International Journal of Computing Academic Research (IJCAR)
ISSN 2305-9184 Volume 4, Number 1(February 2015), pp. 12-18
© MEACSE Publications
http://www.meacse.org/ijcar

Reassessing Mobile Wireless Sensor Networks

Dimple Juneja[1], Aarti Singh[2] and Kavita Gupta [3]

[1] Dronacharya Institute of Management and Technology, Kurukshetra, India

[2&3] MM Institute of Computer Technology & Business Management, Maharishi Markandeshwar University, Mullana, India

Abstract

Mobile Wireless Sensor Network (MWSN) has emerged as a vibrant research field in the domain of sensor networks as execution of applications now primarily depend upon the mobility of sensor nodes. Although, the decreasing cost and significant advantages of sensor nodes is making the implementation of MWSN more practical and possible; but since the deployment of sensor nodes cannot be fully static; the practical implementation of mobility is facing several challenges in connectivity, life time of the network, energy consumption and coverage. This paper reassesses the potential of MWSN and suggests some novel ideas aiming to address the aforementioned challenges.

Keywords: Sensor Network, Mobile Wireless Sensor Network, Life Time of a Sensor Network.

1. Introduction

Mobile Wireless Sensor Network (MWSN) is an anthology of sensor motes sensing the environment with self-healing and organizing capability. Mobility of WSN is a new concept which is making its space at quite a faster pace in the community of wireless networks. A WSN offers numbers of advantages such as monitoring of unreachable areas, habitat monitoring, military applications but it suffers from lot of limitations such as low battery life, lack of control more prominently in a distributed environment, just to list a few. Besides these limitations of WSN the field of MWSN is becoming popular because of locomotive capability of sensor nodes as this ability results in correct location detection for placing the upcoming sensor nodes in the network. In fact, the popularity of mobile wireless nodes is increasing exponentially not only due to its infrastructure-less nature but also due to the limitations of static node architecture [1]. Since, the nodes in MWSN are random and can move arbitrarily, the functional components of MWSN architecture are also mobile and are referred as Mobile Cluster Head (MCH), Mobile Base Station (MBS), Mobile Sensor and Mobile Relying Nodes (MRN).Here, MBS act as collector and gathers information from all sensor nodes. It is trivial that the nodes around base stations vary in numbers and since base station is also of mobile nature and all the nodes continue to dissipate information. Efficient transmissions scheduling scheme is used to reduce the number of transmission hops between base station and sensor node leading to an increase in the lifetime of network. For instance, the cluster head approach of MWSN uses hierarchical network architecture. The selection of cluster head depends on energy efficiency of sensing nodes and cluster head is chosen based on some election process. Since all nodes are mobile, therefore for cluster head also, there is no fixed topology. Few nodes in the network act as mobile relay nodes (MRN) which are responsible for collecting the data from nodes in the cluster and forward either to cluster head or to base station. Although the distribution of mobile nodes is similar to stationary nodes but mobile sensor nodes keeps on changing their topology accordingly to the need of network [14] which is a contrast to conventional sensor nodes. On a contrary note to above attractive features, MWSN are able to offer limited services due to hardware and environment constraints. Here, hardware constraints implies limited

battery power and low cost requirements while environmental constraint deals with shared communication medium and mobile topology. The shared medium dictates that channel access must be regulated in some way.
The paper is structured as follows: section 2 presents the works of eminent researchers who had been putting efforts to lay the foundation of the emerging field. Section 3 discusses various routing protocols and presents a comparison of most dominating ones. Section 4 highlights the challenges and design issues pertaining to the routing in MWSN and also discusses possible solutions addressing the shortcomings. Section 4 discusses about various mobility models that are used to analyze the performance of routing protocols. Finally section 6 concludes with some research directions.

2. Related Work

In MWSN, there are various parameters like long network life time, energy efficiency, secure communication require major attention of the researchers. Use of mobile nodes for communication in wireless sensor network enhance the life time of the network by replacing weak energy nodes with new nodes with high energy level. Sensor network has various attributes like sensors, entities of interest, operating environment, communication, processing architecture, and energy availability. Sensor nodes are categorized in three generations from 1980's to till date on the basis of various parameters like size, node architecture, topology and power supply life time etc [2]. As we have earlier discussed, energy is one of the major aspect in field of mobile wireless sensor network. A large amount of energy of sensor nodes is consumed for searching the neighbouring nodes for communication. The energy consumption process need to be optimized as nodes in MWSN are mobile so position of neighbouring nodes also changes over time. Few works [4] have proposed an energy efficient algorithm for node discovery in MWSN where nodes allowed each other to detect their presence simultaneously by allowing activities like relaying of data on sink andthe logging of encounters.However, there are certain threats for communication in wireless environment such as security of information transferred on wireless communication channel require attention of the researchers. Before proposing security scheme for MWSN certain parameters needs to be considered like application model, network type, network roaming type. These parameters help to locate the node in sensor network environment according to geographical partitioning of the network area [3]. Besides all the facts deployment of sensor nodes in the network plays an important role for efficient data communication. Several researchers have already proposed numbers of schemes for deployment of sensor nodes in MWSN. A group communication deployment scheme for MWSN [5] uses an identity based routing path where change in the position of member changes operation and offers secure routing path for new group as well as for existing group. A model for deployment [6] of sensor nodes in the hostile environment proposes to deploy nodes in the form of groups and nodes in the same group come close to each other leading to effective communication and long network life time. This proposed model is suitable for those applications where location of sensor nodes is difficult to predict. A discussion about deployment of heterogeneous sensors nodes is mentioned in [7] and these sensor nodes are categorized as mobile nodes that are suitable for deployment in uncovered areas, sensor with switching states can be used for storing energy by turned off the states while not in use and reliable sensors are used to offer security for uncovered areas. It uses mathematical function that optimizes the coverage of monitored area and the term coverage is defined in reference with security units collected in collective time period. As we have already discussed mobility is the major factor for consideration for field of MWSN. Researchers had been giving different ideas for introducing mobility in field of wireless sensor network. Data delivery process becomes inefficient because of mobile natured nodes. An efficient and robust method for data delivery [8] computes energy consumed by mobile sink and concludes that energy consumed do not affect the overall network life time and also uses less number of sensor nodes to monitor the region decreasing the operational cost of the network. Authors introduced four types of mobility patterns for sink namely, random walk, biased random walk, walk on spanned graph and predictable mobility. Each of these patterns has their own advantages and disadvantages based on their properties like energy dissipation and efficient timing. Use of mobile sink increases the life time of the network as well as less number of hops in the network reduces the chances the data loss in parallel. Security and adaptability are the essential paradigms considered for wireless communication. Lot of research has been done for communication over wireless links. Security architecture is proposed for authentication during data transmission. Authentication is one of the security mechanisms that involve identification of each node in the network to check validity of node and authentication [10]. A scheme for increasing the security level by reducing the overheads of the nodes in the network in terms of IDS is given in [11]. It proposes a framework for providing network security. Security in multi hop environment can be enhanced by using SNOWNET system that is secure. The scheme proposed by [12] offers data protection for the users and authentication scheme for clients. This proposed technology is portable, deployable and secure. Implementation of security in MWSN is major challenge due to limited resources of sensor nodes. Some of the security algorithms like public key encryption cannot be implemented in WSN. The major problem of MWSN is that the events are detecting by sensing nodes. [14] Offers a new routing protocol that can operate in dual mode simultaneously. The protocol does not consuming energy and operations are simple. This protocol achieves best successful routing rate and hop count. The life time of network depends on the energy consumption by nodes in the network. For a longer life time, the network is partitioned in the form of clusters and data collection and aggregation in managed by the cluster head. For secure data collection in WSN special type of node Mobile Data Collector (MDC) which takes the data from cluster head and transfers to base station [15].Privacy of data is major issue for adhoc network and WSN. The privacy protection in sensor network is required due to malicious node attack. The privacy protection mechanism [16] proposed universal controllable privacy protection framework by using positioned based routing scheme. Security plays important role in wireless environment; a private secure key is deployed in sensing environment. The Proposed solution in [31] is based on multi group authentication protocol where information authentication is independent.

The literature presented above reflects that there are two sets of challenges in MWSNs; hardware and environment. The main hardware constraints are limited battery power and low cost requirements. The limited power means that it's important for the nodes to be energy efficient. Price limitations often demand low complexity algorithms for simpler microcontrollers and use of only a simplex radio. The major environmental factors are the shared medium and varying topology. The shared medium dictates that channel access must be regulated in some way. This is often done using a medium access control (MAC) scheme, such as carrier sense multiple access (CSMA), frequency division multiple access (FDMA) or code division multiple access (CDMA). The varying topology of the network comes from the mobility of nodes, which means that multihop paths from the sensors to the sink are not stable.

In order to address the issues researchers had been putting efforts to improve the efficiency of MWSN. Next section elaborates the routing protocols proposed so far for better working of MWSN.

3. Routing Protocols

Routing protocols for wireless sensor network communication have three basic properties i.e. authentication, data secrecy and replay protection. The mobility based routing protocols use cluster based and zone based communication between the nodes. In each protocol, route discovery mechanism is used to find the route between source node to destination node. The field of MWSN offers a variety of routing schemes that are discussed below:

- **LEACH** (Low Energy Adaptive Cluster Hierarchy) is the first protocol based on clustering technique. It considered rotation of Cluster Head (CH) position for each round. Each node has equal probability of being chosen as Cluster Head. It also incorporates communication between cluster members. LEACH has three key features such as Local coordination of nodes and setting the cluster position, Random rotation of cluster heads in each round where each round is of fixed length and for reducing global communication there is concept of local compression.

- **LIMOC (Enhancement of Network lifetime Using Mobile Clusterheads)** follows hierarchical routing topology for communication along with base station. It controls the movement of CH intelligently by keeping the members of cluster as static during the movement of CH towards the event.

- **Cluster Based Energy Efficient Scheme** (CES) is used to choose CH for distributing energy consumption in the network. Each node calculates its residual energy, mobility and weight then broadcasts to its neighbour. The sensor with high weight value is elected as CH and its neighbouring nodes join it.

- **Mobility and Traffic Adapted** Cluster Based routing scheme offers mobility of nodes with efficient energy. The traffic and mobility scheduling design allows cluster head to reuse timeslots to support mobility of sensor nodes.

- **ZIGBEE** [9] is standard used for high level communication with low energy consumption and low data communication rate. This protocol provides high level of data security and protect from replay attacks of the message. It sends 8 byte code with each data packet which results in high communication overhead and also preserves the pre sender state. Table 1 delineates a comparison of various existing protocols mentioned above.

Table 1 Comparison of Communication Protocols in MWSN

Scheme	**Technique**	**Security**	**Energy Consumption**	**Network Life Time**	**Cluster Head formation**	**Delay in packet transmission**
LEACH	Cluster based	Less	Average	Poor	Y	Y
LIMOC	Hierarchy Based	Average	Low	Good	Y	Y
CES	Multi Hop	Average	Low	Good	Y	N
ZIGBEE	Layered	Y	Low	Average	NA	NO
Mobility & traffic adapted	Cluster based	Y	Average	Poor	Y	Y

In the next section major issues arise in MWSN architecture are being discussed.

4. Design Issues and Open Challenges

Issues in MWSN have been classified into different domains namely design, security and architectural and are reassessed below.

4.1 Design Issues

The main design goal of sensor network is to transmit the data by increasing the life time of network and using the efficient routing protocols. The design of WSN is influenced by various factors like scalability, fault tolerance and power consumption. Major design issues of wireless sensor network are pointed out like limited power, limited resources, location of sensor nodes etc. Some of the main design issues are discussed below:

- **Scalability:** The network should be scalable in terms of expansion. If large number of nodes is connected, then the system must be adaptable for handling design challenges.

- **Fault Tolerance:** Sensor network nodes can fail or get physically damaged. The system must be adaptable for handling these issues. Fault tolerance can be described as the capability of sensing nodes work efficiently even after the node failure or due to low power of node.

- **Production Cost:** The overall cost of wireless sensor network depends upon the cost of individual node. As WSN consist of large number of nodes so each node used must be cheap so that overall network cost could be minimized.

- **Power Supply:** The nodes in sensor network are battery operated and having limited battery life. It becomes difficult to recharge the nodes in hostile environment

- **Hardware:** Processing, transceiver, sensing and power unit are the four main units of sensor node. These components are application dependent.

4.2 Security Issues

Security is one of the major challenges in field of wireless system. Nodes in wireless system are independent and free to move randomly so forms dynamic topology. The node in wireless network forms an ad hoc network. Various security issues like Authenticity, Confidentiality, Integrity, Availability etc are highlighted and discussed below.

- For secure data transmission over wireless network the users must be authenticated so that unauthorised users cannot hack the data. Transmission should be in secure manner.

- There should be network boundaries i.e. data should be confidential for specific users inside the network.

- Nodes in wireless system are free to move and for continuous transmission nodes should available in the network.

- Integrity is also the major requirement in Wireless networks i.e. there should not be data loss due to any accident on the network.

4.3 Architectural Issues

The following issues are raised during architecture design of wireless sensor network.

- **Node distribution**: The nodes in wireless sensor network are distributed in clustered manner. Clusters are of small sizes i.e. containing limited number of nodes for reliable transmission of data.

- **Node dynamicity**: Nodes are of dynamic nature so their structured cannot be freeze or described earlier. So the architecture of WSN is not fixed.

- **Energy Efficiency**: Nodes are of limited battery life, applications like battlefield require energy efficient transmission of data.

- **Data transmission**: Data transmission in network is event driven or query based.

5. Mobility Models

Mobility models are used to analyze the movement of mobile nodes in the hostile environment. These models defines the procedure hoe the position, location and speed of the nodes changes with time. Use of mobility models helps to analyze the routing path of nodes in the simulation field. As we know node movement cannot be restricted to a particular direction and these mobility models are used to predict the node behaviour [13]. Few types of mobility models are discussed below:

- **Random way Point Mobility Model:** This mobility model is enhanced version of random walk model and includes a pause time slot for node to change its position and direction. Mobile node stays at a location for a certain time then moves towards newly chosen destination. Nodes with high speed provides stable network as compared to slow speed nodes. But this model has some limitations, it is memory less model and we are not able to correlate the velocity of current node with previous node.
- **Path way Mobility Model:** In this model nodes are restricted to move along a predefined path and this path is defined randomly or based on a city map. The node chooses its destination randomly and moves along the shortest path edges. On reaching to the boundaries node changes its direction and for each phase of motion destination is chosen randomly. At each intersection node has equal probability of movement in left, right and straight line.
- **Gauss Markov Mobility Model:** This model removes the limitation of random way point mobility model as it has memory level parameter to store the velocity of previous node and we can correlate the velocity of current node with previous node. Nodes are free to move in random manner and on reaching to boundaries to simulation field node changes its direction by 180 degree.
- **Random Point Group Mobility Model:** As per its name in this model nodes are bounded in a group and each group has a group leader, movement of group members is analysed movement pattern of group leader and whole network area is divided in the small regions and each region is assigned for each group.

6. Conclusions

In the above context we have discussed the concept of Mobile Wireless Sensor Network, architecture of MWSN, various areas of applications of MWSN; various issues arise in this emerging field. Security in routing protocols, limited energy resources, dynamic topology and resilience arise as the major issues in Mobile Wireless Sensor Networks. These limitations in MWSN can lead to future research work.

References

[1] Santosh Kumar G, “An Energy Aware Load Balanced Clustering Scheme for Sensor Networks”, National Conference on Computational Science and Engineering, Rajagiri School of Social Sciences, Kochi, Kerala, India, February 6-7 ,2009.

[2] Chee Yee Chong, “Sensor Networks: Evolution, Opportunities and Challenges”, Proceedings of the IEEE, Vol. 91, Issue No. 8, 2003, pp. 1247-1256.

[3] KashifKifayat, MadjidMerabti, Qi Shi, David Llewellyn-Jones, “Security in Mobile Wireless Sensor Network”, Published in Handbook of Information and communication Security, Springer berlin Heidelberg, Book Chap E, 2007, pp. 513-552.

[4] Vladimir Dyo, Cecilia Mascolo, “Efficient Node Discovery in Mobile Wireless Sensor Network”, Published in DCOSSS ’08 Proceedings of the 4th IEEE International Conference on Distributed Computing in Sensor Systems, Springer Verlag Berlin, 2008, pp. 478-485.

[5] Nahar, Eui, “An Efficient Scheme for Secure Group Communication in Mobile Wireless Sensor Network”, Published in ICUIMC ’08 Proceedings of the 2nd International Conference on Ubiquitous Information Management and Communication, ACM Network, 2008, pp. 501-505.

[6] Donggang, Peng,Wenliang, "Group Based Key Predistribution for Wireless Sensor Network", Published in ACM Transaction for Sensor Networks, Vol. 4, Issue 2, March 2008.

[7] Rbie, Khalid, Resham, Mrinal, "Impact of Heterogeneity on Deployment of Wireless Sensor Networks", Published in Proceedings of the 3rd international conference on Wireless Internet organized by ACM, 2007.

[8] Ioannis, Athanasios,Sotiris, "Sink Mobility Protocols for Data Collection in Wireless Sensor Networks", Published in Proceedings of 4th ACM International workshop on Mobility Management and Wireless Access,2nd-3rd October, 2006,pp 52-59.

[9] Mark, Ghita, Adrian, Virgil, "MiniSec : A Secure Sensor Network Communication Architecture", Published in proceedings of the 6th International Conference on Information Processing in Sensor Networks, Vol. 117,2007,pp. 479-488.

[10] D. Boyle, T. Newe, "Security Protocols for use with Wireless Sensor Networks - A Survey of Security Architectures", Proceedings of the Third International Conference on Wireless and Mobile Communications by IEEE,4th-7th March, 2007, pp 54.

[11] Paola Inverardi, Leonardo Mostarda, Alfredo Navarra, "Distributed IDSs for enhancing Security in Mobile Wireless Sensor Networks", Proceedings of the 20th International Conference on Advanced Information , Networking and Applications by IEEE, Vol. 2, 2006, pp. 116-120.

[12] Lusheng Ji, Brian Feldman, Jonathan Agre, "Self-organizing Security Scheme for Multi-hop Wireless Access Networks", Published in Proceedings of Aerospace Conference IEEE, Vol. 2, 2004, pp. 1231-1240.

[13] Javad, marjan, Abdul, " Mobile Wireless Sensor Networks Overview", IJCCN International Journal of Computer Communications and Networks, Volume 2, Issue 1, February 2012, pp. 17-22.

[14] Rei-HengCheng, Chang Wu Yu, Tung-Kuang Wu, Fang-Wei Jin, "A Small-World Routing Protocol and the Effect of Pass-Over for Wireless Sensor Networks", Published in Wireless Personal Communications by Springer, Vol. 68, Issue No. 4, 2013, pp. 1493-1523.

[15] A.S. Poornima, B.B. Amberker, "Secure Data Collection using Mobile Data Collector in Clustered Wireless Sensor Networks", Published in Wireless Sensor Systems IET, Vol. 1, Issue No. 2, 2010.

[16] Isaac Amundson and Xenofon D. Koutsoukos, "A Survey on Localization for Mobile Wireless Sensor Networks", Published in Mobile Entity Localization and Tracking in GPS Less Environments, Second International Workshop MELT proceedings,2009, pp. 235-254.