Recent Challenges And Advances in Ad-Hoc and Sensor Networks

Mr.Suman Kumar Jha[1]
Mr.Bhavesh Mathur[2]
Dr.Yaduvir Singh [3]

***Abstract*- Sensor networks (SNs) have become one of the most interesting areas of research in the past few years. A Sensor Network is composed of a number of wireless sensor nodes which form a sensor field and a sink. These large numbers of nodes, having the abilities to sense their surroundings, perform limited computation and communicate wirelessly form the SNs. Recent advances in wireless and electronic technologies have enabled a wide range of applications of SNs in military, traffic surveillance, target tracking, environment monitoring, healthcare monitoring, and so on.. Ad-hoc network is a self- configuring infrastructureless network of mobile devices connected by wireless. Each device in an ad- hoc network is free to move independently in any direction, and will therefore change its links to other devices frequently. SNs are a smaller, emerging field of research in contrast to their well-established predecessor. SNs are much more versatile than static sensor networks as they can be deployed in any scenario and cope with rapid topology changes. There are many new challenges that have surfaced for the designers of SNs, in order to meet the requirements of various applications like sensed quantities, size of nodes, and nodes autonomy. Therefore, improvements in the current technologies and better solutions to these challenges are required. The future developments in sensor nodes must produce very powerful and cost-effective devices, so that they may be used in applications like underwater acoustic sensor systems, sensing based cyber- physical systems, time-critical applications, cognitive sensing and spectrum management, and security and privacy management. This paper also describes the research challenges for Ad-hoc and Sensor Networks.**

Key-words: Sensor networks, Ad -hoc networks, recent advances, research challenges, Cyber-physical systems.

INTRODUCTION TO ADHOC NETWORKS

Ad hoc networks (AHNs) are wireless multi-hop packet networks without any fixed infrastructure. An AHN network is formed solely by its terminals so that each terminal connected to the network provides also relaying service for others i.e. acts as a router. Advantages of such system are rapid deployment, robustness, flexibility and inherent support for mobility.

AHN can work as a stand-alone autonomous network providing internal connections for a group. Demand for such networks could arise in the contexts of shared desktop meeting, disaster recovery, or in various military applications.

However, no commercial “killer applications” are known for this technology yet.In the future, ad hoc networks probably form the outermost region of the internetwork, where a wired backbone connects both the fixed local area networks and the mobile (both the fixed infrastructure and the ad hoc) networks.

Whereas the base stations of a fixed infrastructure networks are directly connected to the core, an AHN is typically connected through a satellite link or a terrestrial switch (fixed wired connection point, or mobile radiolink). This vision, however, requires still some further developments in ad hoc networking. Basic research and potential applications of ad hoc networks are evolving together, spurring each other into further achievements. The need for an application can give directions for the research and, on the other hand, the research enables new applications to be created. Although this network concept has been originally considered in the context of packet radio networks earlier, it has become very popular again during the past few years. The work is going on within the IETF’s MANET working group for standards and the research is very active throughout the world.Currently the most fundamental research issue in ad hoc networking, between the physical layer and the application layer, is packet routing. In fixed infrastructure mobile networks routing is, for the most part, an engineering problem (implementation of hand-overs etc.), whereas in ad hoc networks it is essentially theoretical. The problems and their solutions considering packet routing are closely related to those widely studied in the case of ordinary fixed networks, but also completely new fundamental challenges have emerged due to the peculiar features of AHNs, such as:

_ Dynamic network topology and structure

– Nodes may join or leave the network

– Some or all nodes may be mobile

_ Limited bandwidth

_ Constrained power

_ Broadcast nature of transmission

In this paper, we discuss the on-going research efforts to tackle the problems between the present day and the vision of practical ad hoc networking solutions. We survey the current work in progress in the field and also anticipate some of the next steps the research is taking. The leading theme is the intellectual challenge posed by this new technology. Therefore, we select the important issues which are to be solved in order to enable widespread ad hoc network deployment and concentrate on very general level instead of protocol specific details The "new world" of AHN technology has been visited by now, there is no such thing that completely unexplored territories in this field. Active research has produced a wide range of proposals, but so far not many problems are solved.

RESEARCH CHALLENGES

ad hoc networking has been a popular field of study during the last few years. Almost every aspect of the network has been explored in some level of detail. Yet, no ultimate resolution to any of the problems is found or, at least, agreed on. On the contrary, more questions have arisen than been answered.This section outlines the major problems remaining to be solved. The protocol dependent development possibilities are mostly omitted and the focus is on the "big picture", on the problems that stand in a way of having peer to- peer connectivity everywhere in the future. The topics are:

_ Scalability

_ Client server model shift

_ Security

_ Interoperation with the Internet

_ Interoperation with other wireless networks

_ Aggregation

3.1 Scalability

Most of the visionaries depicting applications which are anticipated to benefit from the ad hoc networking technology take scalability as granted. Imagine, for example, the vision of ubiquitous computing where the networks can grow to thousands of nodes. How can be the swarm of control messages carried out in this dynamic environment? It is unclear how large an ad hoc network can actually grow. Ad hoc networks suffer, by nature, from the scalability problems in capacity. For a rough idea about this, we may look into simple interference studies. In a non-cooperative network, where omni-directional antennas are being used, the throughput per node decreases at a rate 1= *p*
N, where*N* is the number of nodes That is, in a network with 100 nodes, a single device gets approximately one tenth of the theoretical data rate of the network interface card *at maximum*. This problem, however, cannot be fixed except by physical layer improvements, such as smart antennas. If the available capacity sets some limits for communications, so do the protocols as well. Route acquisition, service location and encryption key exchange are just examples of tasks that will require considerable overhead, which will grow rapidly with the network size. If the scarce resources are wasted with profuse control traffic, it is clear that ad hoc networks will see never dawn in Practice. Scalability is an important research topic for the future, not only because of its necessity for ad hoc networks, but also because of the applicability of same ideas in the Internet.

In the protocol design itself, several issues have to be considered with the potential applications in mind. Whereas proactive routing is not scalable in a dynamic environment as such, on-demand protocols allow deploying large networks in the expense of increased route acquisition latency. The minimum route acquisition latency is the product of maximum network diameter and minimum node traversal time for route requests. Correspondingly, demands for short latencies for route acquisition limit the network size drastically.

3.2 Client-server model shift and service location

In the Internet, a network client is typically configured to use a server as its partner for network transactions. These servers can be found automatically or by static configuration. In ad hoc networks, however, the network structure cannot be defined by collecting IP-addresses into subnets.There may not be servers, but the demand for basic services still exists. Address allocation, name resolution,authentication and the service location itself are just examples of the very basic services which are needed but their location in the network is unknown and possibly even changing over time.
In ad hoc some recent proposals have considered integrating route discovery and service location tasks by allowing only particular kind of services to react to the broadcast requests. This approach, however, can be seen to have the following deficiencies:
_ Inserting application service discovery into a network layer protocol violates the modular protocol design.
_ The client may not be able to specify the required service in a way that the request can be carried on the network layer.
_ Authorization can be difficult at the network layer. Other possibilities are, e.g., using well-known multicast addresses for very basic features, such as DNS. Also protocols for service location have been proposed.

3.3 Security

Ad hoc networks are particularly prone to malicious behavior. Lack of any centralized network management or certification authority makes these dynamically changing wireless structures very vulnerable to infiltration, eavesdropping, interference etc. Security is often considered to be the major "roadblock" in commercial application of ad hoc network technology
Security requirements depend naturally on the application where they are needed. In cases where all the terminals are "on the same side", such as military or emergency rescue applications, it is enough to get protection against outside interference. In civilian, especially commercial, applications even mere lack of cooperation may be enough to bring the network on its knees. The nodes enter and leave the networks as they wish and links may be using nodes that
should not have access to data. How to define membership in ad hoc networks, how to classify nodes to the trusted and the not-trusted ones? Traditional methods of protecting the data with cryptographic methods face a challenging task of key distribution and refresh. Accordingly, the research

efforts on security have mostly concentrated on secure data forwarding. However, many security risks are related to the peculiar features of ad hoc networks. The most serious problem is probably the risk of a node being captured and compromised. This node would then have access to structural information on the network, relayed data, but it can also Send false routing information which would paralyze the entire network very quickly.

3.4 Interoperation with the Internet

It seems very likely that one of the most common applications of ad hoc networks require a connection to the Internet. By ad hoc network technology the coverage of wireless LAN systems can be expanded and complemented. However, the issue of defining the interface between the two very different networks is not straight forward .If a node in ad hoc network has an Internet connection; it could offer Internet connectivity to the other nodes. The node could define itself as a default router and the whole ad hoc network could be considered to be “single-hop” from the Internet perspective although the connections are physically over several hop links.

3.5 Interoperation with other wireless networks

3.5.1 Ad hoc networks

The self-organization of ad hoc networks is a challenge when two independently emerged networks collide. This is an unexplored research topic that has implications on all levels on the system design. What happens when two autonomous ad hoc network move into same area? Surely they are unable to avoid interfering each other. Ideally, the networks would recognize the situation and be merged. However, the issue of joining two networks is not trivial; the networks may be using different synchronization or even medium access or routing protocols. Security becomes also a major concern in these cases. Can the networks adapt to the situation? A common example; a military unit moving into an area covered by a sensor network could be such a situation; moving unit would probably be using different routing protocol with location information support, while the sensor network would have a simple static routing protocol.A similar problem arises when a device is powered on at a border of several networks and it has to choose which one to join.

3.6 Aggregation

Finally, there is the question of rationalizing and collecting the research results. Research has been extremely active during the past few years. The pace has been so fast that the big picture is somewhat blurred. That is why there is a need for summarizing research efforts to combine, not just compare, different approaches. The trend is towards more complete ad hoc networking solutions instead of specific protocols in the near future. The first works on this field has been conducted for energy conserving purposes because of its inherent “multilayer”-structure that provides a natural environment for combining differentideas.

There is work to be done to find best possible combinations of MAC, topology reduction, and routing protocols. There is also work to be done in combining preferable properties of different protocols. This will naturally lead to discussion on specific networks, application tailored solutions, as the ultimate ad hoc networking solution is still far away, if it even can be found.

SENSOR NETWORKS

With the advances in the technology of micro-electromechanical system (MEMS), developments in wireless communications and WSNs have also emerged. WSNs have become the one of the most interesting areas of research in the past few years. Here, we look into the recent advances and future trends in WSNs.

WSNs are usually composed of small, low-cost devices that communicate wirelessly and have the capabilities of processing, sensing and storing. The development of WSNs was motivated by military applications such as battlefield surveillance. WSN are being used in many industrial and civilian application areas, including industrial process monitoring and control, machine health monitoring ,environment and habitat monitoring, healthcare applications, home automation, and traffic control .

A WSN generally consists of a base-station (also called as gateway sometimes) that can communicate with a number of wireless sensors via a radio link. Wireless sensor nodes collect the data, compress it, and transmit it to the gateway directly or indirectly with the help of other nodes. The transmitted data is then presented to the system by the gateway connection.This paper discusses the recent advances in WSNs that enable a wide range of applications and future development in applications like underwater acoustic sensor systems; sensing based cyber-physical systems, time-critical applications, cognitive sensing and spectrum management, and security and privacy management. Rest of the paper is organized as follows..

Recent Advances in Sensor Networks

Recent advances in wireless and electronic technologies have enabled a wide range of applications of WSNs in military sensing, traffic surveillance, target tracking, environment monitoring, healthcare monitoring, and so on. Here we describe such type advances in WSN and their applications in various fields.

1.1. **Sensor Localization and Location-Aware Services**

1.1.1. Smart Home/Smart Office

Smart home environments can provide custom behaviors for a given individual. Considerable amount of research has been devoted to this topic. The research on smart homes is now starting to make its way into the market. It takes a considerable amount of work and planning to create a smart home. There are many examples of products currently on the market which can perform individual functions that are considered to be part of a smart home. Several useful applications which take advantage of information collected by WSN are presented in.

1.1.2 Military

New and emerging technologies, such as networks, support military operations by delivering critical information rapidly and dependably to the right individual or organization at the right time. This improves the efficiency of combat operations. The new technologies must be integrated quickly into a comprehensive architecture to meet the requirements of present time. Improvement in situation awareness is must requirement. Other important application is detection of enemy units' movements on land/sea, sensing intruders on bases, chemical/biological threats and offering logistics in urban warfare.

1.1.3 Traffic Management and Monitoring

Every big city is suffering from traffic congestion around the world. A sincere effort is being made to solve the traffic congestion. Congestion can be alleviated by planning managing traffic. A real-time automatic traffic data collection must be employed for efficient management of rush-hour traffic. Research on this topic is considered as part of the Intelligent Transport System (ITS) research community. It is the application of the computers, communications, and sensor technology to surface transportation.

1.1.4 Structural Healthcare

Structures are inspected at regular time intervals, and repairing or replacing based on the time of use, rather than on their working conditions. Sensors embedded into structures enable condition-based maintenance of these assets. Wireless sensing will allow assets to be inspected when the sensors indicate that there may be a problem. This will reduce the cost of maintenance and preventing harmful failure. These applications include sensors mounted on heavy duty bridges, within concrete and composite materials, and big buildings.

1.1.5 Agriculture

Agriculture can also be benefited by the deployment of WSN to get the information regarding soil degradation and water scarcity. With help of WSNs we can check the clean water consumed in irrigation and manage it.

1.2 Quality of Service (QoS) Provision

QoS support is challenging due to severe energy and computational resource constrains of wireless sensors. Various service properties such as the delay, reliability, network lifetime, and quality of data may conflict; for example, multi-path routing can improve the reliability; however it can increase the energy consumption and delay due to duplicate transmissions. Modeling such relationships, measuring the provided quality, and providing means to control the balance is essential for QoS support.

1.3 Mobility management

Mobility is one of the most important issues in next generation networks. As WSNs are becoming the next elements of the future Internet, it is crucial to study new models that also support mobility of these nodes. WSNs are applicable in variety of cases that make it difficult to produce a standard mobility scenario. Following are some cases where the mobile support is necessary .Intra-WSN device movement is probably the most common scenario in WSNs architectures, where each sensor node has the ability to change from its local position at run time without losing the connectivity with the sensor router (SR). In the case of inter-WSN device movement, sensor nodes move between different sensor networks, each one with its SR responsible to configure and manage all the aggregated devices.

REFERENCES

[1] R. Kay and F. Mattern, "The Design Space of Wireless Sensor Networks", IEEE Wireless Communications vol. 11, No. 6, pp. 54–61, December 2004.

[2] T. Haenselmann, Sensornetworks. GFDL Wireless Sensor Network textbook. http://pi4.informatik.uni- mannheim.de/~haensel/sn_book. Retrieved 2006-08-29.

[3] A. Tiwari, P. Ballal and F.L. Lewis, "Energy- efficient wireless sensor network design and implementation for condition-based maintenance, ACM Transactions on Sensor Networks (TOSN), Vol. 3, Issue 1, 2007.

[4] S. Hadim, N. Mohamed, "Middleware: middleware challenges and approaches for wireless sensor networks," Distributed Systems Online, IEEE , vol. 7, no. 3, pp.1-1, March 2006.

[5] S. Hussain, S. Schaffner and D. Moseychuck, "Applications of Wireless Sensor Networks and RFID in a Smart Home Environment," Proceedings of the 2009 Seventh Annual Communication Networks and Services Research Conference, pp.-153-157, 2009.

[6] Chien-Chung Shen, Chavalit Srisathapornphat and Chaiporn Jaikaeo; "Sensor Information Networking Architecture and Applications"; IEEE Personal Communications, pp. 52-59, August 2001.

[7] S. S. Doumit and D. P. Agrawal; "Self- Organizing and Energy-Efficient Network of Sensors," IEEE, pp. 1-6, 2002.

[8] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam and E. Cayirci, "A Survey on Sensor Networks"; IEEE Communications Magazine, pp. 102-114, August 2002.

[9] J. Chinrungrueng, U. Sununtachaikul and S. Triamlumlerd, "A Vehicular Monitoring System with Power-Efficient Wireless Sensor Networks," ITS Telecommunications Proceedings, 2006 6th International Conference on, pp.951-954, June 2006.

[10] A. Tiwari, A. Lewis, and S-G. Shuzhi, "Design & Implementation of Wireless Sensor Network for Machine Condition Based Maintenance," Int'l Conf. Control, Automation, Robotics, & Vision (ICARV), Kunming, China, 6–9 Dec. 2004.

[11] S.W. Arms, C.P. Townsend and M.J. Hamel, "Validation of Remotely Powered and Interrogated Sensing Networks for Composite Cure Monitoring," paper presented at the 8th International Conference on Composites Engineering (ICCE/8), Tenerife, Spain, August 7–11, 2001.

[12]N. WANG, M. H. Wang, and N. Q. Zhang, "Wireless sensors in agriculture and food industry: Recent development and future perspective," Computers and electronics in agriculture, vol. 50, no. 1, pp. 1-14, 2006.

[13] S. Jardosh and P. Ranjan, "A Survey: Topology Control For

Wireless Sensor Networks," Signal Processing, Communications and Networking,
2008. ICSCN '08. International Conference on, pp.422-427, 4-6 Jan. 2008.

[14] H. Z. Abidin and F. Y. A. Rahman, "Provisioning QoS in Wireless Sensor Networks using a Simple Max-Min Fair Bandwidth Allocation," 2009 World Congress on Computer Science and Information Engineering, 2009.

[15] T. Camilo, P. Pinto, A. Rodrigues, J. Sa Silva and F. Boavida, "Mobility management in IP- based Wireless Sensor Networks," World of Wireless, Mobile and Multimedia Networks,
2008. WoWMoM 2008. 2008 International Symposium on a , vol. 23, no. 26, pp.1-8, June 2008.

[16] V. Devarapalli, R. Wakikawa, A. Petrescu, P. Thubert, "Network Mobility (NEMO) Basic Support Protocol", RFC-3963, January 2005.

[17] R. Wakikawa, P. Thubert, T. Boot, J. Bound and B. McCarthy, , "MANEMO Problem Statement", draft-wakikawa-manemo-00 (work in progress), February 2007.

[18] Na Li, N. Zhang, Sajal K. Das, B. Thuraisingham, "Privacy preservation in wireless sensor networks: A state-of-the-art survey," Ad Hoc Networks 7, pp. 1501–1514, 2009.