Middle-East Journal of Scientific Research 23 (7): 1334-1340, 2015
ISSN 1990-9233
© IDOSI Publications, 2015
DOI: 10.5829/idosi.mejsr.2015.23.07.101

Bandwidth Optimization in Wireless Sensor Networks – A Survey

[1]R. Manjuparkavi, [2]A. Ramya, [3]K. Kalaignanam, [4]Dr. P. Sivakumar, [5]A. Kumaresan and [6]Dr. M. Senthil

[1,2 3]Computer Science and Engineering, SKP Engineering College, Tiruvannamalai, Tamil Nadu, India
[4]Electronics and Communication Engineering, SKP Engineering College, Tiruvannamalai, Tamil Nadu, India
[5]Computer Science and Engineering, SKP Engineering College, Tiruvannamalai, Tamil Nadu, India
[6]Computer Science and Engineering,SKP Engineering College, Tiruvannamalai, Tamil Nadu, India

Abstract: In Wireless Sensor Network (WSN), two major challenges are how to conserve the battery power of a sensor and to impose a series of challenges. The intention of this paper is to investigate the bandwidth consumption techniques related issues and challenges. We also discuss the view for ensuring in Wireless Sensor Networks. To overcome the bandwidth consumption in Steiner tree, we proposed a new algorithm called Shortest Best Path Tree based Decentralization Mechanism (SBPTDM) algorithm.

Key words: Wireless Sensor Network (WSN) · Bandwidth Consumption

INTRODUCTION

A typical Wireless Sensor Network structure has four main parts: Sensors – to sense data, Processor – for data processing with memory, Communication hardware – for data communication and Power supply unit. It is shown in Figure 1.

A wireless sensor networks consist of many wireless sensors that collects the data like temperature, light, humidity, pressure and other physical environmental conditions. The information is processed and sent it to the sink [1]. Each node has a battery with limited capacity which is very difficult to recharge and change due to the environment in which they are deployed.

There are different techniques are used to prolong the lifetime of a sensor networks [2]. During network activities, energy efficient is used to reduce energy consumption to minimum. A large amount of energy is consumed by other components also like CPU and radio in the idle state. So, power management schemes are used to switch off the components that are not used. The sensor network also introduces severe resource constraints due to their lack of data storage and power. These represent major obstacles to the implementation of computer security techniques. Our main challenges are to maximize the processing capabilities and reducing bandwidth consumption of the sensor nodes and also secure them against attackers.

1.

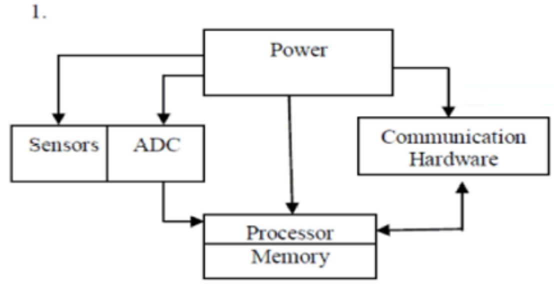

Fig. 1: Structure of Wireless Sensor Networks

In this survey, Bandwidth Optimization or Consumption schemes are explained. This Section highlights some causes of energy loss in Wireless Sensor Networks, discusses the Bandwidth Consumption techniques, security threats and issues in WSN. Finally, we will discuss the conclusion.

Routing Protocol for Wireless Sensor Networks-Survey: In this survey paper presents some recent routing protocols for sensor networks and provides a categorization for many approaches pursued. The three main classifications are explored in this paper there are data-centric protocol, hierarchical protocol and location-based protocol. Each routing protocol is described under the appropriate categories. Moreover, protocols using some methods such as network stream and QoS modeling as well discussed.

Corresponding Author: R. Manjuparkavi, Computer Science and Engineering, SKP Engineering College, Tiruvannamalai, Tamil Nadu, India. E-mail: manjuragu14@gmail.com.

Many new algorithms used for the problem of routing data in wireless sensor networks.

These are the routing types have considered the characteristics of sensor nodes. All of the routing protocols can be categorized as data-centric, hierarchical or location-based protocols although there are a small amount of different ones based on network flow. Data-centric protocols are query-based desired data, which helps in eliminating redundant transmissions. Hierarchical protocol focusing at clustering the nodes to cluster heads can do various aggregation and rejection of data in order to preserve energy. Location-based protocols used to exploit the position information to spread the data to the preferred regions relatively than the entire network. The third type includes routing approaches that are based on common network-flow modeling and protocols that attempt for meeting some QoS requirements beside with the steering function. Using this paper, we will discover the routing mechanisms for sensor network developed in recent years. Every routing procedure is discussed under this proper manner. Our aim is to improve better understanding of the present routing protocols for wireless sensor networks and position exposed open issues that can be focus to further study.In the sector, data-centric routing protocols are covered and summarizes hierarchical routing protocols and Location based routing in sensor networks is going to be discussed.

Data-Centric Protocols: In this protocol, the sink sends queries to certain regions and waits for data from the sensors situated at the preferred regions. Since data is asking through various queries, attribute based naming is essential to identify the properties of data. SPIN [4] is the initial data-centric protocol, which regard as data arbitration between nodes in order to reduce redundant data and accumulate power. Later, aimed at Diffusion [5] has been developed and have grow to be a breakthrough in data-centric routing.

Hierarchical Protocols: Hierarchical routing protocol is to capably sustain the energy consumption of sensor nodes by concerning them in multi hop communication within a exacting cluster and by performing data gathering and merging in order to reduce the amount of transmitted messages to the sink. LEACH [6] is one of the first common hierarchical routing approaches for sensors networks. The new idea planned in LEACH has been an idea for various hierarchical routing protocols [7][8][9][10], We survey hierarchical routing protocols in this section.

Location-Based Protocols: Many of the routing protocols for sensor networks involve location information for sensor nodes. In many cases location information is required in order to compute the detachment between two exacting nodes so that power management must be estimated. Therefore, there is no addressing plan for sensor networks similar to IP-addresses and they are spatially set out on an area, locality information can be utilized in routing data. For example, if the region is to be sensed, by using the location of sensors, the query can be gentle only to that exacting area which will remove the number of transmission considerably.

A Low-Bandwidth Network File System: Wide-area networks or Running network file systems measured more than as the presentation it may be unacceptable and the bandwidth consumption very high. However, remote file access efficiently desirable over the networks—mainly when high latency creates remote login sessions irresponsive. Its relatively running interactive programs such while editors remotely, users can run the programs locally would involve a network file system to facilitate consumes less bandwidth than most existing file systems. LBFS presents a network file organization intended for low-bandwidth networks. LBFS exploits its similarities among files or versions of the identical file to accumulate bandwidth.

It eliminates transfer data over the network when the identical data can existing and be establishing in the server's file structure or the client's cache. By using this technique in conjunction through conventional compression and caching, LBFS uses an order of magnitude lesser bandwidth than classic network file systems on frequent workloads.

LBFS Solution: Using chunks from multiple files on the recipient, LBFS takes a different approach from that of rsync. It consider only for non-overlapping chunks of files and avoids understanding to changing file offsets by setting boundaries of the chunk based upon on file contents, rather than on location inside a file. Insertions and deletions only influence the nearby chunks. Related techniques have been used successfully.

To split up a file into chunks, LBFS examines each (overlapping) 48-byte area of the file and with possibility over each region's contents considers it to be the last part of a data chunk. LBFS selecting these limit regions—called breakpoints— using Rabin fingerprints [11]. A Rabin fingerprint is the polynomial illustration of the data modulo a determined irreducible polynomial. We are using the chose fingerprints as they are efficient

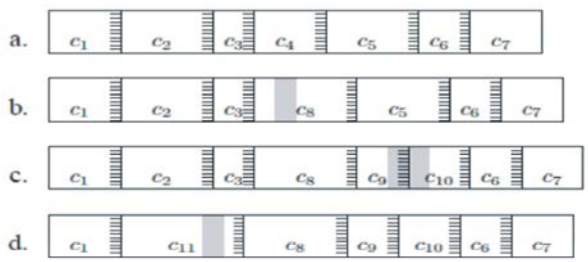

Fig. 1: Chunks of a file before and after various edits. Horizontal stripes show 48-byte regions with magic hash values creating chunk boundaries. Gray shading shows regions of the file that were changed by an edit.

to calculate on a sliding pane in a file. When the low-order 13 bits of a region's fingerprint equal an existing value, the region constitutes a breakpoint. Assuming casual data, the predictable chunk size is 213 = 8192 =8 KBytes (plus the size of the 48-byte breakpoint window).

We experimented with various window sizes and found that 48 bytes provided good results (though the effect of window size was not huge).

Figure 1 shows how LBFS might divide up a file and what happens to chunk boundaries after a series of edits.

It shows the original file, divided into variable length chunks with Breakpoints determined by a hash of each 48-byte region.b. shows the effects of inserting some text into the file. The text is inserted in chunk c4, producing a new, larger chunkc8. However, all other chunks remain the same as previous. Thus, one involves only send c8 to transfer the new file to a recipient.

That already has the old version. Modifying a file can also change the number of chunks. c. shows the effects of inserting data that contains a breakpoint. Bytes are inserted in c5, splitting that chunk into two new chunks c9 and c10. LBFS also uses the recomputed SHA-1 value to detect hash collisions in the database, since the 64-bit keys have a low but non-negligible probability of collision. Not relying on database integrity also frees LBFS from the need to worry about crash recovery. That in turn saves LBFS from making expensive synchronous database updates.

The worst corrupt database can do is degrade performance.

Bandwidth Management: New Use Cases: Since bandwidth is a scarce resource in many Wireless Sensor networks, within a given period of time CSPs may want to control bandwidth of individual subscribers based on how much volume of data they consume. This period of time may be daily, bi-weekly and monthly or based on subscription's period billing cycle). A CSP have to reduce bandwidth if the subscriber has exceeded the data volume usage beyond a threshold for that period. Example would be to reduce the bandwidth by 200Kbits/sec if the data volume has exceeded beyond 2Gbytes during a time of 24-hour period. The bandwidth is returned to the original subscribed value when the period has expired. To handle this use case, the following are the technical requirements for an advanced AAA solution.

AAA SOLUTION: To handle this use case, the following are the technical requirements for an advanced AAA solution. The network elements providing services have to supply the consumed data volume to the AAA server during an on-going client session. The AAA server needs to keep track of the consumed volume by appending up the usage volume numbers provided to it y the network element and maintain that information in real-time user sessions. Thus, session management with tracking of usage is a very basic requirement of a modern AAA solution.

On each Interim or authorization event, the AAA server questioning the policy manager for any action related to a change in bandwidth driven by policy accounting. If the policy manager replies with an action to update subscriber's bandwidth, the AAA carries out that action. A sophisticated policy manager with a rule based engine to specify policy related data on subscriber e.g. subscription details, profiles, bandwidth-quotas and other parameters related to service control, rating/charging etc. is an essential part of today's advanced AAA platforms.

Now, AAA applications need to provide bandwidth management and control capability with several other modules and applications such as to name a few for Policy Managers, Subscriber managers, quota mangers, self-care captive portals.AAA platforms are quickly turning into complete Service Management platforms and must support capability for extensibility, scalability and programmability for realizing advanced business logic and use cases. In this whitepaper we have tried to capture some of the most important use cases business in the context of bandwidth management and the challenges these use cases pose for a modern AAA platform.

Controlling Peer to Peer Bandwidth Consumption: Internet Peer-to-Peer (P2P) is a relatively new technology, which allows the creation of decentralized, logical networks for dynamic and anonymous information switch over the public Internet. As opposed to "traditional" client/server models in which a well-known source provides contented and information's are requesting to clients, Peer-to-Peer applications utilize various techniques to allow users to investigate and distribute information and content involving. There are several different P2P technologies and architectures, central server used to coordinate and conduct searches (e.g., Napster), or those that are completely decentralized in which no central node exists (e.g., Gnutella) and some different levels of interoperability, ranging from application specific P2P networks (e.g., iMesh) to those utilizing an open standard (e.g., Gnutella and OpenNAP).

All of these applications allow individual users (conveniently shielded by the anonymity of the network) to share files over the Internet. These files often contain copyrighted materials (e.g., songs, movies, software, etc.) materials no commercial content provider could legally afford to publish.

The Peer-to-Peer Challenge for Service Providers: While the fame of P2P applications is causing major challenges and issues for the rightful owners of the copyrighted material being freely distributed, they are also creating network capacity and subscriber expectation management problems for Internet service providers. Every IP network is built with assumptions about its usage, which are in turn used to analyze and compute the necessary amount of network capacity and resources needed to support a given client support. This study is necessary for service providers in their attempt to maintain a solid ROI model for their networks and to maintain some level of visibility into their future needs. As P2P applications are different from usual client/server applications in the technique they are used and in turn the way they use the network, In many ways they are, changing the game for service providers trying to architect and maintain their networks.

Evaluation and Characterization of Available Bandwidth Probing Techniques: The packet pairing mechanism has been shown to be flexible technique to determine the bottleneck link capability lying on a network path, but it is used to determine accessible bandwidth is more demanding. Measurements and simulations to develop the communication between probing packets and the opposing the network traffic in this paper. Constructing a simple representation to recognize, how to competing the traffic changes inquiring packet gap. The gap model shows that the early probing gap is a critical factor. To estimate available bandwidth using packet pairs. Based on this, we presenting two available bandwidth measurement techniques, the early gap growing method and the packet transmission rate (PTR).wide-ranging Internet measurements are used to demonstrate that these techniques to estimate available bandwidth closer than obtainable techniques are Path load, with comparable accuracy. Finally, using together Internet capacity and ns simulations, we investigate how the quantity accurateness of active probing is affected by factors are the probing packet size, the duration of probing packet train and the demanding traffic on links further than the tight link.

The available bandwidth defined here, generally, does not equal the achievable bandwidth for an application. Applications often cannot fully utilize the unused bandwidth due to factors such as a small receive socket buffer and reordering the packet, which may limit transmission control protocol (TCP) throughput single-hop gap model. We use this gap model to help understand the interaction between the probing packets and the competing traffic and to identify the conditions under which the packet pair gap can be used to accurately characterize the competing traffic. Second, based on the insights gained from the gap model, we develop two packet pair techniques—initial gap increasing (IGI) and packet transmission rate (PTR)—to characterize the available bandwidth on a network path. The two techniques experimentally determine an initial packet pair gap that will yield a high correlation between the competing traffic throughput on the bottleneck link and the packet gap at the destination

Bandwidth Consumption and Broadband Reliability: The quick growth of Internet-connected procedure in the home is shifting the way broadband services are utilized. In the past few months, the amount of households with four or more devices utilization of the web increased. At the same time, the sum of bandwidth consumption per home is rising and is predictable to rise to four times the present quantity. The growth in mobile, smartphones and tablets are going to characterize the best rising sector of associated devices, more driving the growth of home networking. This improved consumption across many devices creates a new set of test for broadband providers. First, it optimization the cost to set up and sustain these more complex home networks, compared to the classic "one PC" home. Second, it creates contention within the home network for a shared resource of the broadband pipe. At last, it increases on the whole demand for bandwidth, which in turn adds core ability cost to the service provider. It increases the overall require for bandwidth, which in turn adds core capability cost to the service provider finally. The Bandwidth Consumption and Broadband Reliability revise investigated a common issue in the associated home, the supposed "slow connection."

As data stream content and real-time applications become more ordinary in the home network, users have advanced sensitivity to intermittent connectivity, poor video quality and normally issues of slow connection. This section reveals the present state of these issues for the typical broadband user. Reducing Energy utilization and growing Bandwidth on 28-nm FPGAs Lower power utilization and high bandwidth are currently the two leading necessities in designing next-generation high-end applications. Across numerous markets is for higher bandwidth in the similar footprint at the similar or lower power and cost.

The Internet is going for mobile and video is dynamic bandwidth necessities at a development time of 50% year on year. The march to 40G and 100G systems (with 400G on the prospect) is happening to hold this ever-growing bandwidth demand. Fierce rivalry is driving low prices. Space constraints and cooling solutions frequently control the power budget, occasionally it double the power utilization of the electronics. The next generation of 28-nm high end Altera® FPGAs addresses these challenges throughout leading-edge technical modernism, integration and turn down power utilization.

Designing next-generation FPGAs to deal with the present movement of higher bandwidth and lower power is fetching much more demanding. Many factors have to be cautiously measured when planning a new FPGA family to make certain the new devices can deal with the power and performance necessities of the targeted applications in a variety of market segments. These factors include selecting the right process technology, designing the correct architecture, applying the exact software power optimization and enabling easier and power-efficient system-level design. Altera took a holistic approach in scheming Stratix® V FPGAs to deliver the lowest Energy and highest bandwidth FPGAs in the industry. Input innovations were introduced at lots of levels to optimize the Stratix V FPGAs' energy and performance for designers appear to construct a higher bandwidth design while dropping thermal power consumption (Figure 1).

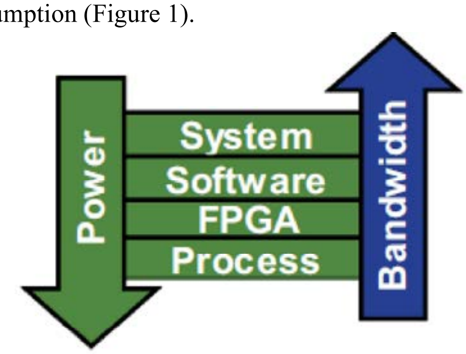

Fig. 1: Altera's Holistic Approach to Reduce Power and Increase Bandwidth

Routing Techniques in Wireless Sensor Networks: A Wireless Sensor Networks (WSNs) consist of little nodes with computing, sensing and wireless communications capabilities. Many routing, Energy organization and data dissemination protocols have been purposely planned for WSNs where energy consciousness is an essential design issue. The focus though, it has been known to the routing protocols which may vary depending on the application and network structural design. This paper, we are presenting a review of the state-of-the-art routing methods in WSNs. First we summarize the design challenges for routing protocols in WSNs pursue by a broad review of different routing techniques. on the whole, the routing methods are divided into three categories based on the core network structure: at, hierarchical and location-based routing. These protocols can be divided into multipath-based, negotiation-based, QoS-based and coherent-based depending on the protocol evolution. We were probing the design tradeoffs between energy and message overhead reserves in every routing paradigm. Some of the routing challenges and design issues that influence routing process in WSNs. Node employment: Node employment in WSNs is application reliant and affects the presentation of the routing protocol. The utilization can be either deterministic or randomized. In deterministic employment, the sensors are physically located and data is routed throughout pre-determined paths. Still, in random node employment, the sensor nodes are spread at random creating an infrastructure in an ad hoc mode. If the resulting allotment of nodes is not uniform, best clustering becomes essential to permit connectivity and allow energy efficient network action. Inter-sensor communication is in general within short transmission ranges suitable to energy and bandwidth boundaries. So, it is possible that route will consist of many wireless hops.

Node/connection Heterogeneity: In several studies, all sensor nodes were implicit to be homogeneous, i.e., having equal ability in terms of calculation, communication and power. Though, depending on the purpose of a sensor node can have dissimilar role or ability. The survival of heterogeneous deposit of sensors increases many technical issues connected to data routing. For example, some applications capacity need a dissimilar combination of sensors for monitoring high temperature, difficulty and humidity of the contiguous environment, detecting movement via acoustic signatures and securing the image or video tracking of affecting objects. These special sensors are able to be either deployed independently or the special functionalities can be included in the identical sensor nodes. Still data reading and reporting can be generated from these sensors at unlike rates, focus to varied quality of service constraints and can pursue multiple data coverage models. For example, hierarchical protocols select a cluster-head node unlike from the standard sensors. These cluster-heads can be preferred from the deployed sensors or can be more powerful than other sensor nodes. Hence, the load of communication to the BS is handled by the set of cluster-heads.

Network Dynamics: Most of the network architectures suppose that sensor nodes are immobile. Though, mobility of either BS's or sensor nodes at times of necessary in many applications. Routing messages establishment or to moving nodes is new demanding since route stability becomes a vital issue, in addition to energy, bandwidth etc. Furthermore, the sensed occurrence can be either dynamic or motionless depending on the purpose, e.g., it is dynamic in a goal finding/tracking application, while it is static in jungle monitoring for early on fire avoidance. Monitoring static actions allows the network to work in an immediate mode, simply generating traffic when reporting. Dynamic actions in mainly applications require periodic reporting and therefore cause major traffic to be routed to the BS.

Information-driven antenna querying and forced anisotropic diffusion routing: Two routing techniques, namely, information-driven antenna querying and constrained anisotropic diffusion routing were proposed in [12] aims to be general form of directed diffusion. The idea is to query sensors and path data in the network hence the information develop is maximized whereas latency and bandwidth are minimized. It diffuses queries by by means of a set of information criteria to choose which sensors can obtain the data. This is done by activating only the sensors that are secure to a exacting event and vigorously adjusting data routes. The main variation from directed diffusion is the concern of information gain in totaling to the communication cost. In this method, each node estimates an information/cost objective and routes data based on the limited information/cost slope and end-user necessities. Evaluation theory was used to model information function measure. In Information-driven antenna querying, the querying node can found which node can supply the most useful information with the supplementary advantage of the energy cost. Conversely, does not purposely identify how the query and the information are routed between sensors and the BS. It can be seen as a corresponding optimization formula. Replication results show that these approaches are more energy-efficient than bound for diffusion where queries are diffused in an isotropic approach and getting nearest neighbors first.

Power-Efficient assembly in Sensor Information Systems (PEASIS): In [13] a development over LEACH protocol was proposed. The procedure, called Power-Efficient Gather in Sensor Information Systems (PEASIS), is a near best chain-based protocol. The fundamental idea of the protocol is that in order to enlarge network lifetime, nodes require only correspond with their nearby neighbors and they take turns in communicate with the base-station. A new surrounding will begin when the surrounding of all nodes communicating with the base-station ends and so on. This reduces the power essential to broadcast data per round as the power challenging is spread regularly over all nodes.

Hence, PEASIS has two major objectives. First, rise the time of each node by using mutual techniques and as a result the network time will be increased. Second, permit only local organization among nodes that are close collectively so that the bandwidth extreme in communication is concentrated. Unlike LEACH, PEASIS avoids cluster arrangement and uses only one node in a chain to send out to the BS as an alternative of using multiple nodes.

Table 1: Comparing the Bandwidth consumption techniques

Sl.no	*Bandwidth consumption techniques*	*Security*	*Bandwidth Consumption*	*Energy saving*	*Time consumption*
1	*Data centric,Hierarchal, Location based protocols*	Very high	Very high	Very less	Very high
2	*LBFS Solution*	High	high	*less*	high
3	*AAA Solution*	Comparatively less	Comparatively less	Comparatively High	Comparatively less
4	*Peer-to-Peer*	High	High	High	less
5	*STDM*	Less	Less	Very high	*Very less*
6	*SBPTDM*	*Very less*	*Very less*	*High*	*Very less*

CONCLUSION

The Steiner tree structure of the network results in minimum number of nodes for data transmission and the decentralization mechanism protects the data against privacy attacks. Thus, we enhance the security of the WSN. To overcome the disadvantage of the Steiner tree, we proposed work called Shortest Best Path Tree based decentralization mechanism (SBPTDM).

REFERENCES

1. Amirthavalli, K. and Dr. P. Sivakumar, 2014. Power Conservation and Security in Wireless Sensor Networks-A Survey in 2014 International Conference on Electronics and Communication Systems (ICECS -2014), Feb. 13 –14, 2014, Coimbatore, India.
2. Akyildiz, I.F., W. Su, Y. Sankarasubramaniam and E. Cayirci, 2002. “Wireless Sensor Networks: A Survey”, Computer Networks, Volume 38, No. 4, March 2002.
3. Culler, D.E. and W. Hong, “Wireless Sensor Networks”, Communication of the ACM.
4. Heinzelman, W., J. Kulik and H. Balakrishnan, 1999. “Adaptive protocols for information dissemination in wireless sensor networks,” in the Proceedings of the 5th Annual ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom’99), Seattle, WA, August 1999.
5. Intanagonwiwat, C., R. Govindan and D. Estrin, 2000. "Directed diffusion: A scalable and robust communication paradigm for sensor networks", in the Proceedings of the 6th Annual ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom'00), Boston, MA, August 2000.
6. Heinzelman, W., A. Chandrakasan and H. Balakrishnan, 2000. "Energy-efficient communication protocol for wireless sensor networks," in the Proceeding of the Hawaii International Conference System Sciences, Hawaii, January 2000.
7. Manjeshwar, A. and D.P. Agrawal, 2001. “TEEN: A Protocol for Enhanced Efficiency in Wireless Sensor Networks”, in the Proceedings of the 1st International Workshop on Parallel and Distributed Computing Issues in Wireless Networks and Mobile Computing, San Francisco, CA, April 2001.
8. Lindsey, S. and C.S. Raghavendra, 2002. "PEGASIS: Power Efficient Gathering in Sensor Information Systems," in the Proceedings of the IEEE Aerospace Conference, Big Sky, Montana, March 2002.
9. Lindsey, S., C.S. Raghavendra and K. Sivalingam, 2001. "Data Gathering in Sensor Networks using the Energy*Delay Metric", in the Proceedings of the IPDPS Workshop on Issues in Wireless Networks and Mobile Computing, San Francisco, CA, April 2001.
10. Manjeshwar, A. and D.P. Agrawal, 2002. "APTEEN: A Hybrid Protocol for Efficient Routing and Comprehensive Information Retrieval in Wireless Sensor Networks," in the Proceedings of the 2nd International Workshop on Parallel and Distributed Computing Issues in Wireless Networks and Mobile computing, Ft. Lauderdale, FL, April 2002.
11. Michael O. Rabin, 1981. Fingerprinting by random polynomials.Technical Report TR-15-81, Center for Research in Computing Technology, Harvard University.
12. Chu, M., H. Haussecker and F. Zhao, 2002. Scalable Information-Driven Sensor Querying and Routing for ad hoc Heterogeneous Sensor Networks," The International Journal of High Performance Computing Applications, Vol. 16, No. 3, August 2002.
13. Lindsey, S. and C. Raghavendra, 2002. PEGASIS: Power-Efficient Gathering in Sensor Information Systems", IEEE Aerospace Conference Proceedings, Vol. 3, 9-16 pp: 1125-1130.