Volume: 09 Issue: 01 Pages: 3321-3328 (2017) ISSN: 0975-0290

Research Challenges and Characteristic Features in Wireless Sensor Networks

Rajkumar
Sambhram Institute of Technology, Bangalore, VTU Belagavi Karnataka, India
Email: pyage2005@gmail.com
Dr H G Chandrakanth
Sambhram Institute of Technology, Bangalore, VTU Belagavi Karnataka, India
Email: ckgowda@hotmail.com
Dr D G Anand
Rajiv Gandhi Institute of Technology, VTU Belagavi Karnataka, India
Email: dg_anand2003@sifymail.com
Dr T John Peter
Sambhram Institute of Technology, Bangalore, VTU Belagavi Karnataka, India
Email: tjpeter.cse@gmail.com

ABSTRACT

Wireless Sensor Networks have come to the forefront of the scientific community recently and it consists of small nodes with sensing, Communications and computing capabilities. The Wireless Sensor Network Systems can be applied to monitor different environments ranging from military to civil applications. It is observed that different protocols necessary for smooth functioning of the network system are highly application specific. Current WSNs typically communicate directly with a centralized controller or satellite. In this paper we survey the different research challenges in Wireless Sensor Networks and purpose of various research Challenges activities is the development of a framework, which is radically simplifies the development of software for sensor network applications and characteristic Features of Sensor Networks.

Index Terms - Wireless Sensor Network, Research Challenge, Characteristic Features.

Date of Submission: Jun 29, 2017 Date of Acceptance: Jul 8, 2017

1 INTRODUCTION

Wireless Sensor Networks have recently emerged as a premier research area. They have great long term economic potential, capability to transform our lives, and pose many latest system-building challenges. Sensor networks also pose a number of latest abstract and optimization problems, some of these such as tracking, location and exploitation are most important issues, in that several applications rely on them for necessary information. Coverage in general, answers the questions about quality of service that can be provided by a particular sensor network. The integration of various types of sensors such as acoustic, seismic, optical, etc. in one network platform and the study of the overall coverage of the system also presents numerous interesting challenges.

Wireless sensors have become an excellent tool for military applications relating intrusion detection, perimeter monitoring, and information gathering and elegant logistics support in an unidentified deployed area. Some additional applications: location detection, sensor-based personal health monitor with sensor networks and movement detection [1].

Sensor networks have different constraints than traditional wired networks. Primary, the nodes in sensor networks are likely to be battery powered, and it is often very complicated to change the batteries for all of the nodes, as energy conserving forms of communication and computation are necessary to wireless sensor networks. Second, since sensors have restricted computing power, they may not be able to run complicated network protocols. Third the nodes deployed may be either in a controlled environment where monitoring, preservation and surveillance are very difficult. Finally in the uncontrolled environments, security for sensor networks becomes extremely difficult.

2 RESEARCH CHALLENGES

The severe constraints and challenging deployment environments of wireless sensor networks build computer security for these systems additional challenging than for conservative networks. However, several properties of sensor networks may help address the challenge of building protected networks. Primarily, we have the possibility to architect security solutions into these systems from the outset, they are still in their early design and research stages. Second, numerous applications are possible to involve the deployment of sensor networks under a single managerial area, simplifying the threat model. Third, it may be possible to build up redundancy, scale, and the physical character of the environment in the solutions. If we build sensor networks so they maintain operating even if some fraction of their sensors is compromised, we have an possibility to use redundant sensors to resist additional attack. The single aspects of sensor networks may permit novel defenses not available in conventional networks. Various other problems also need further research. Single is how to protect wireless communication links against eavesdropping, denial of service, tampering, and traffic analysis. Others involve

Volume: 09 Issue: 01 Pages: 3321-3328 (2017) ISSN: 0975-0290

provide constraints. Ongoing directions hold asymmetric protocols where most of the computational load falls on the base station and on public-key cryptosystems efficient on low end devices. Lastly finding ways to tolerate the lack of physical security, possibly through redundancy about the physical environment, determination remain a continuing overall challenge. We are optimistic that much upgrading will be made on all of them [2].

2.1 Challenges in real time

WSN deals with real world environments. In various cases, sensor data must be delivered within time constraints so that suitable observations can be made or actions taken. Few results exist to date regarding gathering real-time requirements in WSN. Most protocols either ignore real-time or simply attempt to process as fast as possible and expect that this speed is sufficient to meet deadlines. Some preliminary results exist for real-time routing. For example, the RAP protocol [3] proposes a new strategy 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 planned for communication 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 [4]. This protocol uses feedback control to assurance that every node maintains an average delay for packets transiting a node. Given this delay and the distance to travel (in hops), it can be determined if a packet meets its deadline (in steady state). However, transient performance, message losses, congestion, noise and other harms cause these guarantees to be limited. To date, the limited results that have appeared for WSN concerning real-time issues has been in routing. Various other functions must also meet real-time constraints including: data fusion, data transmission, target and event detection and classification, query processing, and security. New results are needed to guarantee soft real time requirements and that deal with the realities of WSN such as lost messages, noise and congestion. Using feedback control to address both steady state and transient behavior seems to hold promise. Dealing with real-time usually identifies the need for differentiated services, e.g., routing solutions need to support different classes of traffic; guarantees for the important traffic and less support for unimportant traffic. It is important not only to develop real-time protocols for WSN, but associated analysis techniques must also be developed.

2.2 Challenges in Real-world Protocols:

Current WSN solutions are developed with simplifying assumptions about environment and wireless communication, even though the realities of environmental and wireless communication sensing are well identified. Many of these solutions work very well in simulation. It is either unidentified how the solutions work in the real world or they can be given away to work poorly in practice. We note that, in general, there is an excellent understanding of both the theoretical and practical issues related to wireless communication. Example, it is well identified how the signal strength drops over distance. Effects of signal reflection, fading and scattering are understood. However, when building an actual WSN, various specific system, cost, and application issues also affect the communication properties of the system. Radio communication in the form of FM or AM broadcast from towers performs quite differently than short range, low power wireless found in self-organizing WSNs. Of course, while the similar basic principles apply, the system performance characteristics vary considerably. In other words, the power, size, cost constraints and their tradeoffs are fundamental constraints. In the current state of the art, the tradeoff among these constraints has produced a number of devices currently being used in WSNs. Example, one such device is the Mica mote that uses 2 AA batteries, an RF Chipcon radio, a 7 MHz microcontroller, and costs about $100. As improved batteries, microcontrollers, and radios become available and as costs reduce, new platforms will be developed. These new platforms will continue to have tradeoffs between these parameters. Novel network protocols that account for the key realities in wireless communication are required.

New research is needed:

- To evaluate and Measure how the theoretical properties of wireless communication are exhibited in today's and tomorrow's sensing and communication devices,
- Establish improved models of communication realities to feed back into improved simulation tools,
- A new network protocols that account for the communication realities of real world environments,
- Test the individual solutions on real platforms in real world settings,
- Synthesize novel solutions into a complete system-wide protocol stack for a real application.

2.3 Challenges in power managements:

Low-cost deployment is one acclaimed benefit of sensor networks. Limited processor bandwidth and small memory are two arguable constraints in sensor networks, which will vanish with the development of fabrication techniques. However, the energy constraint is improbable to be solved soon due to slow progress in developing battery capacity. Furthermore, the untended nature of sensor nodes and hazardous sensing environments preclude battery replacement as a feasible solution. Alternatively, the surveillance nature of many sensor network applications requires a long lifetime; therefore, it is a extremely important research issue to provide a form of energy-efficient surveillance service for a geographic area. Much of the current research focuses on how to provide full or partial sensing coverage in the context of energy conservation. In an approach, nodes are put into a dormant state extended as their neighbors can offer sensing coverage for them. These solutions observe the sensing coverage to a certain geographic area, either it provides coverage or not. However, we argue that, in the

Volume: 09 Issue: 01 Pages: 3321-3328 (2017) ISSN: 0975-0290

majority scenarios such as battlefields there are convinced geographic sections such as the general command center that are much extra security sensitive than others. Based on the reality that individual sensor nodes are not reliable and subject to failure and single sensing readings can be easily distorted by cause background noise and false alarms, it is simply not enough to rely on a single sensor to safeguard a critical area. In this case, it is desired to supply higher degree of coverage in which multiple sensors monitor the same location at the same time in order to obtain high confidence in detection. Alternatively, it is overkill and energy consuming to support the same high degree of coverage for some non-critical area. Middleware sits between the operating system and the application. On traditional desktop computers and portable computing devices, operating systems are well established, both in conditions of systems and functionality. For sensor nodes, however, the recognition and implementation of appropriate operating system primitives is still a research issue [5]. In various current projects, applications are executing on the bare hardware without a separate operating system part. Hence, at this early phase of WSN technology it is not clear on which basis future middleware for WSN can naturally built.

2.4 Challenges in Programming Abstractions:

A key to the development of WSN is raising the level of abstraction for programmers. At present, programmers contract with too various low levels details regarding sensing and node to node communication. For example, they characteristically deal with, fusing data, moving data and sensing data. They deal with demanding node to node communication and particulars. If we raise the level of concept to consider aggregate performance, application functionality and direct support for scaling issues then efficiency increases. Present research in programming abstractions for WSN can be categorized into 7(Seven) areas:, component-based, database centric, virtual machines, event based, scripts, environmental and middleware APIs. For example, consider an environmental based abstraction called Enviro Track [6]. Here the programmer deals with entities establish in an application. If the application tracks vehicles and people, then the programmer can define vehicle and people entities and use library routines that support low level sensing functions that can detect and classify items of these types. They can also easily identify the application level processing associated with each type of entity. This allows programmers to contract with application level functionality rather than low level details. Since WSN contract primarily with collecting, acting and analyzing on data, a database vision of such systems is accepted. In this view, a programmer deals with queries written in an SQL-like format. However, real-world data issues such various levels of confidence in data, as probabilistic data and missing or late data sometimes make the SQL paradigm inadequate. It is possible that no one programming abstraction for WSN will exist. Rather, a number of solutions will emerge, each improved for certain domains. Results in this area are critical in order to enlarge the development of WSN by the general programmer as opposed to the WSN.

2.5 Challenges in Security and Privacy:

WSN are limited in their computation, communication capabilities, and energy. In contrast to traditional networks, sensor nodes are frequently deployed in accessible areas, presenting a threat of physical attacks. Sensor networks interrelate closely with their physical environment and with people, posing extra security problems. Because of these reasons existing security mechanisms are inadequate for WSN. These new constraints pretense new research challenges on key establishment, secrecy and authentication, robustness to denial-of-service attacks, privacy, node capture, and secure routing. To achieve a protected system, security must be included into every component, as a components designed without security can become a point of attack. Therefore, security and privacy pervade every feature of system design. Consider one of the most difficult attacks to protect against. Adversaries can severely limit the cost of a wireless sensor network by denial-of-service attacks [7]. In the simplest form of denial-of service attack, an adversary attempts to disturb an operation by broadcasting a high-energy signal. If the transmission is strong sufficient, the whole system could be jammed. Additional sophisticated attacks are also possible: the adversary can inhibit communication by violating the Message Authentication Control (MAC) protocol, for occurrence by transmitting while a neighbor is also transmitting requesting channel access with a Request-To-Send (RTS). New techniques for dealing with this easy yet potentially devastating attack are needed. Various other security related problems need further research [8]. One challenge is how to safe wireless communication links against tampering and eavesdropping. Overall, security is a difficult challenge for any system. The severe demanding and constraints environments of WSN make computer security for these systems even more challenging.

2.6 Challenges in Analysis:

Few investigative results exist for WSN. Since WSN are in the early stage of growth it is not surprising that few investigative results exist. Researchers are busy inventing new applications and new protocols for WSN. The solutions are built, tested and evaluated either by test beds or simulation; sometimes an actual system has been deployed. Empirical confirmation is beginning to accumulate. However, a more scientific approach is necessary where a system can be analyzed and designed before it is deployed. The analysis needs to offer confidence that the system will meet its necessities and to indicate the performance and efficiency of the system. Consider the following motivating analysis questions. What density of nodes is necessary to meet the lifetime requirements of the system? What communication and sensing ranges are needed to detect report and classify a target to a base station by a deadline? What is sensing range and what is nodes need to be awake in order to assurance a certain degree of sensing coverage for a

Volume: 09 Issue: 01 Pages: 3321-3328 (2017) ISSN: 0975-0290

system? Given *n* streams of periodic sensing traffic characterized by a message size, start time, period, deadline, source location and destination location for a known WSN will all the traffic meet their deadlines? To answer this final question, the interference patterns of wireless communication must be taken in an account. An analysis techniques and solutions are developed for these types of questions; they must also be validated with actual systems.

2.7 Scope and Functionality:

The key purpose of middleware for sensor networks is to support the development, execution, deployment, and maintenance of sensing-based applications. This includes mechanisms for formulating complex sophisticated sensing tasks, communicating this task to WSN, management of sensor nodes to divide the task and distribute to the individual sensor nodes, data fusion for integration the sensor readings of the individual sensor nodes into a high-level result, and reporting the result back to the job issuer. Moreover, appropriate mechanisms and abstractions for dealing with the heterogeneity of sensor nodes must be provided. All mechanisms provided by a middleware system should respect the design values sketched above and the special characteristics of the WSN, which mostly boils down to energy efficiency, scalability and robustness. The scope of middleware for WSN is not limited to the sensor network only, but also covers devices and networks connected to the WSN. Classical infrastructures and mechanisms are typically not well suited for interaction with WSN. Single reason for this are the limited resources of a WSN, which may make it required to execute resource intensive functions or store huge amounts of data in external components. This may result in a secure interaction of processes executing in a traditional network and the WSN. One example of such "outer" functionality is called virtual counterparts, mechanism residing in the Internet which supplement real world objects with information-processing capabilities [9]. Thus, middleware for sensor networks should supply a holistic view on both traditional networks and WSN, which is a challenge for architectural design and implementation. Another single property of middleware for WSN is imposed by the design principle application information in nodes. Traditional middleware is designed to accommodate a extensive variety of applications without necessarily needing application information. Middleware for WSN, however, has to provide mechanisms for injecting application information into the infrastructure and the WSN. Data-centric communication mandates a communication paradigm which extra closely resembles content-based messaging systems than traditional RPC-style communication. Moreover, event based communication matches the characteristics of the WSN much improved than traditional request-reply schemes. In general, application and communication specific data processing is more integrated in WSN middleware than in traditional systems. The design principle adaptive fidelity algorithms requires the infrastructure to provide suitable mechanisms for selecting parameters or complete algorithms which solve a certain problem with the most excellent quality under given resource constraints.

2.8 Physical Layer Secure Access:

Physical layer secure access in wireless sensor networks may very well be offered by using frequency hopping. A dynamic mixture of the parameters like hopping set (available frequencies for hopping), dwell time (interval per hop) and hopping pattern (the sequence in which the frequencies in the available hopping set is used) could be combined with a little expense of memory, processing and resources. Important points in physical layer secure access will be the efficient design in order that the hopping sequence is modified in less time than is required to discover it and for employing this both sender and receiver should maintain a synchronized clock. A scheme as proposed in may be utilized which introduces secure physical layer access employing the singular vectors while using channel synthesized modulation. Attacks against wireless sensor networks may very well be broadly considered from two different levels of views. One is the attack from the security mechanisms and this band are brilliant from the basic mechanisms (like routing mechanisms). Ideas signalize the most important attacks in wireless sensor networks [27].

2.9 Localization:

It is amongst the key techniques in wireless sensor network. The place estimation method is usually classified into Target / source localization and node self-localization. In target localization, we mainly introduce the energy-based method. Then we investigate the node self-localization methods. Considering that the widespread adoption on the wireless sensor network, the localization methods are wide and varied in several applications. There are some challenges using some special scenarios. With this paper, we present a wide survey these challenges: localization in non-line-of-sight, node selection criteria for localization in energy-constrained network, scheduling the sensor node to optimize the tradeoff between localization performance and energy consumption, cooperative node localization, and localization algorithm in heterogeneous network. Finally, we introduce the evaluation criteria for localization in wireless sensor network. The entire process of estimating the unknown node position inside the network is known as node self-localization. And WSN comprises a large number of inexpensive nodes which are densely deployed in a very region of interests to measure certain phenomenon. The leading objective would be to determine the location of the target [28]. Localization is significant travelers have an uncertainty with the exact location of some fixed or mobile devices. One example has been in the supervision of humidity and temperature in forests and/or fields, where thousands of sensors are deployed by way of plane, giving the operator minimal possible ways to influence may location of node. An efficient localization algorithm might utilize all the free information from the wireless sensor nodes to infer the positioning of the individual devices. Another application

Volume: 09 Issue: 01 Pages: 3321-3328 (2017) ISSN: 0975-0290

will be the positioning of an mobile robot determined by received signal strength from your number of radio beacons placed at known locations around the factory floor. The primary function of an location estimation method to calculate the geographic coordinates of network nodes with unknown position in the deployment area. Localization in wireless sensor networks is the process of determining the geographical positions of sensors. Only a number of the sensors (anchors) inside the networks have prior knowledge about their geographical positions. Localization algorithms utilize location information of anchors and estimates of distances between neighboring nodes to discover the positions in the rest of the sensors [29].

3 CHARACTERISTIC FEATURES OF SENSOR NETWORKS

In ad-hoc networks, wireless nodes self-organize into infrastructure less network with a dynamic topology. Sensor networks distribute these traits, but also have numerous distinguishing features. The number of nodes in a characteristic sensor network is much higher than in a typical ad-hoc network, and dense deployments are frequently desired to ensure connectivity and coverage: for these reasons, sensor network hardware must be cheap. Nodes classically have stringent energy limitations, which create them more failure-prone. They are normally assumed to be stationary, but their relatively common breakdowns and the volatile nature of the wireless channel nonetheless result in a variable network topology. The sensor network hardware should be small, reliable, inexpensive and power-efficient in order to maximize network lifetime, facilitate data collection, add flexibility and minimize the need for maintenance.

3.1 Lifetime:

Network lifetime is extremely critical for most applications, and its main limiting factor is the energy consumption of the nodes, it requires being self-powering. Although it is frequently assumed that the transmit power related with packet transmission accounts for the lion's share of sensing, power consumption, signal processing and even hardware operation in standby manner consume a consistent amount of power as well [10], [11]. In some applications, additional power is needed for macro-scale actuation. Many researchers recommend that energy consumption could be reduced by considering the presented interdependencies between individual layers in the network protocol stack. Channel access protocols and Routing, for instance, could greatly advantage from an information exchange with the physical layer. At the physical layer, benefits can be obtained with dynamic modulation scaling and lower radio duty cycles (varying the constellation size to minimize energy expenditure [12]). Using low-power mode for the processor or disabling the radio is generally beneficial, even though periodically turning a subsystem on and off may be more expensive than always keeping it on. Techniques aimed at reducing the idle mode leakage current in CMOS-based processors are also noteworthy [13]. MAC (Medium Access Control) solutions have a direct impact on energy consumption, as some of the main causes of energy waste are found at the MAC layer: control packet overhead, collisions, and idle listening. The power saving forward error control techniques is not easy to implement due to the high amount of computing power that they need, the fact that extensive packets are normally not practical. Energy-efficient routing should avoid the loss of a node due to battery depletion. Numerous proposed protocols tend to minimize energy consumption on forwarding paths, but if some nodes happen to be situated on the most forwarding paths (close to the base station), their lifetime will be reduced.

3.2 Flexibility:

The Sensor networks should be scalable and they should be able to dynamically adapt to changes in topology and node density, like in the case of the self-healing minefields. In surveillance applications, the majority of nodes may remain quiescent as long as not anything interesting happens. However, they must be able to respond to special actions that the network intends to study with a few degree of granularity. In a self-healing minefield, a number of sensing mines may sleep as long as nothing of their peers explodes, but need to rapidly become operational in the case of an enemy attack. Response time is also very critical in control applications (sensor/actuator networks) in which the network is to present a delay-guaranteed service. Unmetered systems need to self-configure and adapt to different conditions. Sensor networks should also be robust to changes in topology, for instance due to the failure of particular nodes. In particular, coverage and connectivity should for all time be guaranteed. Connectivity is achieved if the base station can be reached from any node. Coverage can be seen as a measure of quality of service in a sensor network [14], as it defines how well a particular area can be observed by its characterize and network the probability of detection of geographically constrained phenomena or events. Whole coverage is particularly important for surveillance applications.

3.3 Maintenance:

The maintenance in a sensor network is the partial or complete update of the program code in the sensor nodes over the wireless channel. All sensor nodes should be reorganized, and the restrictions on the size of the new code should be the similar as in the case of wired programming. The portion of code for all the time running in the node to guarantee reprogramming support should have a little footprint, and updating actions should only cause a brief interruption of the normal operation of the node [15]. The performance of the network as a whole should not be endangered by unavoidable failures of single nodes, which may happen for a number of reasons, from battery depletion to unpredictable exterior events, and may either be independent or spatially correlated [16]. Fault tolerance is mainly crucial as ongoing maintenance is

Volume: 09 Issue: 01 Pages: 3321-3328 (2017) ISSN: 0975-0290

rarely an choice in sensor network applications. Self-configuring nodes are necessary to allow the deployment process to run easily without human interaction, which in principle be limited to placing nodes into a specified geographical area. It is not desirable to have humans organize nodes for destructively interfere and habitat monitoring with wildlife in the process, or configure nodes for urban warfare monitoring in a hostile environment. The nodes should be able to review the quality of the network deployment and indicate any problems that may happen, as well as adjust to changing environmental situation by automatic reconfiguration. Position awareness is important for self configuration and has specific advantages in terms of routing [17] and security. Time synchronization [18] is advantageous in promoting cooperation among nodes, such as channel access, data fusion, coordination of sleep mode, or security-related interaction.

3.4 Data Collection:

Data collection is associated to network coverage and connectivity. An interesting solution is the use of ubiquitous mobile agents that arbitrarily move around to gather data bridging access points and sensor nodes, whimsically named data MULEs (Mobile Ubiquitous LAN Extensions) in [19]. The predictable mobility of the data sink can be used to save power [20], as nodes can learn its schedule. A similar idea has been implemented in Intel's Wireless Vineyard. It is frequently the case that all data are relayed to a base station, but this form of centralized data collection may shorten network lifetime. Relaying data to a data sink causes non-uniform power utilization patterns that may overburden forwarding nodes [21]. This is particularly harsh on nodes providing end links to base stations, which may finish up relaying traffic coming from all other nodes, thus forming a critical bottleneck for network throughput [22], [23]. An interesting technique is clustering [24], nodes team up to form transmits and cluster their information to their cluster heads, which fuse the data and forward it to a sink. Fewer packets are transmitted, and a consistent energy consumption pattern may be achieved by periodic re-clustering. Data redundancy is a minimized, as the aggregation method fuses strongly correlated measurements. Several applications require that queries be sent to sensing nodes. This is true, for example, when a goal is gathering data regarding a particular area where various sensors have been deployed. This is the justification behind looking at a sensor network as a database [25]. A sensor network should be able to protect itself and its data from external attacks, but the severe limitations of lower-end sensor node hardware make security a correct challenge. Typical encryption schemes, for example, need large amounts of memory that are unavailable in sensor nodes. Data confidentiality should be preserved by encrypting data with a secret key shared with the intended receiver. Data integrity should be ensured to avoid unauthorized data alteration. An authenticated broadcast must permit the verification of the legitimacy of data and their sender. In a number of commercial applications, a serious disservice to the user of a sensor network is compromising data accessibility (denial of service), which can be achieved by sleep-deprivation torture [26]: batteries may be drained by nonstop service requests or demands for legitimate but intensive tasks, preventing the node from incoming sleep mode.

4 CONCLUSION

This paper provides different research challenges areas in academia, industry and government. Research into exact location techniques, free of infrastructure, will translate into greater ease of installation and usefulness of sensor data. Paramount to the success of the wireless sensor network concept is achieving unprecedented end-to-end energy efficiency across all layers of the system architecture. While many challenges lie ahead, there are great opportunities for those who share the vision to bring this concept to fruition and characteristic features of sensor networks

REFERENCES

[1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A survey on sensor networks", IEEE Communications Magazine, Vol. 40, No. 8, pp. 102-114, August 2002.

[2] M. Haenggi, "Opportunities and Challenges in Wireless Sensor Networks," in Handbook of Sensor Networks: Compact Wireless and Wired Sensing Systems, M. Ilyas and I. Mahgoub, eds., Boca Raton, FL, pp. 1.1–1.14, CRC Press, 2004.

[3] C. Lu, B. Blum, T. Abdelzaher, J. Stankovic, and T. He, RAP: A Real-Time Communication Architecture for Large-Scale Wireless Sensor Networks, RTAS, June 2002.

[4] T. He, J. Stankovic, C. Lu, and T. Abdelzaher, SPEED: A Stateless Protocol for Real-Time Communication in Ad Hoc Sensor Networks, IEEE ICDCS, May 2003.

[5] R. Bronson and G. Naadimuthu, Operations Research, 2 ed., Schaum's Outlines, McGraw Hill, New York, 1997.

[6] Wood, A., Stankovic, J., and Son, S. JAM: A mapping service for jammed regions in sensor networks. In Proceedings of the IEEE Real-Time Systems Symposium (Cancun, Mexico, Dec. 3–5, 2003).

[7] A. Wood and J. Stankovic, Denial of Service in Sensor Networks, IEEE Computer, Vol. 35, No. 10, October 2002, pp. 54-62.

[8] A. Perrig, J. Stankovic, and D. Wagner, Security in Wireless Sensor Networks, invited paper, CACM, Vol. 47, No.6, June 2004, pp. 53-57.

Volume: 09 Issue: 01 Pages: 3321-3328 (2017) ISSN: 0975-0290

[9] T.-S. Chen, C.-Y. Chang, and J.-P. Sheu, "Efficient pathbased multicast in wormhole-routed mesh networks," J. Sys. Architecture, vol. 46, pp. 919-930, 2000.

[10] A. Goldsmith and S. Wicker, "Design challenges for energy-constrained ad hoc wireless networks," IEEE Wireless Communications Magazine, vol. 9, pp. 8–27, Aug. 2002.

[11] L. Yuan and G. Qu, "Energy-efficient Design of Distributed Sensor Networks," in Handbook of Sensor Networks: Compact Wireless and Wired Sensing Systems, M. Ilyas and I. Mahgoub, eds., Boca Raton, FL,pp. 38.1–38.19, CRC Press, 2004.

[12] C. Schurgers, O. Aberthorne, and M. Srivastava, "Modulation scaling for energy aware communication systems," in Proceedings of the 2001 International Symposium on Low Power Electronics and Design, Huntington Beach, CA, pp. 96–99, Aug. 2001.

[13] A.P. Chandrakasan, R. Min, M. Bhardwaj, S. Cho, and A. Wang, "Power aware wireless microsensor systems," in 28th European Solid-State Circuits Conference (ESSCIRC'02), Florence, Italy, 2002.

[14] S. Meguerdichian, F. Koushanfar, M. Potkonjak, and M. Srivastava, "Coverage problems in wireless ad-hoc sensor networks," in Proceedings of the 20th Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM'01), vol. 3, Anchorage, AK, pp. 1380–1387, Apr. 2001.

[15] N. Reijers and K. Loangendoen, "Efficient code distribution in wireless sensor networks," in Second ACM International Workshop on Wireless Sensor Networks and Applications, San Diego, CA, Sept. 2003.

[16] D. Ganesan, R. Govindan, S. Shenker, and D. Estrin, "Highly resilient, energy efficient multipath routing in wireless sensor networks," in Proceedings of the 2nd ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc'01), Long Beach, CA, pp. 251–254, 2001.

[17] M. Mauve, H. Hartenstein, H. Fuessler, J.Widmer, and W. Effelsberg, "Positionsbasiertes Routing fuer die Kommunikation zwischen Fahrzeugen," it—Information Technology (formerly it + ti)—Methoden und innovative Anwendungen der Informatik und Informationstechnik, vol. 44, pp. 278–286, Oct. 2002.

[18] F. Sivrikaya and B. Yener, "Time synchronization in sensor networks: A survey," IEEE Network, vol. 18, pp. 45–50, July–Aug. 2004.

[19] R.C. Shah, S. Roy, S. Jain, and W. Brunette, "Data MULEs: Modeling and analysis of a three-tier architecture for sparse sensor networks," in Ad Hoc Networks Journal, vol. 1, pp. 215–233, Elsevier, Sept. 2003.

[20] A. Chakrabarti, A. Sabharwal, and B. Aazhang, "Using predictable observer mobility for power efficient design of sensor networks," in Information Processing in Sensor Networks (IPSN'03), Palo Alto, CA, Apr. 2003.

[21] M. Haenggi, "Twelve Reasons not to Route over Many Short Hops," in IEEE Vehicular Technology Conference (VTC'04 Fall), Los Angeles, CA, Sept. 2004.

[22] M. Haenggi, "Opportunities and Challenges in Wireless Sensor Networks," in Handbook of Sensor Networks: Compact Wireless and Wired Sensing Systems, M. Ilyas and I. Mahgoub, eds., Boca Raton, FL,pp. 1.1–1.14, CRC Press, 2004.

[23] M. Haenggi, "Energy-Balancing Strategies for Wireless Sensor Networks," in IEEE International Symposium on Circuits and Systems (ISCAS'03), Bangkok, Thailand, May 2003.

[24] O. Younis and S. Fahmy, "HEED: A Hybrid, Energy-Efficient, Distributed Clustering Approach for Ad-hoc Sensor Networks," in IEEE Transactions on Mobile Computing, vol. 3, pp. 366–379, 2004

[25] R. Govindan, J. Hellerstein, W. Hong, S. Madden, M. Franklin, and S. Shenker, "The Sensor Network as a Database," Tech. Rep. 02–771, University of Southern California, 2002. ftp://ftp.usc.edu/pub/csinfo/ tech-reports/papers/02-771.pdf.

[26] F. Stajano and R. Anderson, "The resurrecting duckling: Security issues for ad-hoc wireless networks," in 7th International Workshop on Security Protocols, Cambridge, UK, Apr. 1999.

[27] Security in Wireless Sensor Networks: Issues and Challenges, Al-Sakib Khan Pathan, Hyung-Woo Lee, Choong Seon Hong, ISBN 89-5519-129-4 Feb. 20-22, 2006 ICACT2006.

[28] A Survey of Localization inWireless Sensor Network, Long Cheng,ChengdongWu, Yunzhou Zhang,HaoWu, Mengxin Li, and CarstenMaple, Hindawi Publishing

Volume: 09 Issue: 01 Pages: 3321-3328 (2017) ISSN: 0975-0290

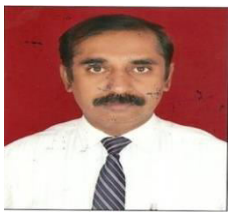
Corporation International Journal of Distributed Sensor Networks Volume 2012, Article ID 962523, 12 pages doi:10.1155/2012/962523.

[29] New Technique of Wireless Sensor Networks Localization based on Energy Consumption, Anouar Abdelhakim Boudhir Bouhorma Mohamed Ben Ahmed Mohamed, International Journal of Computer Applications (0975 – 8887) Volume 9– No.12, November 2010.

Author Biography

Rajkumar is native of Bidar, Karnataka, India. He received his B.E Degree in Computer Science and Engineering from VEC, Bellary, Gulbarga University Gulbarga and M.Tech in Computer Engineering from SJCE Mysore, Visvesvaraya Technological University Belgaum. Presently he was serving as Associate Professor in the department of Information Science and Engineering at Sambhram Institute Of Technology, Bangalore. His areas of interest are wireless sensor network, adhoc network and security. (pyage2005@gmail.com)

Dr. H. G. Chandrakanth is native of Bangalore, Karnataka, India. He received B.E Degree from UVCE, Bangalore University, Bangalore, India in 1991, MSEE from Southern Illinois University Carbondale, USA in 1994 and PhD from Southern Illinois University Carbondale, USA in 1998. Presently he was working as Principal in Sambhram Institute of Technology, Bangalore. (ckgowda@hotmail.com)



Dr. D. G. Anand is native of Madikeri, Karnataka, India. He received his B.E Degree from AIT, Chikamagalore, Mysore University and ME from UVCE Bangalore University, Bangalore and PhD from Jawaharlal Nehru Technological University Anantapur, Andra Pradesh. Presently he was working as Principal in Rajiv Gandhi Institute of Technology, Bangalore. His areas of interest are wireless communication, sensor networks. (dg_anand2003@sifymail.com)

Dr.T.Johnpeter is native of Chennai, Tamilnadu, India. He received his B.E Degree from Manonmaniyam sundaranar University, Tirunelveli and ME Madras University,and PhD from Manonmaniyam Sundaranar University,Tirunelveli. Presently he is working as HOD/CSE in Sambhram Institute of Technology, Bangalore. His areas of interest are Data mining, Neural Networks, wireless communication, sensor networks.(tjpeter.cse@gmail.com)