capabilities [22-32].

Sensor network protocols and algorithms must possess self-organizing capabilities. Another unique feature of sensor networks is the cooperative effort of sensor nodes. Sensor nodes are suitable with an onboard processor. Instead of sending the raw data to the nodes responsible for the fusion, they use their processing abilities to locally carry out simple computations and transmit only the required and partially processed data.

Sensor networks are predominantly data-centric rather than address-centric, so sensed data are directed to an area containing a cluster of sensors rather than particular sensor addresses. Given the similarity in the data obtained by sensors in a dense cluster, aggregation of the data is performed locally.

IV. History of Wireless Sensor Networks

As with many other technologies, the military has been a driving force behind the development of wireless sensor networks. For example, in 1978, the Defense Advanced Research Projects Agency (DARPA) organized the Distributed Sensor Nets Workshop, focusing on sensor network research challenges such as networking technologies, signal processing techniques, and distributed algorithms. DARPA also operated the Distributed Sensor Networks (DSN) program in the early 1980s, which was then followed by the Sensor Information Technology (SensIT) program.

In collaboration with the Rockwell Science Center, the University of California at Los Angeles proposed the concept of Wireless Integrated Network Sensors or WINS [16]. One outcome of the WINS project was the Low Power Wireless Integrated Micro-sensor (LWIM), produced in 1996. This smart sensing system was based on a CMOS chip, integrating multiple sensors, interface circuits, digital signal processing circuits, wireless radio, and microcontroller onto a single chip. The Smart Dust project at the University of California at Berkeley focused on the design of extremely small sensor nodes called *motes*. The goal of this project was to demonstrate that a complete sensor system can be integrated into tiny devices, possibly the size of a grain of sand or even a dust particle. The PicoRadio project by the Berkeley Wireless Research Center (BWRC) focuses on the development of low-power sensor devices, whose power consumption is so small that they can power themselves from energy sources of the operating environment, such as solar or vibrational energy. The MIT μAMPS (micro-Adaptive Multidomain Power-aware Sensors) project also focuses on low-power hardware and software components for sensor nodes, including the use of microcontrollers capable of dynamic voltage scaling and techniques to restructure data processing algorithms to reduce power requirements at the software level.

While these previous efforts are mostly driven by academic institutions, over the last decade a number of commercial efforts have also appeared (many based on some of the academic efforts described above), including companies such as Crossbow (www.xbow.com), Sensorial (www.sensoria.com), World sense (http://worldsens.citi.insa-lyon.fr), Dust Networks (http://www.dustnetworks.com), and Ember Corporation (http://www.ember.com).

These companies provide the opportunity to purchase sensor devices ready for deployment in a variety of application scenarios along with various management tools for programming, maintenance, and sensor data visualization [4].

V. Wireless Sensor Networks vs Traditional Wireless Networks (ad-hoc network)

There are also many fundamental differences which lead to the need of new protocols and techniques. Some of the most important characteristic differences are summarized below [2]:

- Number of nodes in wireless sensor network is much higher than any traditional wireless network. Possibly a sensor network has to scale number of nodes to thousands. This needs a highly scalable solution to ensure sensor network operations without any problem.
- Due to large number of sensor nodes, addresses are not assigned to the sensor nodes. Sensor networks are not address-centric; instead they are data-centric network. Operations in sensor networks are centered on data instead of individual sensor node. As a result sensor nodes require collaborative efforts.
- Sensor nodes mainly use a broadcast communication paradigm, whereas most ad hoc networks are on point-to-point communications.
- Sensor nodes are much cheaper than nodes in ad hoc networks.
- Wireless sensor networks are environment-driven. While data is generated by humans in traditional networks, the sensor network generate data when environment changes. As a result the traffic pattern changes dramatically from time to time.

VI. WSN Characteristics

WSN middleware should support the implementation and basic operation of a sensor network. However, this is a non-trivial task, as WSNs have some unique characteristics: First, sensor nodes are small-scale devices with volumes approaching a cubic millimeter in the near future. Such small devices are very limited in the amount of energy they can store or harvest from the environment. Furthermore, nodes are subject to failures due to depleted batteries or, more generally, due to environmental influences. Limited size and energy also typically means restricted resources (CPU performance, memory, wireless communication bandwidth and range) [9-12].

Node mobility, node failures, and environmental obstructions cause a high degree of dynamics in WSN. This includes frequent network topology changes and network partitions. Despite partitions, however, mobile nodes can transport information across partitions by physically moving between them. However, the resulting paths of information flow might have unbounded delays and are potentially unidirectional [2-7].

Communication failures are also a typical problem of WSN. Another issue is heterogeneity. WSN may consist of a large number of rather different nodes in terms of sensors, computing power, and memory. The large number raises scalability issues on the one hand, but provides a high level of redundancy on the other hand. Also, nodes have to operate unattended, since it is impossible to service a large number of nodes in remote, possibly inaccessible [13].

VII. Applications of WSN

Military Applications : There are two example important programs the Distributed Sensor Networks (DSN) and the Sensor Information Technology (SenIT) form the Defense Advanced Research Project Agency (DARPA), are applied very successfully in the military sensing.

Environmental Monitoring: Nowadays sensor networks are also widely applied in habitat monitoring, agriculture research, fire detection.

Medical Application : Sensor networks are also widely used in health care area. In some modern hospital sensor networks are constructed to monitor patient physiological data, to control the drug administration track and monitor patients and doctors and inside a hospital.

Traffic Monitoring: The sensor node has a built-in magneto-resistive sensor that measures changes in the Earth's magnetic field caused by the presence or passage of a vehicle in the proximity of the node.

Robotics Control

Home Application

VIII. Challenges and Constraints

While sensor networks share many similarities with other distributed systems, they are subject to a variety of unique challenges and constraints. These constraints impact the design of a WSN, leading to protocols and algorithms that differ from their counterparts in other distributed systems. **These challenges** are summarized below [9,17]::

- **Application requirements and Environment interaction**: WSNs are environmental event-driven, their activity graph can vary a lot during time.
- **Physical Resource Constraints:** The most important constraint imposed on sensor network is the limited battery power of sensor nodes. The effective lifetime of a sensor node is directly determined by its power supply. Hence lifetime of a sensor network is also determined by the power supply. the choices made at the physical layer of a sensor node affect the energy consumption of the entire device and the design of higher-level protocols. Hence the energy consumption is main design issue of a protocol. Limited computational power and memory size is another constraint that affects the amount of data that can be stored in individual sensor nodes. So the protocol should be simple and light-weighted.

ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

Communication delay in sensor network can be high due to limited communication channel shared by all nodes within each other's transmission range. Besides network protocols, the goal of energy efficiency impacts the design of the operating system (e.g, small memory footprint, efficient switching between tasks), middleware, security mechanisms, and even the applications themselves. For example, *in-network processing* is frequently used to eliminate redundant sensor data or to aggregate multiple sensor readings. This leads to a tradeoff between computation (processing the sensor data) and communication (transmitting the original versus the processed data), which can often be exploited to obtain energy savings.

- **Self-Management:** It is the nature of many sensor network applications that they must operate in remote areas and harsh environments, without infrastructure support or the possibility for maintenance and repair. Therefore, sensor nodes must be *self-managing* in that they configure themselves.
- **Ad Hoc Deployment:** Many applications are requires the ad-hoc deployment of sensor nodes in the specific area. Sensor nodes are randomly deployed over the region without any infrastructure and prior knowledge of topology. In such a situation, it is up to the nodes to identify its connectivity and distribution between the nodes. Many sensor networks, once deployed, must operate without human intervention, that is, configuration, adaptation, maintenance, and repair must be performed in an autonomous fashion. For example, sensor nodes are exposed to both system dynamics and environmental dynamics, which pose a significant challenge for building reliable sensor networks, A *self-managing* device will monitor its surroundings, adapt to changes in the environment, and cooperate with neighboring devices to form topologies or agree on sensing, processing, and communication strategies. *Self-organization* is the term frequently used to describe a network's ability to adapt configuration parameters based on system and environmental state. *Self-optimization* refers to a device's ability to monitor and optimize the use of its own system resources. *Self-protection* allows a device to recognize and protect itself from intrusions and attacks [22-32]. Finally, the ability to *self-heal* allows sensor nodes to discover, identify, and react to network disruptions. In energy-constrained sensor networks, all these self-management features must be designed and implemented such that they do not incur excessive energy overheads.
- **Wireless Networking:** The reliance on wireless networks and communications poses a number of challenges to a sensor network designer. For example, *attenuation* limits the range of radio signals, that is, a radio frequency (RF) signal fades while it propagates through a medium and while it passes through obstacles. As a consequence, an increasing distance between a sensor node and a base station rapidly increases the required transmission power. Therefore, it is more energy-efficient to split a large distance into several shorter distances, leading to the challenge of supporting *multi-hop* communications and routing. Multi-hop communication requires that nodes in a network cooperate with each other to identify efficient routes and to serve as relays. This challenge is further exacerbated in networks that employ *duty cycles* to preserve energy. That is, many sensor nodes use a power conservation policy where radios are switched off when they are not in use. As a consequence, during these down-times, the sensor node cannot receive messages from its neighbors nor can it serve as a relay for other sensors. Therefore, some networks rely on *wakeup on demand* strategies to ensure that nodes can be woken up whenever needed. Usually this involves devices with two radios, a low-power radio used to receive wakeup calls and a high-power radio that is activated in response to a wakeup call. Another strategy is *adaptive duty cycling*, when not all nodes are allowed to sleep at the same time. Instead, a subset of the nodes in a network remain active to form a network backbone.
- **Decentralized Management:** The large scale and the energy constraints of many wireless sensor networks make it infeasible to rely on *centralized* algorithms Instead, sensor nodes must collaborate with their neighbors to make localized decisions, that is, without global knowledge. As a consequence, the results of these *decentralized* (or *distributed*) algorithms will not be optimal, but they may be more energy-efficient than centralized solutions. Consider routing as an example for centralized and decentralized solutions. A base station can collect information from all sensor nodes, establish routes that are optimal (e.g., in terms of energy), and inform each node of its route. However, the overhead can be significant, particularly if the topology changes frequently. Instead, a decentralized approach allows each node to make routing decisions based on limited local information (e.g., a list of the node's neighbors, including their distances to the base station). While this decentralized approach may lead to non optimal routes, the management overheads can be reduced significantly.
- **Design Constraints:** the primary goal of wireless sensor design is to create smaller, cheaper, and more efficient devices. These constraints and requirements also impact the software design at various levels, for example, operating systems must have small memory footprints and must be efficient in their resource management tasks. However, the lack of advanced hardware features (e.g., support for parallel executions) facilitates the design of small and efficient operating systems. A sensor's hardware constraints also affect the design of many protocols and algorithms executed in a WSN. For example, routing tables that contain entries for each potential destination in a network may be too large to fit into a sensor's memory. Instead, only a small amount of data (such as a list of neighbors) can be stored in a sensor node's memory. Further, while in-network processing can be employed to eliminate redundant information, some sensor fusion and aggregation algorithms may require more computational power and storage capacities than can be provided by low-cost sensor nodes. Therefore, many software architectures and solutions (operating system, middleware, network protocols) must be designed to operate efficiently on very resource-constrained hardware.
- **Security:** Many wireless sensor networks collect sensitive information. The remote and unattended operation of sensor nodes increases their exposure to malicious intrusions and attacks. Further, wireless communications make it easy for an adversary to eavesdrop on sensor transmissions. For example, one of the most challenging security threats is a *denial-of-service* attack, whose goal is to disrupt the correct operation of a sensor network. While there are numerous techniques and solutions for distributed systems that prevent attacks or contain the extent and damage of such attacks, many of these

incur significant computational, communication, and storage requirements, which often cannot be satisfied by resource-constrained sensor nodes. As a consequence, sensor networks require new solutions for key establishment and distribution, node authentication, and secrecy.

- **Fault-Tolerance:** In a hostile environment, a sensor node may fail due to physical damage or lack of energy (power). If some nodes fail, the protocols that are working upon must accommodate these changes in the network. As an example, for routing or aggregation protocol, they must find suitable paths or aggregation point in case of these kinds of failures.
- **Scalability:** Most of the applications are needed; the number of sensor nodes deployed must be in order of hundreds, thousands or more. The protocols must scalable enough to respond and operate with such large number of sensor nodes.
- **Quality of Service:** Some real time sensor application are very time critical which means the data should be delivered within a certain period of time from the moment it is sensed, otherwise the data will be unusable .So this must be a QOS parameter for some applications. For example, the RAP protocol proposes a new policy called velocity monotonic scheduling. Here a packet has a deadline and a distance to travel. Using these parameters a packet's average velocity requirement is computed and at each hop packets are scheduled for transmission based on the highest velocity requirement of any packets at this node. While this protocol addresses real time, no guarantees are given. Another routing protocol that addresses real-time are called SPEED. This protocol uses feedback control to guarantee that each node maintains an average delay for packets transiting a node. However, transient behavior, message losses, congestion, noise and other problems cause these guarantees to be limited. Many other functions must also meet real-time constraints including: data fusion, data transmission, target and event detection and classification, query processing
- **Heterogeneity and Complexity:** The more heterogeneous the network is the more powerful and generic it becomes. But on the other hand, more robust and complex routing and communications protocols it requires.

IX. Motivation

In wireless sensor network, there are so many challenges. The main challenges are how to provide maximum lifetime to network and how to provide secure communication to network. As sensor network totally rely on battery power, the main aim for maximizing lifetime of network is to conserve battery power or energy with some security considerations.

In sensor network, the energy is mainly consumed for three purposes: data transmission, signal processing, and hardware operation. It is said in that 70 percent of energy consumption is due to data transmission. So for maximizing the network lifetime, the process of data transmission should be optimized. The data transmission can be optimized by using efficient routing protocols and effective ways of data aggregation.

Routing protocols providing an optimal data transmission route from sensor nodes to sink to save energy of nodes in the network. Data aggregation plays an important role in energy conservation of sensor network. Data aggregation methods are used not only for finding an optimal path from source to destination but also to eliminate the redundancy of data, since transmitting huge volume of raw data is an energy intensive operation, and thus minimizing the number of data transmission. Also multiple sensors may sense the same phenomenon, although from different view and if this data can be reconciled into a more meaningful form as it passes through the network, it becomes more useful to an application.

Moreover when data aggregation is performing data is compress as it is passed through the network, thus occupying less bandwidth. This also reduces the amount of transmission power expended by nodes. Hence secure data aggregation can be considered as a very challenging problem in wireless sensor network.

X. Research Fields

- More studies are required on different types of neural network topologies and training algorithms which would be more compatible with WSNs platforms in the terms of lower computation time and power consumption.
- Provide defined and investigated a novel distributed clustering protocol for WSN.
- The ability of nodes to maintain membership in auxiliary clusters can reinforce the current state of sensor network reliability.
- Invent new network protocols that account for the communication realities of real world environments, Test the individual solutions on real platforms in real world settings, and Synthesize novel solutions into a complete system-wide protocol stack for a real application.
- Measure and assess how the theoretical properties of wireless communication are exhibited in today's and tomorrow's sensing and communication devices, Establish better models of communication realities to feed back into improved simulation tools,
- How to secure wireless communication links against eavesdropping, tampering, traffic analysis, and denial of service. Others involve resource constraints.
- An additional topic of research is the cost-effective identification and maintenance of redundant routing paths in the presence of regularly sleeping nodes. This study will be applied to the setup and maintenance of disjoint reverse broadcast trees routed at the sink.
- A research topic, of importance to real-time industrial applications, is the study of latency guarantees for heterogeneous traffic. This study will be based on the use of the TSMP protocol. The analysis can then be generalized to different transport and routing protocols and application-level mechanisms can be designed to compensate for the variations of transmission delay.
- most of the projects are in an early stage focusing on developing algorithms and components for WSN, which might later serve as a foundation for middleware. Moreover, most of the current results are based on simulations or small-scale experiments in laboratory settings. The suitability for large scale networks still has to be proven. First concrete experiments show that even very simple protocols and algorithms can exhibit surprising complexity at scale. After all, there is still a long way to go for successful WSN middleware, both in terms of design concepts and system implementations.
- Communication protocols for WSN should be energy-efficient to avoid useless wasting of energy resources through minimization of the control and retransmission overhead; should have distributed functionality to exploit the WSN resources in cooperative way, so that overall WSN operation

ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

is not hindered by the limited capacities of individual nodes, and should provide reliability differentiation to support different reliability grades in order to suit the requirements of different applications regarding throughput, latency and energy consumption.

- Although a topic for some years: many problems are not solved yet: Scalability, Robustness, self-organization, heterogeneity
- There are lots of open problems that need further investigation to make reprogramming highly usable and efficient. Code dissemination is a continuing focus of current research. However, design trade-offs and impact factors have not been fully understood. Approaches to solving the broadcast storm problem need further study to improve system performance by reducing control overhead. There has been little research on scope selection, complete validation, and code acquisition functions. Design and implementation of energy-efficient routing and one-to-many communication protocols for WSN are still evolving. For practical use, security measures in reprogramming need to be considered.
- Building adaptive WSN applications through reprogramming is a fantastic area. With reprogramming technology advances, it is envisioned that WSNs not only can embed intelligence into environments, but also have embedded intelligence by reprogramming themselves on the fly to dynamic environments.

Conclusion

In this paper we briefly described wireless sensor networks topic, we presented the definition of sensing process, sensor and wireless sensor networks. After that we gave an overview of wireless sensor networks history and showed that wireless sensor networks is developed for military using, it also can used in different applications such as environment monitoring, medical application, traffic monitoring, robotics control and home application.

We also introduce the differences between wireless sensor networks and traditional wireless networks which lead to the need of new protocols and techniques as a result of wireless sensor networks special characteristics as limited size, energy, communication bandwidth and processing capabilities.

In our paper we summarized most unique challenges and constraints that impact the design of a WSN as Self-Management, Decentralized Management, Fault-Tolerance and Scalability.

At the last of this paper we provide some research fields in wireless sensor network topic.

References

[1]. *DAR (1978) Proceedings of the Distributed Sensor Nets Workshop. Pittsburgh, PA, Department of Computer Science, Carnegie Mellon University.*

[2]. *Pottie, G.J. (2001) Wireless integrated network sensors (WINS): The web gets physical. National Academy of Engineering: The Bridge 31*

[3]. *Bult, K., Burstein, A., Chang, D., Dong, M., Fielding, M., Kruglick, E., Ho, J., Lin, F., Lin, T.H., Kaiser, W.J., Marcy, H., Mukai, R., Nelson, P., Newburg, F.L., Pister, K.S.J., Pottie, G., Sanchez, H., Sohrabi, K., Stafsudd, O.M., Tan, K.B., Yung, G., Xue, S., and Yao, J. (1996) Low power systems for wireless microsensors. Proc. of the International Symposium on Low Power Electronics and Design.*

[4]. *Rabaey, J., Ammer, J., da Silva, Jr J.L., and Patel, D. (2000) Picoradio: Ad hoc wireless networking of ubiquitous low-energy sensor/monitor nodes. Proc. of the IEEE Computer Society Annual Workshop on VLSI.*

[5]. *Kahn, J.M., Katz, R.H., and Pister, K.S.J. (1999) Mobile networking for smart dust. Proc. of the ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom).*

[6]. *Calhoun, B.H., Daly, D.C., Verma, N., Finchelstein, D.F., Wentzloff, D.D., Wang, A., Cho, S.H., and Chandrakasan, A.P. (2005) Design considerations for ultralow energy wireless microsensor nodes. IEEE Transactions on Computers 54*

[7]. *Vijay Garg b M.S. Meitei c S. Raman c A. Kumar c N. Tewari R.K. Ghosh a, Ad hoc networks., 2006.*

[8]. *Wei Ding and et.al. Energy equivalence routing in wireless sensor networks.*

[9]. *Ismail H. Kasimoglui Ian .F. Akyildiz. Wireless sensor and actor: research challenges. (Elsevier) Journal, 2, 2004.*

[10]. *Shih, E., Cho, S.H., Ickes, N., Min, R., Sinha, A., Wang, A., and Chandrakasan, A. (2001) Physical layer driven protocol and algorithm design for energy-efficient wireless sensor networks. Proc. of the 7th Annual International Conference on Mobile Computing and Networking.*

[11]. *Sohrabi, K., Gao, J., Ailawadhi V., and Pottie, G. (2000) Protocols for self-organization of a wireless sensor network. IEEE Personal Communications Magazine 7.*

[12]. *Shih, E., Bahl, P., and Sinclair, M. (2002) Wake-on wireless: An event driven energy saving strategy for battery operated devices. Proc. of the ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom).*

[13]. *Ye,W., Heidemann, J., and Estrin, D. (2004) Medium access control with coordinated adaptive sleeping for wireless sensor networks. IEEE/ACM Transactions on Networking 12.*

[14]. *Mills, K.L. (2007) A brief survey of self-organization in wireless sensor networks. Wireless Communications and Mobile Computing 7*

[15]. *Przydatek, B., Song, D., and Perrig, A. SIA: Secure information aggregation in sensor networks. In Proceedings of the 1st ACM International Conference on Embedded Networked Sensor Systems (SenSys 2003) (Los Angeles, Nov. 5–7). ACM Press, New York, 2003.*

[16]. *Perrig, A., Szewczyk, R., Wen, V., Culler, D., and Tygar, J. SPINS: Security protocols for sensor networks. J.Wireless Nets. 8, 5 (Sept. 2002).*

[17]. *Sensing the World: Challenges on WSNs Válter Rocha 2008*

[18]. *J. M. Kahn, R. H. Katz, and K. S. J. Pister. Mobile Networking for Smart Dust. In MobiCom 99, Seattle, USA, August 1999.*

[19]. *D. Ganesan, B. Krishnamachari, A. Woo, D. Culler, D. Estrin, and S. Wicker. Complex Behavior at Scale: An Experimental Study of Low-Power Wireless Sensor Networks. Technical Report CSD-TR 02-0013, UCLA, February 2002.*

[20]. *N. Glance, D. Snowdon, and J.-L. Meunier. Pollen: using people as a communication medium. Computer Networks, 35(4), 2001.*

[21]. *I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci. Wireless Sensor Networks: A Survey. Computer Networks, 38(4), March 2002.*

[22]. *Hazem M. El-Bakry, and Nikos Mastorakis, "A Perfect QoS Routing Algorithm for Finding the Best Path for Dynamic*

Networks," WSEAS Transactions on Communications, Issue 12, vol. 7, December 2008, pp. 1123-1136.

[23]. Hazem M. El-Bakry, and Nikos Mastorakis, "A Real-Time Intrusion Detection Algorithm for Network Security," WSEAS Transactions on Communications, Issue 12, vol. 7, December 2008, pp. 1222-1234.

[24]. Hazem M. El-Bakry, Alaa M. Riad, Mervat M. Fahmy, and Nikos Mastorakis "Fast Intrusion Detection by using High Speed Focused Time Delay Neural Networks, " Proc. of WSEAS International Conference on Communication and Information, Athens, Greece, December 29-31, 2009, pp.278-295.

[25]. Hazem M. El-Bakry, and Nikos Mastorakis, "Fast Packet Detection by using High Speed Time Delay Neural Networks," Proc. of the 10th WSEAS Int. Conference on MULTIMEDIA SYSTEMS & SIGNAL PROCESSING, Hangzhou University, China, April 11-13, 2010, pp. 222-227.

[26]. Hazem M. El-Bakry, and Mamoon H. Mamoon, "A New Efficient Fast Routing Protocol for MANET," Proc. of Int. Conf. on Applied Informatics and Communications (AIC'10), Taipei, Taiwan, August 20-22, 2010, pp. 443-451.

[27]. Hassan H. Soliman, Hazem M. El-Bakry and, Mona Reda, "Studying the Performance of Transmitting Video Streaming over Computer Networks in Real Time," International Journal of Computer Science and Information Security, vol. 9, no. 11, November, 2011, pp. 90-100.

[28]. H. H. Soliman, Hazem M. El-Bakry and, Mona Reda, "REAL-TIME TRANSMISSION OF VIDEO STREAMING OVER COMPUTER NETWORKS," Mansoura Journal for Computer Science and Information Systems, vol. 6, no. 1, Jan 2012, pp. 7-16.

[29]. Hassan H. Soliman, Hazem M. El-Bakry, and Mona Reda, " Real-Time Transmission of Video Streaming over Computer Networks," Proc. of 11th WSEAS International Conference on Electronics, Hardware, Wireless and Optical Communications (EHAC '12), Cambridge, UK, Feb. 22-27, 2012, pp 51-62.

[30]. Alaa Eissa, Hazem M. El Bakry, Mamoun H. Mamoun, and Samir Zied, "Intrusion Detection In Wireless Sensor Networks: A survey," International Journal of Information Science and Intelligent System, vol. 3, No. 4, October 2014, pp. 87-111

[31]. Alaa Eissa, Hazem M. El Bakry, and Samir Ziad, "A Hybrid Intrusion Detection System for WSN," International Journal of Advanced Research in Computer Science & Technology, vol. 3, issue 4, October-December 2015, pp. 10-15.

[32]. Abdelrahman M. Ahmed, Hazem M. El Bakry, "A New Technique for Optimal Data Manipulation Through WANs," International Journal of Advanced Research in Computer Science & Technology, vol. 4, issue 1, April-June 2016, pp. 177-180.