J. Basic. Appl. Sci. Res., 3(6)248-258, 2013
© 2013, TextRoad Publication

ISSN 2090-4304
Journal of Basic and Applied
Scientific Research
www.textroad.com

How the Two Wireless Networks Can Be Different: WSNS and VANETS

Vandana Jindal, A.K.Verma, Seema Bawa

Thapar Univ., Patiala, Thapar Univ., Patiala, Thapar Univ., Patiala

ABSTRACT

Reasons for switching over from a wired network to a wireless network are many. To name a few - sharing internet access along with the files and printers, playing games, always on, no more messy wires required and the list goes on. For a more mobile solution where a user needs to access network resources on the move then radio technology is the only logical choice. The number of people using their mobile devices to access online news and other information on a daily basis is rising sharply. According to a report issued by marketing research firm comScore, the number of people who used their mobile devices every day increased from 10.8 million to 22.4 million between Jan 2008 and Jan 2009.

KEYWORDS:–WSN, CAN, SAN, DAN, VANET, historical queries, one time queries, persistent queries, DSRC, IEEE 802.15.4,ZigBee,IEEE 1609.

1. INTRODUCTION

A network may be defined as a connection between two or more computers either through cables, telephone lines, satellites, radio waves or infrared beams, such that they are able to share resources like- CD-ROMs, printer etc., or exchange files or allow electronic communication. From the above definition networks can be classified into two broad categories: wired networks or wireless networks. We have seen a rapid development in the field of wireless networks because of their capability to cater to the needs of today's executives, a common man, researchers, tourists etc., where the desire to connect to anything - anytime has become an integral part of everyone's life. Here we shall confine our study to the area of two types of wireless networks i.e. Vehicular adhoc network and wireless sensor network (WSN).

Vehicular communication system is a promising technology. Its users will be undoubtedly benefitted with various services from safety alert to in-car entertainment. Due to its huge application potential, it attracts attentions both from academia and industry. While talking about the WSNs, these overweigh traditional networks in the areas of deployment, scalability, ease of use and mobility. WSNs are becoming a powerful tool for information gathering, environmental monitoring, terrain surveillance, battlefields etc. Micro Electrical Mechanical Systems (MEMS) technology, miniaturization, cost-effective and wireless networking allow the deployment of sensors in a wireless ad hoc fashion for numerous applications. The scientific contribution of this paper is highlighting the contrasting features between the two mobile networks with respect to the characteristics, protocols used and their architecture.

Sec II and III give a brief description of the types of wireless networks along with their advantages and limitations. Sec IV emphasizes the importance of wireless technology. Sec V and VI explain about the WSNs and VANETs respectively. Finally, Sec VII sums up the paper giving the differences between the two mobile networks at a glance in a tabular form.

2. Types of networks

The networks may broadly be classified as under:

1. LAN - Local Area Network
2. WLAN - Wireless Local Area Network
3. WAN - Wide Area Network
4. MAN - Metropolitan Area Network
5. SAN - Storage Area Network or referred with names like System Area Network, Server Area Network, or sometimes Small Area Network
6. CAN - Campus Area Network, Controller Area Network or Cluster Area Network
7. PAN - Personal Area Network
8. DAN - Desk Area Network

2.1 LAN - Local Area Network

The area covered under LAN is short i.e. small offices, home, internet cafes etc. It can be controlled and administrated by a single person. It uses TCP/IP network protocol for communication between computers.

[*] **Corresponding Author:** Vandana Jindal, Thapar Univ., Patiala, Thapar Univ., Patiala, Thapar Univ., Patiala

2.2 WAN - Wide Area Network

The area covered under WAN is a large distance for communication between computers. An example of WAN is **'The Internet'**, which covers the entire earth. WAN is a collection of geographically distributed LANs. A network connecting device router, connects LANs to WANs. WAN uses network protocols like ATM, X.25, and Frame Relay for long distance connectivity.

2.3 Wireless - Local Area Network

A LAN, based on wireless network technology often referred to as **Wi-Fi** or WLAN has no wires for communication instead it uses radio signals as the medium (for communication). Wireless network cards are employed (installed) for accessing any wireless network around. Generally wireless cards connect to wireless routers for communication among computers or accessing WAN, internet.

2.4 MAN - Metropolitan Area Network

MAN, metropolitan area network falls in the middle of LAN and WAN, covering physical area greater than LAN but smaller than WAN, such as a city.

2.5 CAN - Campus Area Network

As the name suggests i.e. campus area network, it is usually used in local business offices/ buildings or large universities. It is composed of a number of LANs. The physical area covered is less than a MAN.

2. 6 SAN - Storage Area Network

SAN technology is basically used by data oriented organizations where the primary requirement is data storage. SAN connects servers to data storage devices by using Fiber channel technology.

2.7 SAN - System Area Network

SAN, system area networks also referred to as cluster area network connects high performance computers with high speed connections (in cluster configuration).

3. Why Wireless Networks/Communication?

In today’s world where the technology is changing at the blink of an eye, people prefer to update themselves anywhere – anytime. This requires installation of a wireless network i.e. a network without cables which otherwise would have been scattered in offices or homes. The wireless is now cheaper to install. It was 10% of the cost of the wired system in 2010. Rapid deployment, flexibility in placement, low maintenance, last but not the least expensive and unreliable connectors (used in wired networks) are the striking features for its massive use. Wireless communication is not a new technology but cellular phones have brought a big revolution in wireless communication. World has moved from fixed to wireless networks **a**llowing people, mobile devices & computers talk to each other, without a cable. In a wireless network interconnectivity with multiple devices takes place with the help of radio-waves or sometimes even light.

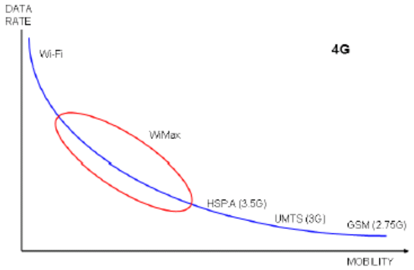


Fig.1 Data Speed V/s Mobility for wireless system

(From the above Fig. it is clear that Wi-Fi has the highest data rate with no mobility where as the GSM has the maximum mobility supporting data rates up to 180kbps. The most widely used one of the 3G cell phone technology is Universal Mobile Telecommunication System (UMTS) supporting 384kbps of data).

3.1 Advantages

The main reasons for the popularity of wireless networks are as follows:

Convenience: Wireless Networks help connecting to the internet more conveniently. There is no need to pull an Ethernet connection through walls and ceilings and people can connect anywhere with a strong enough signal and a wireless network that is publicly accessible.
Availability: Wireless Networks WLANs are available anywhere in the world at an affordable cost.
Productivity: The universal access to the network and Internet can translate into real savings.
Reduced Cost: Initially, the investment needed for wireless LAN hardware is higher than the cost of wired LAN hardware, but the overall installation expenses and life-cycle costs are significantly lower. Long-term cost benefits are greatest in dynamic environments requiring frequent moves and changes.
Mobility: Wireless LAN systems can provide LAN users with access to real-time information, enhancing productivity and dispensing services anywhere in their organization which otherwise would have not been possible with the wired networks.
Time saving: Very easy and rapid installation.
Scalability: Wireless LAN systems can be configured in a variety of topologies to meet the needs of specific applications and installations. Configurations can be easily changed ranging from peer-to-peer networks (suitable for a small number of users) to full infrastructure networks (of thousands of users that enable roaming over a broad area).

3.2 Limitations

Various limitations posed by wireless networks:

Wireless Links

- Packet loss due to transmission errors
- Variable capacity links
- Frequent disconnections/partitions
- Limited communication bandwidth
- Broadcast nature of the communications

Mobility

- Dynamically changing topologies/route
- Lack of mobility awareness by system/applications

Limitations of the Mobile Computer

- Short battery lifetime
- Limited capacities

4. Wireless technologies around

Wireless technologies often tend to increase convenience.

In order to cater to the needs (general or specific) of the people, various wireless technologies have come up each with its own benefits and limitations and the research is still going on. Various wireless technologies that are either already into existence or coming into shape are - Wi-Fi, Bluetooth, WiMax. The reason for popularity of these fast upcoming technologies are – ease of installation at home/ office, affordable, scalable and the mobility of the devices within the network. It is a simple matter to relocate a communicating device, with no additional cost of rewiring and excessive downtime. It is very easy to add in a communication device to the network or remove one from the network without any disruption to the remainder of the system. Other than the initial outlay on setting up a wireless network, the cost of running and maintaining it is minimal. These factors show the appeal of wireless technology for the home and office environment.

In the following sections we shall be concentrating on various aspects of WSNs (Wireless Sensor Networks) and VANETs (Vehicular Ad-Hoc Networks). This paper summarizes our initial investigation about the duo. In the subsequent sections efforts have been made in highlighting the differences between the two adhoc networks with respect to the characteristics, protocols used and their architecture. By no means do we claim that the search has been exhaustive but every effort has been made to cover maximum areas and parameters.

5. WSN: An Introduction

A wireless sensor network (WSN) as the name suggests is a wireless network with spatially distributed autonomous devices making use of sensors for monitoring physical or environmental conditions. [1,2] WSNs were originally motivated by military applications like battlefield surveillance, but now they find their applications in areas like healthcare applications, home automation, traffic control etc. Each node in a sensor network is equipped with a radio transceiver, a microcontroller and an energy source (usually battery). Size and cost constraints on sensor nodes result in limitations on resources like energy, memory, computational speed and bandwidth. A sensor network is usually made up of a wireless ad-hoc network. Each sensor supports a multi-hop routing algorithm.

Sensor node Architecture

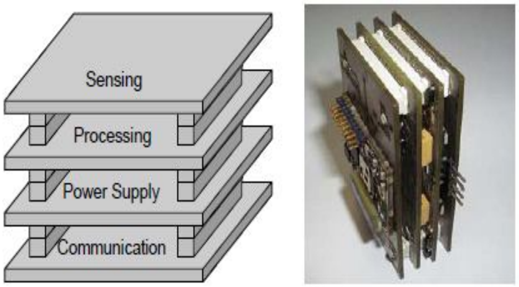


Fig. 2 Architecture and aspect of a node

The data/information may be collected by firing a query from the base station to the WSN. The query may be one of the three types i.e. historical queries (analysis of data collected over time), one time queries (snapshot view of the network), persistent queries (periodic monitoring at long and regular intervals).

The main function of a sensor node is to acquire information from the areas of their deployment. These nodes are usually deployed in those areas/regions where human intervention is not possible. They may accomplish the tasks like measuring temperature, voltage, or even dissolved oxygen. The nodes are a part of a wireless network. The gateway collects the measured data from each node and sends it over to the sink node.

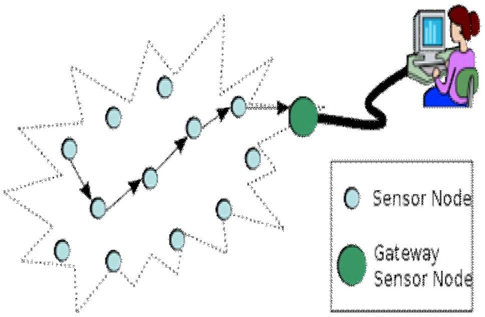


Fig. 3 WSN Communication

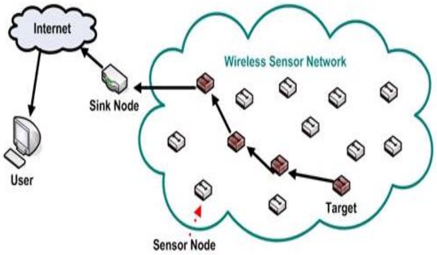


Fig. 4 Wireless Sensor Network

In WSNs, each node may be equipped with a variety of sensors, such as acoustic, seismic, infrared, still/motion video camera, etc. The nodes get organized in clusters, detecting events. Each node has sufficient processing power to make a decision, and in turn broadcasts the decision to other nodes in the cluster. One node may act as the cluster master and the communication takes place through radio waves using protocols such as IEEE 802.11 or Bluetooth etc.

5.1 Characteristics of WSNs

Unique characteristics of a WSN include:

- Limited power they can harvest or store
- Ability to withstand harsh environmental conditions

- Ability to cope with node failures
- Mobility of nodes

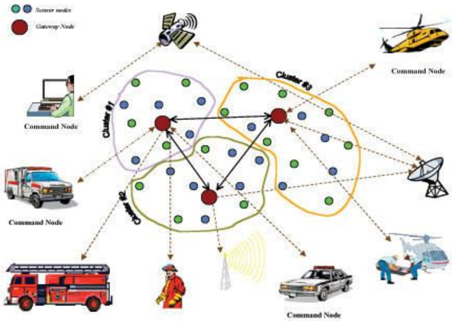


Fig.5 Wireless Sensor Network

- Dynamic network topology
- Communication failures
- Heterogeneity of nodes
- Large scale deployment
- Unattended operation

5.1.2 Applications of WSNs

The applications for WSNs are many and varied. Some of the applications for WSNs are:

- Habitat monitoring
- Object tracking
- Nuclear reactor control
- Fire detection
- Traffic monitoring
- Area monitoring
- Environmental monitoring
- Patient monitoring
- In Kindergartens
- Seismic Monitoring
- Field Experiment
- Contaminant Transport

5.1.3 Factors affecting WSNs

- Battery life
- Cost
- Data latency
- Data rate
- Data reliability
- Data security
- Physical size
- Transmission range

5.1.4 Routing Protocols in WSNs

1. **Flooding:** A method for relaying data in WSNs without the need for any routing algorithms or and topology maintenance.
2. **Gossiping:** The receiving node sends the packet to a randomly selected neighbor which picks another neighbor to forward the packet to and so on.
3. **Flat routing**[3]: The 3 protocols that fall into this category are-

SPIN (Sensor Protocols for Information via Negotiation): sends data to sensor nodes only if they are interested.

DD (Directed diffusion): sets up gradients for data to flow from source to sink during interest dissemination.

Rumor routing [4]: It is a variant of DD, which uses events table and an agent.

4. **Hierarchical** [5]: These protocols are proposed to address scalability and energy consumption challenges of sensor nodes. Sensor nodes form clusters where the cluster-heads aggregate and fuse data to conserve energy.

LEACH (Low Energy Adaptive Clustering Hierarchy): forms clusters to minimize energy dissipation.

PEGASIS [6] (Power-Efficient Gathering in Sensor Information Systems): An enhancement over LEACH protocol. It increases the lifetime of each node by using collaborative techniques.

TEEN [7] (APTEEN) (Threshold-Sensitive Energy Efficient Protocols): Most suitable for time critical sensing applications.

5. **Location based routing:** In this type of protocols sensor nodes are addressed depending on their locations. Relative coordinates of neighboring nodes is obtained either by exchanging information between neighbor nodes or by directly communicating with a Global Positioning System (GPS).

GEAR [8] (Geographic and Energy Aware Routing): Restricts the number of interests in DD by only considering a certain region rather than sending the interests to the whole network.

GEM: GEM is based on the optimization of two metrics: number of received packets (depending upon the network topology/environmental features); and energy consumption, (depending upon the system performance).

5.1.5 Architecture of WSN

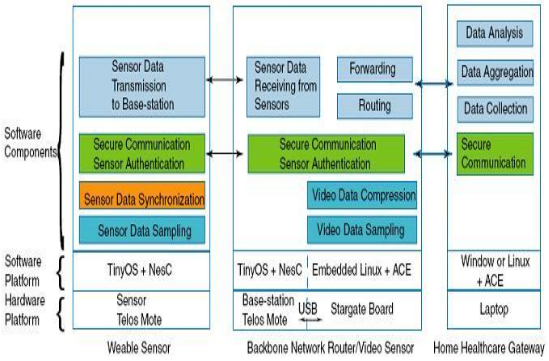


Fig.6 Sample Layered Architecture

5.1.6 Metrics Involved

- Efficiency
  - System lifetime/System resources
- Resolution/Fidelity
  - Detection, Identification
- Latency
  - Response time
- Robustness
  - Vulnerability to node failure and environmental dynamics
- Scalability
  - Over space and time

6. VANET: An Introduction

VANETs may be regarded as a subset of Mobile Ad hoc Networks (MANETs). It is a technology which employs moving cars as nodes in a network creating a mobile network. Each car that participates is used as a wireless router or node by the VANET, just permitting nearly 100 to 300 meters of distance between each other to connect and, in turn, creating a wide range of network. As cars fall out of the signal range and drop out of the network, other cars can join in, connecting vehicles to one another so that a mobile Internet is created. VANETs have grown out of the need to support the growing number of wireless products that can now be used in vehicles [9, 10]. The products may be remote keyless entry devices, personal digital assistants (PDAs), laptops and mobile telephones. As mobile wireless devices and networks become increasingly important, the demand for Vehicle-to-Vehicle (V2V) and Vehicle-to-Roadside (VRC) or Vehicle-to-Infrastructure (V2I) Communication will continue to grow [10].

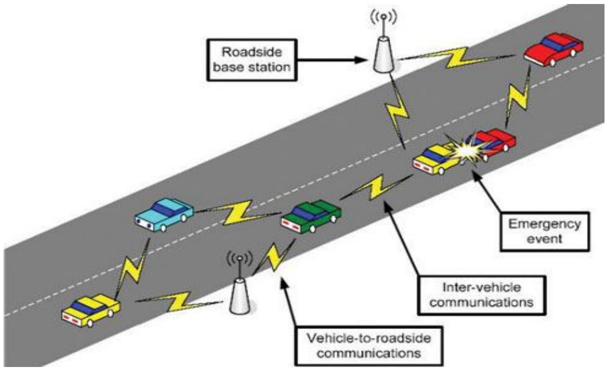

Roadside base station
Emergency event
Inter-vehicle communications
Vehicle-to-roadside communications

Fig. 7 Schematic representation of VANET

VANET an Intelligent Transportation System (ITS), where each vehicle acts as a sender, receiver and router [11] broadcasts information to a vehicular network, which then uses the information for the safety and free-flow of the traffic.

The protocol that has been standardized for communication in VANET is DSRC (**Dedicated short-range communications)** are one-way or two-way short- to medium-range wireless communication channels specifically designed for automotive use, having a communication range between 300 meters to 1 km. The roadside base station provides information to the driver throughout his journey so that he can find a best route to his destination. The information is periodically exchanged. In VANET the moving cars act as nodes in a network creating a mobile network. The autonomous distributed Inter Vehicle Communication (IVCN) does not have any base station. Each vehicle transmits its cruising information and receives another vehicle's information. Each vehicle communicates with unknown and unspecified vehicles accidentally neighbouring on the road. The cruising information that a vehicle needs differs from what another vehicle needs. Therefore, the importance for a vehicle of another vehicle's information grows with decreasing the distance between the vehicle and another vehicle.

As a cooperative approach, vehicular communication systems can be more effective in avoiding accidents and traffic congestions than if each vehicle tries to solve these problems individually.

5.1.7 Standards available

A technical standard is an established norm or requirement. It is usually a **formal document that establishes uniform engineering or technical criteria, methods, processes and practices**.

1. IEEE 802.15.4: It offers fundamental lower network layers of a type of Wireless personal area network (WPAN) targeting mainly low cost, low speed, ubiquitous communication between devices.

2. ZigBee: It is used for high level communication protocols employing small, low-power digital radios based on IEEE 802.15.4 for WPANs. E.g. wireless head phones connecting with cell phones via short range radio.

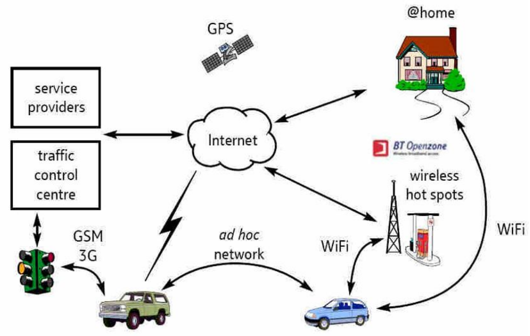


Fig.8 The Connected car scenario.

For communication between vehicles and Road Side Units (RSUs), vehicles must be equipped with some sort of radio interface or On Board Unit (OBU) enabling short-range wireless ad hoc networks to be formed [12]. Vehicles must also be fitted with hardware that permits detailed position information such as Global Positioning System (GPS) or a Differential Global Positioning System (DGPS) receiver. Fixed RSUs, which are connected to the backbone network, must be in place to facilitate communication. The number and distribution of roadside units is dependent upon the communication protocol used. InVANET (Intelligent Vehicular adhoc network) integrates on multiple ad-hoc networking technologies such as WiFi IEEE 802.11p, WAVE IEEE 1609, WiMAX IEEE 802.16, Bluetooth, IRA, ZigBee for easy, accurate, effective and simple communication between vehicles on dynamic mobility. Effective measures like media communication between vehicles as well as methods to track the automotive vehicles can be enabled. InVANET helps in defining safety measures (in vehicles), streaming communication between vehicles, infotainment and telematics. It is estimated that the first systems that will integrate this technology are police and fire vehicles to communicate with each other for safety purposes.

Why Ad hoc networks?

Ad hoc networks are useful when infrastructure is absent, destroyed or impractical. These networks do not require backbone infrastructure support and are easily deployable. Setting up of fixed access points and backbone infrastructure is not always viable as infrastructure may not be present in a disaster area or war zone and may be impractical for short-range radios - Bluetooth (range ~ 10m). Adhoc networks are basically those networks that don't have a base-station. In other words, every device (node) in the network can act as a base and a receiver. A fixed base transmitter is no more required, thus adding to the portability of the network. These networks setup quickly, providing a boon during emergency situations like natural disasters. These find applications in everyday life like a private home network. Having an adhoc network, through which all the devices in a house, like Fridge, Lights etc. can be controlled from any computer in the house. This technology has great potential in the future for many practical applications as it is well suited to free unlicensed spectrum.

6.1.1 Characteristics of VANET

- VANET can be considered a subset of MANET.
- Nodes do not move in any random direction.
- Nodes are powered (energy is not an issue).
- Node contact time is limited
- Intermittent connectivity might occur
- Node speed is bounded
- Mostly high speed, but occasionally stop and slow moving

6.1.2 Applications of VANETs

- Safety–Intersection warning
- Vehicle-based
- Infrastructure-based
- Vehicle probe (travel time estimation, environmental data collection, road surface data collection)
- Emergency vehicle (pre-emptive traffic control)
- Navigation

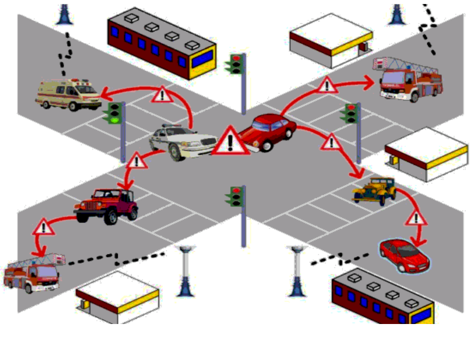


Fig.9 Vehicular Ad hoc Networks

6.1.3 Factors affecting VANETs

- Short radio transmission range
- Omni directional broadcast
- Limited storage capacity
- Dynamic Topologies
- Bandwidth-constrained, variable capacity links
- Energy-constrained

- Limited Physical security
- Scalability
- No prior control messaging
- Hidden terminal problem
- Different traffic volumes
- Different environments (Urban or rural)

6.1.4 Routing Protocols in VANETs

The routing protocols in VANETs may be classified into various categories: **Flat routing protocols, Hierarchical routing protocols, Location-based routing protocols, Hybrid Schemes, Geographical Routing, Routing with dynamic address.**

1. Flat routing protocols: The following protocols fall under this category:

Pro-active (Table driven): Routes are set up based on continuous control traffic and all the routes are maintained all the time. These types of protocols maintain fresh lists of destinations and their routes by periodically distributing routing tables throughout the network. The drawbacks associated with them are that large amount of data exists for maintenance and the reaction is slow on restructuring and failures. E.g. FSR (Fisheye State Routing), FSLS* (Fuzzy Sighted Link State), OLSR (Optimized Link State Routing), TBRPF (Topology Broadcast Based on Reverse Path Forwarding), etc. The prime characteristics of such protocols are: Large routing table, large flooding of routing information (for large network population), and frequent updating when mobility is high. These types of protocols are most suited for network with small population.

Re-active (On-demand): Does not take initiative for finding routes but establish routes "on demand" by flooding a query. E.g., AODV(adhoc On-demand Distance Vector routing), DSR(Dynamic Source Routing), TORA(Temporally-Ordered Routing Algorithm), etc. As the communication takes place between the leaders of the groups, overhead of routing processing is reduced. The problem associated with this is **-** the overhead of routing between the groups.

2. Hierarchical routing protocols: When the size of a network increases, the flat routing schemes become infeasible because of link and processing overhead. Thus, hierarchical routing protocols were developed. Here the network is partitioned into various groups where each node is assigned different function within and outside the group. E.g. CGSR(Cluster head-Gateway Switch Routing), HSR (Hierarchical State Routing), ZRP (Zone Routing Protocol), LANMAR (Landmark Ad Hoc Routing Protocol), etc.

3. Location-based routing protocols: This protocol is aided by GPS where every node has its location information. Universal time is provided by the aid of GPS. It uses geographical forwarding to send packets.

4. Hybrid Schemes: It is a combination of reactive and pro-active branches. Routing may be divided into two categories: Inter zone and intra zone routing where the former uses the reactive protocols and the latter the pro-active protocols. E.g. Zone routing protocol (ZRP).

5. Geographical Routing: The nodes know their geo coordinates (GPS) i.e. the geographic position. A route is found which moves the packet close to the destination. The information is propagated through flooding. E.g. DREAM, GPSR, LAR.

6. Routing with dynamic address: Use of address-based routing protocols requires that each of the participating nodes be assigned a unique address. This implies that a mechanism for assigning a unique address to vehicles should be there. Unfortunately these protocols do not guarantee the avoidance of allocation of duplicate addresses in the network. [13].

6.1.5 Architecture of VANET

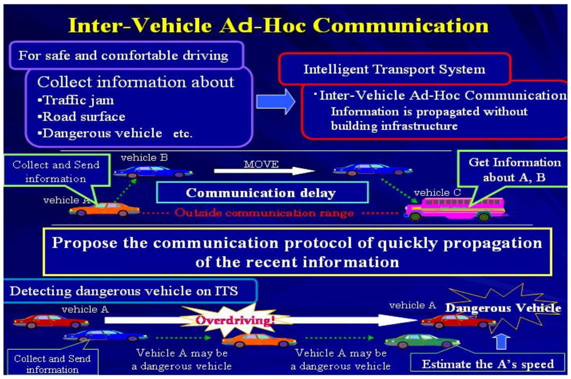

Inter-Vehicle Ad-Hoc Communication
For safe and comfortable driving
Collect information about
•Traffic jam
•Road surface
•Dangerous vehicle etc.
Intelligent Transport System
·Inter-Vehicle Ad-Hoc Communication
Information is propagated without building infrastructure
Collect and Send information
vehicle B
MOVE
Get Information about A, B
Communication delay
vehicle A
vehicle C
Outside communication range
Propose the communication protocol of quickly propagation of the recent information
Detecting dangerous vehicle on ITS
vehicle A
Overdriving!
vehicle A
Dangerous Vehicle
Collect and Send information
Vehicle A may be a dangerous vehicle
Vehicle A may be a dangerous vehicle
Estimate the A's speed

Fig.10 Architecture of VANET

6.1.6 Metrics Involved

- Receipt rate
- Dissemination speed
- Redundancy

6.1.7 Standards available

The standards available in VANET are:

1. Dedicated Short Range Communication (DSRC): DSRC spectrum is allocated for vehicle-to-vehicle and infrastructure-to-vehicle communication in the U.S. It is meant to save lives and improve traffic flow, and also to provide value through private applications. It is an IEEE 802.11 based technology.

2. IEEE 1609 – A standard for Wireless Access in Vehicular Environments (WAVE) (IEEE 802.11p). Security Services for applications and management messages, defines secure message formats and processing. It also defines the circumstances for using secure message exchanges and how those messages should be processed based upon the purpose of the exchange.

6.1.8. Problems in a mobile environment

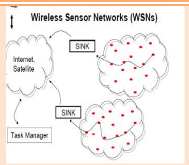
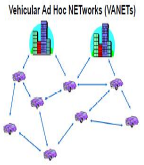
- Variable Bandwidth
- Disconnected Operation
- Limited Power
- Implications on distributed file system support**.**

VANET is an important component of Intelligent Transportation Systems. It has a future potential with regard to applications and services to its customer. It is a special kind of mobile Ad Hoc network constituting wireless equipped (road side) vehicles forming a network with no additional infrastructures.

7. Conclusion

Ad Hoc Wireless Sensor Networks have the capacity to revolutionize the contemporary technical arena. Offering a more convenient means of communication, this idea of infrastructure-less networks can transform many applications, including military strategy, home security, information transfer, environment monitoring, and surveillance. This concept can initiate wave of wireless interaction that the world has not yet seen.

Table 1: WSN V/s VANET

Factors/ Issues	WSNs	VANETs
Nodes deployed	Very large	**Not many**
Population of nodes	Densely populated	Sparsely populated
Failure rate	High	Low
Communication	Broadcast	Point-to-Point
Metrics	Efficiency, Resolution, Latency, Scalability, Robustness	Receipt rate, Dissemination speed Redundancy
Power	Limited	Not an issue
Identification	Not global	-
Memory	Limited	High
Topology	Dynamic	Dynamic
Standards	ZigBee, IEEE 802.15.4, ISA100, IEEE 1451	DSRC,IEEE 1609
Structure	 Wireless Sensor Networks (WSNs) SINK Internet, Satellite SINK Task Manager	

REFERENCES

[1] Römer, Kay; Friedemann Mattern (December 2004). "The Design Space of Wireless Sensor Networks". IEEE Wireless Communications 11 (6): 54–61. doi: 10.1109/MWC.2004.1368897. http://www.vs.inf.ethz.ch/publ/papers/wsn-designspace.pdf.
[2] Thomas Haenselmann (2006-04-05). "Sensor net works". GFDL Wireless Sensor Network textbook. Retrieved on 2006-08-29.
[3] JAMAL N. AL-KARAKI, AHMED E. KAMAL," ROUTING TECHNIQUES IN WIRELESS SENSOR NETWORKS: A SURVEY**",** *IEEE Wireless Communications • December 2004*
[4] D. Braginsky and D. Estrin, "Rumor Routing Algorithm for Sensor Networks," *Proc. 1st Wksp. Sensor Networks and Apps.*, Atlanta, GA, Oct. 2002.
[5] Heinzelman, A. Chandrakasan and H. Balakrishnan, "Energy-Efficient Communication Protocol for Wireless Microsensor Networks," *Proc. 33rd Hawaii Int'l. Conf. Sys. Sci.*, Jan. 2000.
[6] S. Lindsey and C. Raghavendra, "PEGASIS: Power-Efficient Gathering in Sensor Information Systems," *IEEE Aerospace Conf. Proc.*, 2002, vol. 3, 9–16, pp. 1125–30.
[7] A. Manjeshwar and D. P. Agarwal, "TEEN: a Routing Protocol for Enhanced Efficiency in Wireless Sensor Networks," *1st Int'l. Wksp. on Parallel and Distrib. Comp. Issues in Wireless Networks and Mobile Comp.*, April 2001.
[8] Y. Yu, D. Estrin, and R. Govindan, "Geographical and Energy-Aware Routing: A Recursive Data Dissemination Protocol for Wireless Sensor Networks," UCLA Comp. Sci. Dept. tech. rep., UCLA-CSD TR-010023, May 2001.
[9] Raya, M. and Hubaux, J., "The Security of Vehicular Ad Hoc Networks", in Proceedings of the 3rd ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN 2005), Alexandria, VA, pp 1 – 11.
[10] Harsch, C., Festag, A. & Papadimitratos, P., "Secure Position-Based Routing for VANETs", in Proceedings of IEEE 66th Vehicular Technology Conference (VTC-2007), Fall. 2007, September 2007, pp 26 – 30.
[11] Jinyuan, S., Chi, Z. & Yuguang, F., "An ID-based Framework Achieving Privacy and Non-Repudiation", in Proceedings of IEEE Vehicular Ad Hoc Networks, Military Communications Conference (MILCOM 2007), October 2007, pp 1 – 7.
[12] Stampoulis, A. & Chai, Z., A Survey of Security in Vehicular Networks, http://zoo.cs.yale.edu/~ams257/projects/wireless-survey.pdf. (accessed: May 29, 2010).
[13] Mohandas, B. & Liscano, R., "IP address configuration in VANET using centralized DHCP", in Proceedings of 33rd IEEE Conference on Local Computer Networks, Montreal, Canada, October 2008.

Vitae

Vandana Jindal is currently working as an Assistant Professor in the department of Computer Science at D.A.V College, Bathinda. She holds degrees of B.Tech, MCA, M.Phil. Since January 2009, she has been with the Thapar University, Patiala in Punjab as a Ph.D. student. Her research interests include database management systems, wireless sensor networks. She is a member of IEEE and IEI.

A K Verma is currently working as Assistant Professor in the department of Computer Science and Engineering at Thapar University, Patiala in Punjab (INDIA). He received his B.S. and M.S. in 1991 and 2001 respectively, majoring in Computer Science and Engineering. He has worked as Lecturer at M.M.M. Engg. College,Gorakhpur from 1991 to 1996. From 1996 he is associated with the Thapar University. He has been a visiting faculty to many institutions. He has published over 100 papers in referred journals and conferences (India and Abroad). He is member of various program committees for different International/National Conferences and is on the review board of various journals. He is a senior member (ACM), MIEEE, LMCSI (Mumbai), GMAIMA (New Delhi). He is a certified software quality auditor by MoCIT, Govt. of India. His main areas of interests are: Bioinformatics, database management systems and Computer Networks. His research interests include wireless networks, routing algorithms, securing ad hoc networks and design/develop applications for other fields based on IT.

Seema Bawa holds M.Tech (Computer Science) degree from IIT Kharagpur and Ph.D. from Thapar Institute of Engineering & Technology, Patiala. She is currently Professor and Dean of Students' affairs (DOSA). Her areas of interest include Parallel and distributed computing, Grid computing, VLSI Testing and network management. Prof. Bawa is member of IEEE, ACM, Computer society of India and VLSI Society of India.