A Study on Wireless Sensor Networks and Mobile Ad hoc Networks

S.V.Karthik[1]
[1](Assistant Professor, Computer Science and Engineering,
Star Lion College of Engineering and Technology, Thanjavur, Tamilnadu, India)

Abstract

The Wireless Sensor Networks (WSN) are becoming very trending technology, it is very essential to understand the architecture for this kind of networks before deploying it in any application. Ad hoc networking has been a animatedly growing research area for the last years. The need for a network when there is no infrastructure is no more limited under military and emergency applications; ad hoc networks can include private (home, entertainment, business) and public sectors (fast outdoor downloading) applications as well. In ad hoc networks, wireless mobile computing devices can perform critical network topology functions that are normally the job of routers within the Internet infrastructure.

Keywords: *Mobile AdHoc Network (MANET), On Demand Routing protocol, Routing Protocol, Table Driven Routing protocol, Wireless Sensor Network (WSN)*

I. Introduction

Wireless Sensor Networks(WSN) is a collection of sensors that can communicate through wired or wireless medium. The sensors are allowed to communicate within its communication range. It which consist of one sink(or)base station able to manage all communication in the network.

A Wireless Adhoc network is a decentralized type of wireless network.The Mobile Adhoc networks can be used in many applications,ranging from sensors for environment,vehicular communications,road safety,home,peer-to-peer messaging,disaster rescue operations,robots etc.

An ad-hoc network is a self-configuring network of wireless links connecting mobile nodes. These nodes may be routers and/or hosts. The mobile nodes communicate directly with each other and without the aid of access points, and therefore have no fixed infrastructure.

II. Wireless Sensor Network

A WSN is a collection of sensors that can communicate through wired or wireless medium. The sensors are allowed to communicate within its communication range. It has received a greater interest in various applications such as disaster management, border protection, military for security surveillance, structural health monitoring, industrial automation, civil structure & biologically hazards monitoring in variety of applications.

A sensor network must be able to operate under changing environment. Specifically, our protocols must be able to enable network operation during start-up, steady state, and failure.The necessity of operation under these conditions is required because in most cases, the sensor network must operate unattended. Once the nodes have booted up and a network is formed, most of the nodes will be able to maintain a steady state of operation.

A Sink node is act as a cluster head which gather, control and forward data collected by other sensor nodes. A sink node is having the large transmission range as compare to other nodes. The sink may also be a mobile node or active node acting as information sink, or any other entity that is extracting the information from the sensor network. Although the multi-hop network can operate in both the sensor-to-sink and sink-to-sensor.

Sensor nodes are expected to operate and adjust in changing environments and should be applicable in large areas. Failures are susceptible in wireless sensor networks due to inhospitable, unstable environment and unattended deployment. The data communication from transmitter to receiver and vice versa may cause energy depletion in sensor nodes and therefore, it is common for sensor nodes to exhaust its energy completely and stop operating and thus, need to switch between wakeup and sleep modes.

III. AD HOC Networks

An ad-hoc network is a self-configuring network of wireless links connecting mobile nodes. These nodes may be routers and/or hosts. The mobile nodes communicate directly with each other and without the aid of access points, and therefore have no fixed infrastructure. They form an arbitrary topology, where the routers are free to move randomly and arrange themselves as required.

Each node or mobile device is equipped with a transmitter and receiver. They are said to be purpose-specific, autonomous and dynamic. This compares greatly with fixed wireless networks, as there is no master slave relationship that exists in a mobile ad-hoc network. Nodes rely on each other to established communication, thus each node acts as a router. Therefore, in a mobile ad-hoc network, a packet can travel from a source to a destination either directly, or through some set of intermediate packet forwarding nodes.In a wireless world, dominated by Wi-Fi, architectures which mix mesh networking and ad-hoc connections are the beginning of a technology revolution based on their simplicity.

Adhoc networks date back to the Seventies.They were developed by the Defense Forces, to comply with a military framework. The aim was to rapidly deploy a robust, mobile and reactive network, under any circumstances. These networks then proved useful in commercial and industrial fields, first aid operations and exploration missions.Ad hoc networks, also called peer-to-peer networks, still have a long way to go in order to be fully functional and commercial, as it has its defects such as security and routing which we will discuss further.

IV. Mobile AD HOC Network (MANET)

A mobile ad hoc network (MANET) is a continuously self-configuring, infrastructure-less network of mobile devices connected wirelessly. Each device in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently.

"A collection of wireless mobile hosts forming a temporary network without the aid of any centralized administration or standard support services."

Ad-hoc network topology is dynamic-nodes enter and leave the network continuously. No centralized control or fixed infrastructure to support network configuration or reconfiguration.

1) How does it work?

Wireless Sensor Networks is a class of special wireless ad hoc networks. A wireless ad hoc network is a collection of wireless nodes that communicate directly over a common wireless channel. There is no additional infrastructure needed for

adhoc networks. Therefore, every node is equipped with a wireless transceiver and has to be able to act as a router, to process packets to their destinations. A strength of these networks is their ability to self-organize the infrastructure of the routing, after they were deployed. The following figure shows an example for a typical ad hoc network.

V. Routing Protocols

Routing protocols between any pair of nodes within an ad hoc network can be difficult because the nodes can move randomly and can also join or leave the network. This means that an optimal route at a certain time may not work seconds later. Discussed below are three categories that existing ad-hoc network routing protocols: Table Driven ProtocolS,On Demand Protocols Hybrid Protocols.

1) Table Driven Routing Protocols-Table Driven Routing Protocols, also known as Proactive Protocols, work out routes in the background independent of traffic demands. Each node uses routing information to store the location information of other nodes in the network and this information is then used to move data among different nodes in the network. This type of protocol is slow to converge and may be horizontal to routing loops.These protocols keep a constant overview of the network and this can be a disadvantage as they may react to change in the network topology even if no traffic is affected by the topology modification which could create unnecessary overhead. Even in a network with little data traffic, Table Driven Protocols will use limited resources such as power and link bandwidth therefore they might not be considered an effective routing solution for Ad-hoc Networks.Example-Fisheye State Routing(FSR).

2) On Demand Routing Protocols-On Demand Routing Protocols, also known as Re-active Protocols, establish routes between nodes only when they are required to route data packets.

There is no updating of every possible route in the network instead it focuses on routes that are being used or being set up. When a route is required by a source node to a destination for which it does not have route information, it starts a route discovery process which goes from one node to the other until it arrives at the destination or a node in-between has a route to the destination.

On Demand protocols are generally considered efficient when the route discovery is less frequent than the data transfer because the network traffic caused by the route discovery step is low compared to the total communication bandwidth. This makes On Demand Protocols more suited to large networks with light traffic and low mobility.Example-Dynamic Source Routing(DSR).

3) Hybrid Routing Protocols-Hybrid Routing Protocols combine Table Based Routing Protocols with On Demand Routing Protocols. They use distance-vectors for more precise metrics to establish the best paths to destination networks, and report routing information only when there is a change in the topology of the network.

Each node in the network has its own routing zone, the size of which is defined by a zone radius, which is defined by a metric such as the number of hops. Each node keeps a record of routing information for its own zone. Zone Routing Protocol (ZRP) is an example of a Hybrid routing protocol.

VI. Security Issues in AD HOC Network

1) Susceptible to Channels- messages can be eavesdropped and bogus messages can be injected into the network without the difficulty of having physical access to network components which violent the security issue.

2) Lack of Infrastructure-Ad hoc networks are considered to operate independently of any fixed infrastructure.

VII.Security Requirements for AD HOC Network

1)Confidentiality-Ensures certain information is never disclosed to unauthorized users.

2)Integrity- Message received at the receiver side must be original.

3)Authentication:-Only the authorized user can access the data.

4)Non-impersonation-No one can act to be another authorized member to learn any useful information.

5)Attacks using fabrication:-Attackers created the false route to access the information. This type of attacks is hard to identify

VIII. Figures and Tables

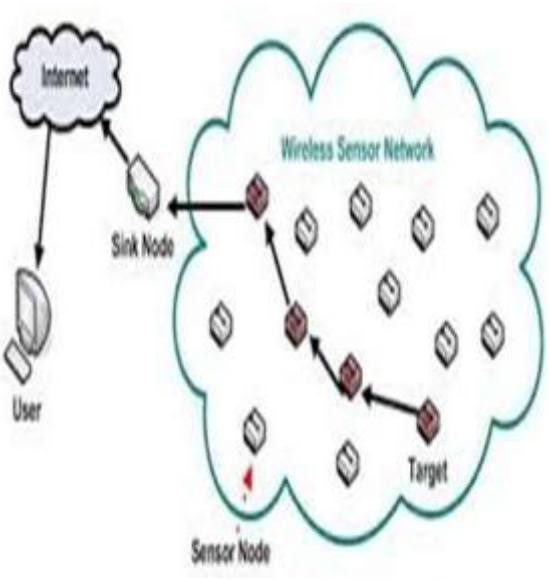

Fig 1-Wireless Sensor Network(WSN)

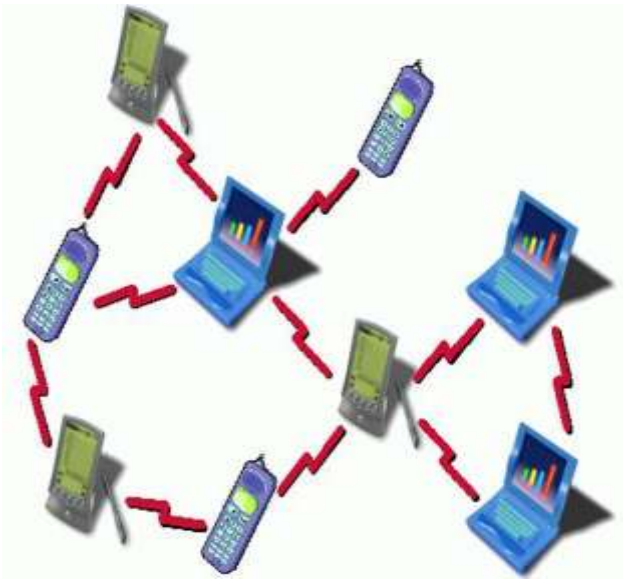

Fig 2-Mobile Ad Hoc Network Diagram

Fig 4-Ad-hoc Mobile Routing Protocols

IX. Conclusion

This paper proposed the comparison between sensor networks, mobile adhoc networks and various security issues requirements of the above networks. Also it includes the architecture and various routing protocols of these main wireless networks

References

Books:

[1] C.Sivaram murthy,B.S.Manoj, Ad hoc wireless netwoks:Architectures and protocols,pearson Edu,2004.

[2] H. Yang, H. Luo, F. Ye, S. Lu, and L. Zhang (2004), "Security in mobile adhoc networks: challenges and solutions," IEEE Wireless Communications, vol. 11, no. 1, pp. 38-47.

[3] Roberto Di Pietro, Pietro Michiardi, Refik Molva (2007), "Confidentiality and Integrity for Data Aggregation in WSN using Peer Monitoring".

[4] Nandini. S. Patil, Prof. P. R. Patil (2010), "Data Aggregation in Wireless Sensor Network,"IEEE International Conference on Computational Intelligence and Computing Research, 2010.

[5] Li, Raghu Kisore Neelisetti, Cong Liu, and Alvin Lim (2010), "Efficient Multipath Protocol for WSN", International Journal of Mobile and Wireless, Vol 2, No.1.

[6] Simarpreet Kaur, and Leena Mahajan (2011),"Power Saving MAC Protocols for WSNs and Optimization of S-MAC Protocol",

[7] International Journal of Radio Frequency Identification and Wireless Sensor Networks.

[8] Cork,Ireland Utz Rodig,Cormac J.Sreenan "Wireless Sensor Networks"-6th European Conference,EWSN 2009.

[9] Stefano Basagani,macro Conti,Silvia Giordano,ivan Stojmenovic,"Mobile Ad hoc Networking, John Wiley&Sons2004.