Wireless Sensor Network- A Survey: Design Challenges, Security issues, Application and its Routing Protocols

Abarna Sri R[1] , K.Devasenapathy [2]*

Abstract

WSN – Wireless Sensor Network in a wireless network in which more than thousands of nodes (motes) were deployed to monitor the environmental conditions which is difficult for the humans to do. Each and all nodes in the network establish communication with each other to exchange information among them. The primary purpose of Wireless Sensor Networks (WSNs) is to engage in monitoring activities.Two distinct forms of communication exist among the nodes in a Wireless Sensor Network (WSN), namely Single hop communication – the nodes communicate with each other directly, multi hop communication – here it communicates with many nodes. In this article we will come to know about the challenges we face while designing the WSN, along with security issues, applications of WSN and its routing protocol.

Keywords: Cluster head, Architecture, Sensor nodes, Sink, Base Station, Gateway

I. INTRODUCTION

For data and voice communication, radio frequency waves are used. Wireless Ad-Hoc Network is classified as MANET, WMN and WSN [1] (figure 1).

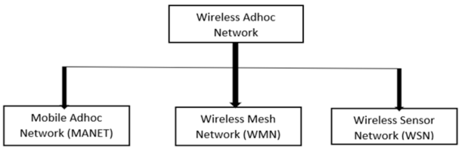

Wireless Adhoc Network
Mobile Adhoc Network (MANET)
Wireless Mesh Network (WMN)
Wireless Sensor Network (WSN)

Figure 1 : Classification of Wireless Adhoc Network

MANET vs. WSN

An ad hoc network is a short-range, instant network in which devices can be connected immediately with self-configuration. It is permissible for all wireless devices connected within the communication range to collaborate. The way MANET works is that it can set up a network anywhere and at any time without the right infrastructure to support the user's mobility. The performance of the nodes in the networks in MANET is dependent on the stability of the network architecture and is subject to severe blocking. The transceiver provides support for nodes in the wireless ad hoc network. Because the MANET's nodes form an independent network from an infrastructure, they ought to be able to manage their own network[2]. The network's nodes have to deal with issues like routing and security because of their complexity. The nodes that make up an ad hoc network should be able to change their topology quickly and unexpectedly. The process of transmitting information using an electrical conductor between two or more points is referred to as wireless communication. It offers features like portability and location independence to the user. The term "wireless sensor network" refers to a collection of thousands of nodes that are linked by signals to exchange data with other networks and facilitate communication. In order to detect the area of interest, the nodes of the wireless sensor network are dispersed widely. The power supply, bandwidth, and computational capacity of the WSN nodes are limited. The motes (nodes) ought to be capable of adapting to changes in the WSN's number of nodes. The failure of the nodes can be affected by changes in the environment. As a result, WSN nodes are frequently added and removed (see figure 2). Wireless Sensor Networks (WSNs) are an emerging class of wireless networks that are gaining popularity in various domains, including commercial and military applications. A WSN comprises multiple individual sensor devices

Department of Computer Science
Karpagam Academy of Higher Education, Coimbatore, Tamil Nadu, India
*Corresponding Author

distributed throughout the network, which are employed to observe and monitor physical or environmental conditions [3]. AWSN is a network of interconnected, microscopic sensor nodes that share data and information with one another. These nodes transmit environmental data to a base station, such as temperature, pressure, humidity, or levels of pollution. The latter either sends the data to a wired network or causes an alert or action, depending on the type and volume of data being watched.

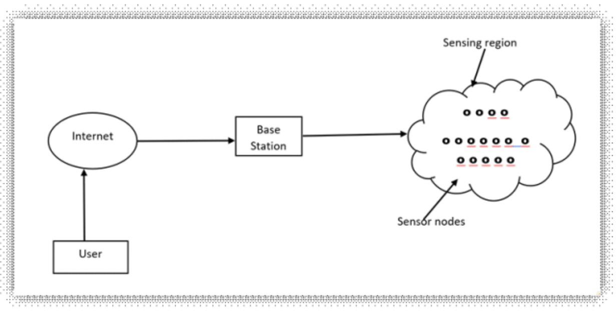


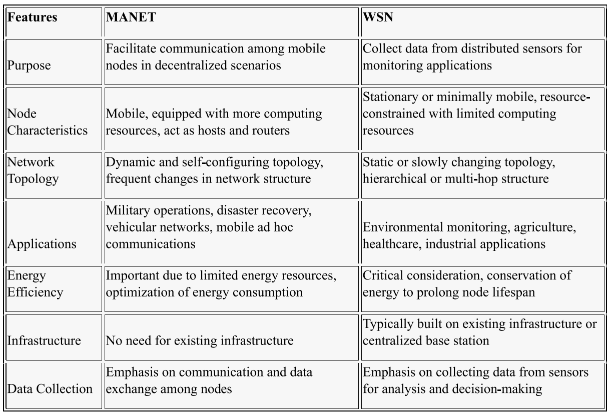
Figure 2 : Wireless Sensor network

The failures in the nodes have to be updated to the base station.Due to the node failure, we may face many conflicts such as changes in the route that the data has to be transmitted, immediate employment of the new nodes in the same path and even the data flow.

Since the sink node (base station) receives the collected information from multiple sensor nodes via the network and distributes it to the end user, the placement of the sink node has a great impact on the life and power consumption in WSN. The WSN provides a variety of sensors with the following key features [4].

- Data acquisition and signal conditioning
- Temporary storage of received data.
- Data processing.
- Analysis of processed data for diagnostics and alert generation as needed.
- Self-monitoring.
- Scheduling and implementation of measurement tasks.
- Managing sensor node configurations.
- Receive, send, and forward data packets.
- Communication and Networking Management and Coordination.

Features of MANET vs. WSN



Features	MANET	WSN
Purpose	Facilitate communication among mobile nodes in decentralized scenarios	Collect data from distributed sensors for monitoring applications
Node Characteristics	Mobile, equipped with more computing resources, act as hosts and routers	Stationary or minimally mobile, resource-constrained with limited computing resources
Network Topology	Dynamic and self-configuring topology, frequent changes in network structure	Static or slowly changing topology, hierarchical or multi-hop structure
Applications	Military operations, disaster recovery, vehicular networks, mobile ad hoc communications	Environmental monitoring, agriculture, healthcare, industrial applications
Energy Efficiency	Important due to limited energy resources, optimization of energy consumption	Critical consideration, conservation of energy to prolong node lifespan
Infrastructure	No need for existing infrastructure	Typically built on existing infrastructure or centralized base station
Data Collection	Emphasis on communication and data exchange among nodes	Emphasis on collecting data from sensors for analysis and decision-making

Applications of MANET Vs WSN :

MANET are mostly used for Battlefield communication and Mini site operation and search-and-rescue. Data acquisition is carried out with robots3]. Examples: Personal area networking using PDAs, laptops, and hand phones, vehicular networks, students on campus, cellular network and wireless Hot Spot extension, etc. [5].Vehicular networks facilitate wireless communication among vehicles, enabling enhanced connectivity and information exchange on the road.Students on a campus can establish personal area networks using their devices, fostering seamless communication and collaboration within the educational environment.Cellular networks and the extension of wireless hotspots offer widespread connectivity options, ensuring internet access and network availability in various locations.Personal area networking utilizing PDAs, laptops, and mobile phones provides wireless connectivity, enhancing communication and data transfer capabilities for individuals.Vehicular networks enable wireless communication between vehicles, promoting efficient information sharing and enhancing connectivity on the go.On a university campus, students can create personal area networks with their devices, facilitating easy communication and collaboration within the academic community.The expansion of cellular networks and wireless hotspots allows for broad connectivity, extending internet access and network coverage to a larger area. WSNs, on the other hand, are made specifically for a variety of applications, including biomedical applications, traffic monitoring, fire detection, industrial automation, field experiments, environmental monitoring, seismic and structural monitoring, object tracking, physical security for military operations, etc.

II. WSN's problems with design

Due to the compact size of nodes in a wireless sensor network, their power supply may be depleted in the near future as a result of their numerous small components.Node failure may be the final result. The lifespan of WSN nodes cannot be predicted [6, 7, 8, and 9]. Since the WSN has a variety of nodes, heterogeneity should be supported. During the transmission process, the wireless sensor network's number of nodes fluctuates due to the possibility of death-related additions or deletions. Fault tolerance is just one of many other design issues that WSN faces. Node failure and changes to the network topology are very likely in WSN. Therefore, in the event of node failure or topology changes, network designers must make their networks robust and dependable. No matter what happens to nodes or how the topology changes, the network should work well and smoothly.

The Lifetime: The WSN should require little power to operate for a considerable amount of time. They ought to last between six and twelve months. It should be noted that the WSN only allows one 3V battery to power each node for the duration of its existence. The WSN protocol should be designed so that the node uses as little power as possible. This will make the WSN last longer.

Scalability: New nodes should always be supported by the WSN design. Likewise, some WSN applications might require a critical number of sensor hubs, so the plan should uphold an enormous number of hubs.

Aggregation of Data : The proximity of the sensor nodes in the WSN greatly increases the likelihood that the adjacent nodes will produce comparable data. As a result, the most expensive WSNs are outbound and inbound data, which must be aggregated to avoid duplicate data. At various levels of the WSN, the data must be aggregated to ensure that only the necessary data is sent and received, eliminating redundant data [10, 11].

Cost:The projected expense for each sensor node in a WSN is approximately $1, reflecting the potential high costs associated with deploying a significant number of nodes. Hence, developers of WSNs must determine the optimal quantity of nodes required for their specific application to manage expenses effectively [12].

Environment: The WSN's design should make it possible for the WSN to survive in any environment, regardless of how harsh the WSN's deployment environment may be.

Heterogeneity assistance: WSN-specific protocols must be capable of supporting a variety of sensor node types and applications.

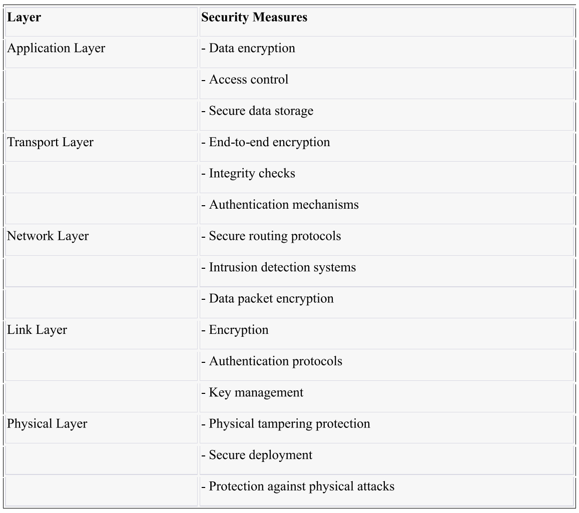
Operation on one's own: WSNs may be deployed in places where humans cannot live, so they must be able to organize, reorganize, and operate on their own.

Memory and processing capacity limitations: All WSN designs ought to require little processing and memory because sensor nodes have limited processing, power, and memory capabilities.

III. WSN security concerns

Layers are used in the design of WSN. The sensor is shielded from a variety of threats thanks to these layers. The safety of wireless sensor networks is in need of some attention[13, 14]. Limited physical resources like dynamically changing topologies, frameworks without infrastructure, power supplies, storage capacity, or wireless communication between sensor nodes, and very low communication are typical issues. bandwidth. For safe data communication and routing in WSNs, numerous analysts have proposed numerous threat handling models and security protocols.

Figure 3 shows the layer model of security in wireless sensor networks [15].



Layer	Security Measures
Application Layer	- Data encryption
	- Access control
	- Secure data storage
Transport Layer	- End-to-end encryption
	- Integrity checks
	- Authentication mechanisms
Network Layer	- Secure routing protocols
	- Intrusion detection systems
	- Data packet encryption
Link Layer	- Encryption
	- Authentication protocols
	- Key management
Physical Layer	- Physical tampering protection
	- Secure deployment
	- Protection against physical attacks

Figure 3 : Layer Model of Security in Wireless Sensor

Secure communication should always be available through a sensor network. General security necessities are accessibility, privacy, trustworthiness and confirmation. Source localization, self-organization, and data freshness are all examples of secondary requirements. The information sent over the sensor network is shielded from attacks thanks to these requirements.

Security Difficulties We sum up security requesting circumstances in sensor networks from as follows:

- Keeping aid intake to a minimum and maximizing protection performance [16].

- The deployment of sensor networks increases the number of link attacks, ranging from passive eavesdropping to active interference.

- Handling intra-group communications involves transitional hubs to ensure uninterrupted data transfer [17].

- The characteristics of wireless communication make wired-based security schemes unsuitable.

- The affair becomes more complicated due to the large scale of the network and node mobility.

- The network topology is dynamic due to node additions and failures.

- Attacks are primarily responsible for security issues, with WSN base stations typically considered trustworthy. Most studies focus on security issues between sensor nodes.

- If there were no attacks, there might not be a need for protection. However, due to their deployment environments and resource limitations, sensor networks are more vulnerable to attacks compared to other networks, such as wireless LANs.

- Attacks can be categorized as external or internal. In an external attack, the attacking node is not authorized to be a member of the sensor network.

Internal attacks are more challenging to detect and prevent, posing higher security risks. Compromised nodes can:

- Steal secrets and techniques from encrypted data that passes through them.

- Submit false information to the network.

- Declare regular nodes to be compromised.

- Introduce various routing attacks, such as selective forwarding, black hole, altered routing information, etc., to compromise routing. These activities are difficult to identify, and standard encryption techniques are ineffective in preventing them since the compromised nodes possess the necessary game name information, including keys.

- Compromised nodes may also engage in arbitrary behaviour and collaborate with other compromised nodes. A wireless sensor node's components include:

A wireless sensor network primarily consists of sensor nodes, which are small devices capable of sensing and storing information about their immediate environment. The price of these devices has been constantly decreasing due to advancements in semiconductor technology.

The essential components of these small devices include:

- Microprocessor: A microprocessor is a small computer on a chip that manages the operations of other connected devices and performs significant tasks. It typically includes a central processing unit (CPU), RAM memory, and necessary peripherals. Microprocessors are commonly used in embedded systems of small to very small sizes due to their low power consumption and moderate to high processing capabilities.

- Transmitter: The transmitter-receiver is used for communication, allowing the sensor nodes to send and receive commands and data. Radio frequency is the preferred mode of communication for WSNs, with sensor nodes often utilizing the ISM frequency range for industrial, scientific, and medical applications.

- Flash Memory: Wireless sensor nodes commonly employ flash memories due to their small size and increasing storage capacity. Flash memory is used for both user memory and program memory in these nodes, and the size of the external memory depends on the specific requirements of the program.

- Power Supply: Power consumption in sensor nodes is primarily driven by activities such as data collection, processing, and communication. Data transmission often consumes a significant portion of the energy. Sensor nodes typically store electrical energy using batteries, which have become more affordable. These batteries are often designed for single-use applications.

Comparison between wireless sensor networks and wireless mesh networks: Wireless sensor networks are mainly used in operations, environmental monitoring, industrial surveillance, critical infrastructure, and military applications. Compared to network organizations, WSNs have lower data capabilities and power-saving requirements. They are frequently designed to operate with low activity, resulting in significant power savings. Attempts have been made to implement VoIP over IEEE 802.15.4, the standard for low-rate wireless personal area networks, but with limited success.

The key differences between WSNs and mesh networks include:

- WSN traffic has a lower data rate and is less complex compared to mesh networks.

- WSN traffic is usually application-specific, meaning that the design of the nodes is driven by the application and cannot be easily changed.

- WSN nodes are generally less reliable than mesh network nodes due to their small size.

- The radio range of WSNs is limited, but they can have a higher density of nodes.

IV. Protocols for Wireless Sensor Network Routing

Routing protocols in WSNs determine how nodes communicate with each other and how data is transferred between them. There are different types of routing protocols for WSNs, including:

1. Node-centric routing: These protocols focus on individual nodes and their connectivity to the network.

2. Data-centric routing: These protocols are based on the content or data being transmitted and aim to efficiently route data to specific destinations.

3. Source-initiated routing: These protocols are initiated by the source node, which determines the path for data transmission.

4. Destination-initiated routing: These protocols are initiated by the destination node, which controls the data delivery process.

Each type of protocol has its own characteristics and suitability for specific applications and network requirements.Figure4: depicts the fundamental classification of routing protocols:

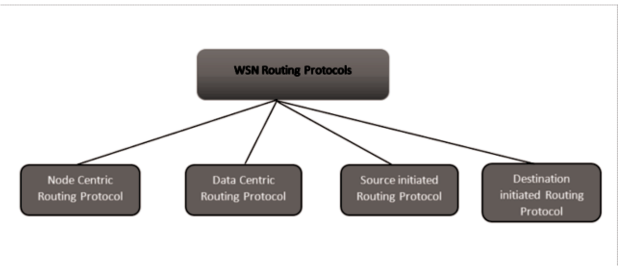

WSN Routing Protocols
Node Centric Routing Protocol
Data Centric Routing Protocol
Source initiated Routing Protocol
Destination initiated Routing Protocol

Figure 4: Wireless Sensor Network Routing Protocols

Low energy adaptive clustering hierarchy (LEACH):

The Drain protocol is a coordination mechanism that ensures equal distribution of battery usage among sensor nodes within a network. In this protocol, multiple clusters are formed within the network, with one node designated as the cluster head or routing node for all the other nodes within the cluster. The Filter protocol allows for multiple clusters in the network based on the availability of sensor nodes, while selecting one node as the cluster head based on battery level to monitor the overall routing of the other nodes [18]. The Drain protocol incorporates randomization and dynamically selects cluster heads from a pool of nodes, ensuring robustness by preventing a single node from being continuously selected as the cluster head and exhausting its battery. Sensor nodes autonomously determine their cluster head based on predefined probability rules and communicate this information to other nodes.

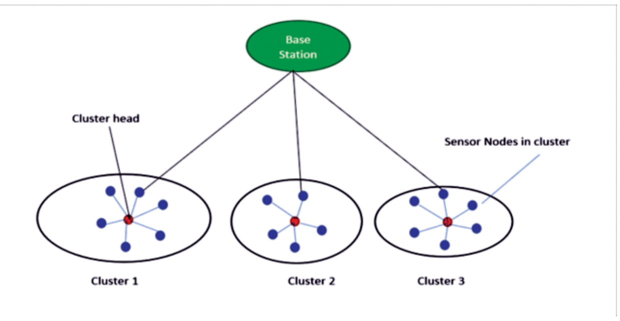


Figure 5 : Diagrammatic portrayal of Bunch Head and hubs.

Data-centric :

In numerous remote sensor networks, the value lies more in the data collected than in the individual nodes themselves. Therefore, data-driven routing methods focus on transmitting information based on specific characteristics rather than gathering data from a particular node. Data-driven routing relies on a characteristic-based naming scheme to describe the properties of the data. This allows the sink node to query specific areas and collect data with specific properties, enabling efficient and targeted data retrieval. The naming scheme helps in organizing and categorizing the data based on its attributes, facilitating effective data-driven routing in the network.

Sensor protocols for information via negotiation (SPIN):

SPIN stands for Sensor Protocol for Information via Negotiation, which is a protocol specifically designed for wireless sensor networks. SPIN is used to address issues such as excessive flooding and unnecessary communication that can occur in other protocols [19].

The primary concept behind SPIN is that sharing the metadata (information about the data collected by a node) can require fewer resources than sharing the actual data itself. Nodes in the network have a resource manager that monitors and adjusts the utilization of resources based on the metadata. This approach helps optimize resource usage in the network.

The negotiation aspect of SPIN refers to the exchange of metadata between nodes to determine the relevance and need for sharing actual data. By negotiating and selectively transmitting relevant metadata, SPIN aims to reduce unnecessary communication and conserve network resources.

It's important to note that SPIN is a fictional protocol used as an example in wireless sensor network research. It is not an actual standardized protocol in use.

Objective started (Dst-intiated) :

Objective initiated protocols, such as Directed Diffusion (DD) and Filter, are routing protocols where the path establishment originates from the destination node.

Directed Diffusion is a data-driven routing method used to gather and disseminate information in a wireless sensor network. This routing protocol is designed to be energy-efficient and power-saving, thereby prolonging the network's lifespan. In Directed Diffusion, communication occurs between nodes, eliminating the need for addressing.

The basic principle of Directed Diffusion involves data-centric communication, where nodes advertise their data interests or queries to the network. Other nodes that have relevant data respond by forwarding the requested data towards the sink or destination node. This process creates a dynamic path for data flow based on data interests and responses.

By utilizing data-centric communication and adapting the routing based on data demands, Directed Diffusion aims to optimize energy consumption and efficiently transmit relevant data within the network.

It's worth noting that Filter is not specifically mentioned in relation to Objective Initiated protocols. However, both Directed Diffusion and Filter are examples of data-driven routing protocols used in wireless sensor networks.

Source-started (Src-intiated):

Source-started protocols, also known as source-initiated protocols, are routing protocols in which the source node initiates the communication and data transmission process. One example of a source-started protocol is the TWIST (The Weather Information Service Through a sensor network) protocol.

In source-started protocols, the source node announces or advertises its data availability to the network when it has information to share. The routing path is then established from the source node to the destination based on this announcement.

TWIST is a specific example of a source-started protocol designed for weather information services using a wireless sensor network. In TWIST, the source node, which collects weather data, initiates the transmission by broadcasting the availability of weather information. The routing path is then formed from the source node to the destination node, allowing the weather data to be efficiently transmitted through the network.

Source-started protocols provide a way for source nodes to actively initiate data transmission and establish paths to deliver the data to the intended destinations. This approach allows for flexibility in data dissemination and can be beneficial in scenarios where specific nodes or destinations need to receive the data.

V. Conclusion

In conclusion, routing protocols play a crucial role in facilitating continuous and efficient communication between source and destination nodes. The performance, management, and reliability of a network often depend on the selection of an appropriate routing protocol. In wireless sensor networks (WSNs) and ad hoc networks, routing protocols are typically designed to be loop-free, ensuring effective data transmission and minimizing network overhead.WSN routing protocols can be categorized in various ways based on their characteristics, objectives, and techniques used. Examples include data-driven routing protocols, source-initiated protocols, and objective-initiated protocols. Each type of protocol offers different advantages and is suited for specific network requirements and application scenarios.Choosing the right routing protocol is critical in optimizing network performance, minimizing energy consumption, and ensuring reliable communication. Factors such as network size, topology, traffic patterns, and resource constraints need to be considered when selecting a routing protocol for a wireless sensor network or ad hoc network. Continued research and development in routing protocols are essential to further enhance the efficiency, scalability, and robustness of communication in these networks, ultimately enabling various applications and services to operate effectively in diverse environments.

References

[1] G Yin, G Yang, W Yang, B Zhang, W Jin. An energy-efficient routing algorithm for wireless. In. International Conference on Internet Computing in Science and Engineering (ICICSE'08), IEEE, China; 2008.

[2] Zang Z, Qi JD, Cao YJ. A robust routing protocol in wireless sensor networks. In: IET International Conference on Wireless Sensor Network. China: IET; 2010. pp. 276-29

[3] Ehsan S, Hamdaoui B. A survey on energy-efficient routing techniques with QoS assurances for wireless multimedia sensor networks. IEEE Communications Surveys & Tutorials. 2012;14(2), PP. 265-278.

[4] Hassan SR. Performance analysis of ZigBee based wireless sensor networks [thesis]. Lahore: GCU; 2014. Available from: http://library.gcu.edu.pk/theses.htm

[5] Nawaz R. Performance analysis of WLAN based routing protocols [thesis]. Lahore: GCU; 2015. Available from: http://library.gcu.edu.pk/theses.htm

[6] Shabbir N, Nawaz R, Iqbal MN, Zafar J. Routing protocols for a small scale WLAN based wireless sensor networks. In: 9th International Conference on Sensing Technologies. New Zealand: IEEE; 2015

[7] Khan AA. A survey of routing protocol in wireless sensor networks [thesis]. Lahore: GCU; 2016. Available from: http://library.gcu.edu.pk/theses.htm

[8] Bakr BA, Lilien L. LEACH-SM: A protocol for extending wireless sensor network lifetime by management of spare nodes. In: International Symposium on Modelling and Optimization in Mobile, Ad Hoc and Wireless Networks (WiOpt); IEEE; New Jersey, Princeton; 2011

[9] Y.-C. Tseng, M.-S. Pan and Y.-Y. Tsai, "Wireless sensor networks for emergency navigation," IEEE Computer, Vol. 39, No. 7, pp. 55–62, 2006.

[10] C.-Y. Chong and S. P. Kumar, "Sensor networks: evolution, opportunities, and challenges," Proceedings of IEEE, Vol. 91, No. 8, pp. 1247–1256, 2006.

[11] S. Cheekiralla and D. W. Engels, "A functional taxonomy of wireless sensor network devices," Proceedings of the 2005 International Conference on Broadband Networks Conference, BroadNets 2005, Vol. 2, pp. 949–956, 2005.

[12]Ankur O., Prabhakar L., "MANET: History,Challenges and Applications", International Journal of Application or Innovation in Engineering & Management (IJAIEM),

Volume 2, Issue 9, September 2013.

[13]Gang W.,Guodong W., “An Energy Aware Geographic Routing Protocol for Mobile Ad Hoc Networks”, International Journal of Software informatics, Vol. 4, No. 2, pp. 183-196, June 2010.

[14]Ashwini P. and et al., “A Survey of Network Security in Mobile Ad-Hoc Network”, IOSR Journal of Computer Engineering, Volume 18, Issue 5, Ver. III (Sep. 2016), PP 29-36.

[15]Samba S. and et al., ““A Survey on Mobile Ad-Hoc Wireless Network”, Information Technology Journal, ISSN: 1682-6027, Volume 3, Issue 2, 2004.

[16]Amit Sh., Nitin Ch., “Overview of Routing Protocols in MANET’s and Enhancements in Reactive Protocols’, Beaumont TX 77710 project, 2008.

[17]Ajay J. and et al., “Wireless Sensor Network: Architectural Design issues and Challenges”, International Journal on Computer Science and Engineering, Vol. 02, No. 09, 2010.

[18]Gowrishankar.S. and et al., “Issues in Wireless Sensor Networks”, Proceedings of the World Congress on Engineering, London, U.K Vol. I, July 2 - 4, 2008.

[19]Madhav B. and Anagha R., “Wireless Sensor Network”, International Journal of Computer Engineering Science (IJCES), Vol. 2, Issue 3, March 2012.