A Critical Review: SANET and Other Variants of Ad Hoc Networks

Ekansh Chauhan, Manpreet Sirswal, Deepak Gupta and Ashish Khanna

June 2, 2021

A critical Review: SANET and other variants of ad hoc networks

Ekansh Chauhan[1,*], Manpreet Sirswal[1], Dr. Deepak Gupta[1], Dr. Ashish Khanna[1]

[1] Maharaja Agrasen Institute of Technology

[*] Corresponding Author. Email-id: echauhan09@gmail.com (Ekansh Chauhan)

echauhan09@gmail.com, manpreetsirswal9102@gmail.com, deepakgupta@mait.ac.in, ashishkhanna@mait.ac.in

A B S T R A C T

In recent years the technology has advanced and developed at a tremendous rate, wireless mobile ad hoc networks and its variants have played a salient role in several critical applications. Due to the different topologies and features the variants of ad hoc networks have become a networking standard to explore the unmapped and unplumbed areas of land and oceans where infrastructure-based networks cannot be installed. The variants of ad hoc networks, like, flying ad hoc networks (FANETs) have nodes that operate on high altitudes with lower node density and in Vehicular ad hoc networks (VANETs) nodes operate on the ground with higher mobility. Similarly, Sea ad hoc networks (SANETs) is relatively an unexplored area of research. Therefore, in the presented exposition, a detailed critical review of SANETs is given. Additionally, differences between SANETs and other variants of ad hoc networks are also provided. SANETs facilitate applications for seismic monitoring, environment monitoring, military uses and many more. The paper also provides the overview of the challenges needed to overcome for the development of SANET system. Some of the challenges are security and peer to peer connections. Different deployment procedures and their issues related to the discussed technology are also scrutinized. Moreover, the different routing protocols are analysed and their applications in SANETs are studied. Finally, future areas of research and development in SANETs are also discussed.

KEYWORDS : MANET, VANET, FANET, SANET, AUV, USV, Distributed system.

INTRODUCTION

According to [1], "A wireless ad hoc network is a bracket of communication nodes which can compose and sustain a network among themselves, without the help of a main station or a leading administrator (infrastructure)". In recent years the characteristics of the wireless networks provided the opportunity for many researchers to discover the types of ad hoc networks, MANET, VANET, and FANET [2]. There have been multiple surveys and innumerable researches conducted on these ad hoc networks. So, examination of a new ad hoc network called Sea ad hoc network (SANET) is done.

A mobile ad hoc networks (MANETs) consists of different mobile routers connected to form random diagrams and figures. The routers are presently independent to interchange arbitrarily and systematize themselves randomly; therefore, the topology of network might modify quickly and uncertainly [3].
Vehicular ad hoc networks (VANETs) are a more challenging version of MANETs. Inquiry in the field of automative industries as well as wireless networking is being conducted on it [4, 5]. In VANET the nodes are constituted by moving vehicles. The extraordinary speed of mobile vehicles is the main distinguishing feature of VANETs [6].
According to [7] "Flying ad hoc networks (FANETs) are ad hoc network between UAV's. With the progress of embedded systems now it is feasible to produce small or mini UAV's at a low cost". However, coordination and collaboration of multiple UAVs is a very complex system and can't be handled by one UAV leading to the formation of multi UAV system, which makes FANET more challenging and acts as a distinguishing factor for it.
Most of the existing work in the field of ad hoc networks concentrates on land and air, totally neglecting the ocean. The ocean covers about 2/3rd of the earth's surface and it has been interesting humans for centuries now. Yet the majority of ocean is unexplored. In the fields of military and transportation, the ocean has played a notable role in the past centenary [8]. Hence the need of building a wireless data acquisition network called ad hoc network for aquatic applications arises, which is called as SANET.
Moreover, with the increase in global warming the polar ice sheets are melting at a very rapid rate, leading to increase in sea level. Therefore, a system that can accurately record the change in sea level is very necessary to be installed, for example an underwater ad hoc network that can accurately and timely provide information to the government [1].
The nodes in SANET are boat nodes whose main aim is to provide network when a node is in the sea. It can also be used to save and guide the refugees trying to cross through any water medium. While in FANET there may be obstruction in forming networks because of high mountains, no such obstruction can affect SANET and instead there is open space for communication between the nodes.

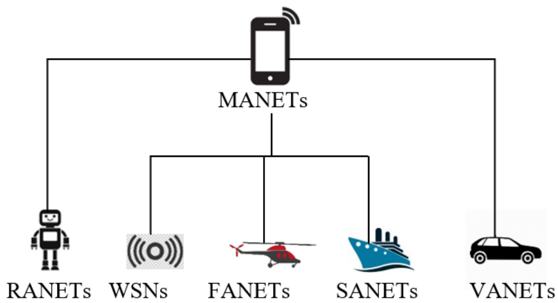

FIGURE 1. Classification of Ad Hoc Networks

SANET APPLICATIONS

The various applications of SANET system are as follows:

1) Catastrophe: SANET is helpful when some accident or disaster happens such as sinking of boats, oil barges or shipwrecks [2]. The nodes of SANET would send the information as soon as the mishappening occurs or if any error occurs during transmission of message, that error can be identified and the message will still be conveyed. Whenever a distressed or missing vessel is located, the authorised organisations deploy helicopters, rescue vessels or any other appropriate vessel to return them to land.

2) Seismic monitoring: SANET can be used to detect and record the earth's motion under sea or any water body from man-made and natural sources. It works on the principle of inertia. The seismometer body rests or floats on the surface of the sea. Inside the body, a heavy mass is suspended between the two magnets. With the movement of the earth, the seismometer moves too and so does the magnets, but the mass remains unchanged in its place. With the oscillation of the mass through the magnetic field, an electric current is produced which is measured by the instrument [9]. We note and record the variations in the oil reservoir over a fixed time duration, there is a whole branch of study dedicated to it, called "4-D seismic". Terrestrial oil fields are only annually or quarterly monitored using this technique since it involves large capital and operational costs [10].

3) Environment monitoring: SANET can be used to monitor and observe the changes in the normal ocean waves, earthquakes, volcanic eruptions and other underwater explosions above or below water, the gravitational pull of the earth and sun generates the wind and tides, which in turn produce these natural disasters. Therefore, it can be used to predict the tsunami or predict weather conditions and also transfer this information to the ships or vessels in any water body. Hence the information about natural disasters like tsunami can be conveyed to the concerned authorities well before time and arrangements can be made to save people and reduce the casualties as much as possible.

Hence the climatic observations made at sea can help us in following ways:

A. In sending warning to other ships and coastal administrators.

B. In understanding the global climate.

C. In predicting the future weather.

D. In sending the data to meteorological and hydrological services (NHMS) centres, which form the part of climatic prediction models from where local and global forecasts are generated.

E. In making observations at sea, at the same time period as that on land, therefore helping in understanding the different weather conditions. There is an old saying "Garbage in garbage out", therefore the forecasts will be as good as the data received.

4) Military: SANET can act as a promising technique for exchanging information between the military headquarters and the ships. Earlier satellites were used by navy ships to communicate with each other or with ground station back on land. But these

communications were usually delayed and had a restriction of limited bandwidth. On the other hand SANET allows us to form a ship area network while at sea, thus helping in high speed transmission of data among ships, enhancing their sharing of multimedia data and better coordination in battlefield operations [11].
SANET can also help in detection, tracking and identification of submarines. It can be designed to work at a very low frequency, ranging from a few hertz to a few kHz. Due to low frequency the detection range increases. Therefore, SANET can correctly detect and discover low-frequency noise sources [1].

5) Underwater robots: A very important application of SANET is autonomous underwater robots who can coordinate sensing of oil leaks or any biological phenomena such as phytoplankton concentrations [10] i.e. the chores that would seem difficult for a man. SANET will require a multi robot network. In the multi robot network the robots form a communication network on the fly i.e. talk to each other and collaborate in a distributed fashion [10]. However, the communication between these robots is expected to be of low rate, but they are still expected to be able to solve any issue efficiently by coordinating and planning with each other.

COMPARISON BETWEEN AD HOC NETWORKS

1) MANET

According to [12] "A mobile ad hoc network is comprised of number of mobile nodes connected together to form a network without any existing infrastructure. MANETs are peer-to-peer, multi-hop wireless networks in which data is transferred to a random destination node, through various middle nodes". MANET node movement is relatively slow and its mobility model is random and can sometimes result in undesirable path plans. Based on the node movement, the topology alters in MANET are also slow when compared to other ad hoc networks [3]. The nodes in ad hoc networks can act as routers as well, hence they have various computational properties to operate the information. MANET nodes are battery powered since the power consumption is low [13].

2) VANET

According to [14] "VANET is a subclass of MANET, where mobile nodes are moving vehicles. VANETs are a fundamental part of the International Transport System (ITS) framework". Sometimes, VANETs are referred as Intelligent Transportation Networks. The nodes in VANET have unlimited energy and high mobility which is foreseeable due to the finite street designs [15]. In VANET, the use of GPS receiver for coordinates can get information accurate to 10-15 metres, which is enough for route navigation. Somehow, this accuracy is not enough for security operations like crash alerts. Hence some researchers use Assisted GPS (AGPS) or Differential GPS (DGPS) with accuracy of about 10 cm [16, 17].

3) FANET

FANET can be explained as a subdivision of VANET, where the nodes are usually UAVs (unmanned aerial vehicles). FANET presents itself as a low cost, versatile answer for extension of web framework around the world. Perhaps the greatest difference of UAVs is the high movability and speed variation they have, which permits them to get to hard to arrive at places. According to [18], “a FANET node can have a speed of 30-460 km/h. Due to the high mobility of UAVs, the topology change is faster and more frequent in FANET”. UAVs have a random mobility model but in some cases they move on a prearranged path and have a regular mobility model. UAVs are generally dispersed in the sky, so their density is lower than the density of nodes in MANET and VANET. When it comes to power consumption FANET communication system is supported by the power source of UAVs, which means there is no power resource problem [19]. The only limitation in FANET when it comes to computational powers is weight however, most of the UAVs have high computational powers. Because of high speed multiple UAV framework, FANET requires exceptionally precise location data. GPS alone is not enough for that therefore a GPS and an Inertial Measurement Unit (IMU) is fitted inside every UAV.

4) SANET

Sea Ad Hoc Network (SANET) is comprised of boat nodes such as ships, boats, underwater vehicles, USVs (unmanned surface vehicle) and vessels connected together to form a large network. The intent of SANET is to increase the extent of the aquatic connectivity [20]. “Node density is defined as the average number of nodes present in a unit area”, since the nodes in SANET are dispersed in oceans or other water bodies, the node density is medium. The nodes in SANET move at a speed that is faster than the nodes in MANET but slower than the nodes in VANET and FANET. The line of movement of underwater vehicles can be random and unpredictable causing the mobility model to be random too. Due to high mobility of USVs in SANET, the topology change of SANET is also faster than the topology change of MANET but slower than the topology change of VANET and FANET. Since the nodes are on the water, the line of sight between various boat nodes is very high. Energy consumption in FANET is also quite high. The frequency band of SANET lies between 5-8 GHz. To track the various nodes in SANET accurately GPS would not be able to give the desired results, therefore we use AGPS, DGPS and Automatic Identification System (AIS) in every node. Since, SANET supports so many applications that can help in several ways, which is only restricted by the delay in data transfer, a stable multi-hop synchronization mechanism for the reliable communication of nodes needs to developed [21].

TABLE 1. Comparison between Ad Hoc Networks

PARAMETERS \ AD HOC NETWORKS	MANET	VANET	FANET	SANET
NODE TYPE	Smartphone, Laptop, PDA, Tablet	Car, Bus, Motorbike, Truck	Drone, Aircraft, Copter, Satellite	Ship, Boat, Underwater vehicle, USV (Unmanned surface vehicle), Vessel
NODE DENSITY	Low	High	Very Low	Medium
NODE MOBILITY	Low	High	Very High	Medium
MOBILITY MODEL	• Random • 2D or 3D	• Regular • 2D	• Random or Regular under special Conditions • 3D	• Random • 2D or 3D
TOPOLOGY CHANGE	Slow	Fast	Fast	Medium
CONNECTIVITY	Medium	High (Rush Hours)	Low	Low
PROPAGATION MODEL	• On the ground • Low LoS	• On the ground • Low LoS	• In the air • High LoS	• On the water • High LoS
POWER CONSUMPTION	Low	High	High (Depends on the UAV)	High
SETUP	Positioning	Road	• Airfields • Hands	Water
LOCALIZATION	GPS	GPS, AGPS, DGPS	GPS, AGPS, DGPS, IMU (Inertial Measurement Unit)	GPS, AGPS, DGPS, AIS (Automatic Identification System)
FREQUENCY BAND	2.4 GHz	5.9 GHz	2.4/5 GHz	5/8 GHz

DEPLOYMENT SCHEMES FOR SANET

According to [25], “There are three schemes for SANET that will be applied in positions of harbour, shore and ocean, respectively”. Since the current land networks can be used at harbour, we will focus on other two positions in this paper i.e. shore and ocean.

1) SANET network at Shore:

If a node lies in the radius where it can directly contact or connect with the Radio Access Station (RAS), it can convey everything directly, but if a node is outside that radius, then it will have to form a network with other nodes in order to communicate. FIG 2 shows the network architecture of SANET at the shore where solid lines represent the UHF band link for terrestrial communications and dotted lines represent the VHF band link for SANET communications.

2) SANET network in Ocean:

There is no root station available in the ocean because of the large distance from land and it is not practically possible to deploy a root station in the ocean. Therefore, peer to peer communication is required since it requires no base station. FIG 3 shows the network architecture of SANET in the ocean. The solid, dotted and white lines represent the UHF, VHF, and HF band link. Since we cannot access link to RAS even with multi hop VHF, the communication needs to be done using the available HF band modem.

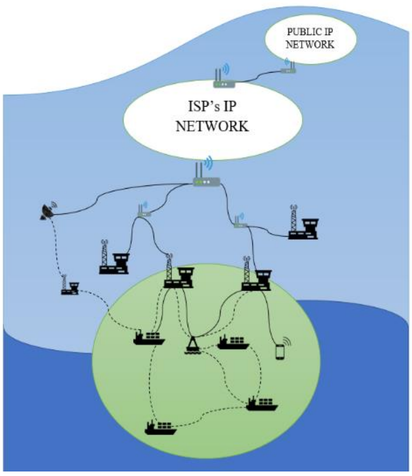

FIGURE 2. Proposed maritime wireless communication architecture for shore.

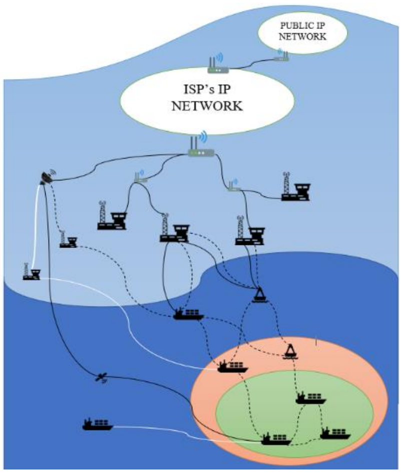

FIGURE 3. Proposed maritime wireless communication architecture for ocean.

ROUTING PROTOCOLS IN SANET

The routing protocols in SANET are designed and classified into various categories based on the way routing data is shared, and the way paths are established [26]. Based on these criteria we have following routing protocols:

1) Proactive Routing Protocols:

Proactive routing protocols use routing tables to store data related to the connections between each pair of nodes. Every node keeps one or more routing tables, thus forming the full topographic anatomy of the network. These routing tables need to be refreshed consistently to provide correct data from source node to destination node [1]. Consequently, it becomes easier to choose the shortest route from root to target node, hence decreasing latency significantly [21].

But to keep up with the latest routing information, topographic data must be exchanged among the USVs regularly**,** causing congestion of network, consumption of more bandwidth and slow reaction to disconnections [27].

Therefore, the main advantages of such algorithms are:

1) Routes are always available on request.
2) Less delivery delays.
3) Easier to choose the shortest route.

And the disadvantages are:

1) Slow reaction to reconstruction.
2) A lot of packets and data needs to be maintained for smooth working.

Examples of these algorithms are OLSR and DSDV.

1.1) Destination Sequenced Distance Vector (DSDV):
DSDV is a table-driven routing scheme, which means it is a proactive routing protocol. It is established as improved version of bellman ford algorithm. The usage of sequence numbers in routing protocols leads to the advancement in bellman ford algorithm as it provides freedom from loops. In DSDV every node must maintain a routing table comprising of the addresses of all the possible destination nodes, count of jumps needed to get to the target, and the address of the next node. The routing table modification process is generated through the exchange of data between nearest nodes.
According to [28] "sequence number is also attached with every route to a target address. Whenever the topology of the network changes, a new sequence number is assigned to the changed paths".
Therefore, sequence number indicates the validity of a path. Higher the sequence number, more reliable is the path, thus avoiding the formation of loops. Every time a path changes, its sequence number is incremented by two. Thus, all the paths with even sequence numbers are reachable.
If a node notices that a path to destination is not working, then the path is assigned a high number of hopes (meaning infinity) and its sequence number is made odd, therefore an odd sequence number means that the path is not reachable. Now to reduce the traffic, "full dump" and "incremental" data is exchanged in this system, "full dump" contains all the information about the changed path and "incremental" contains the information about the changes made [29]. Assigning of new sequence numbers every time the topology changes, takes time, hence DSDV is not suited for networks with high activity.

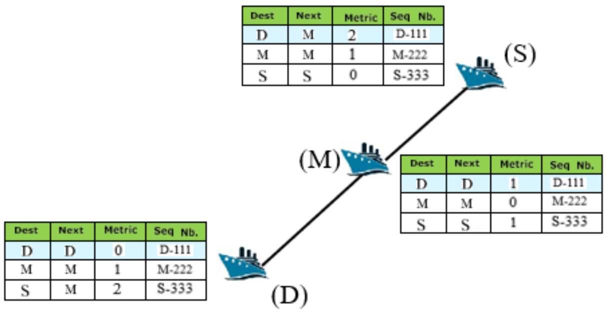

FIGURE 4. Mechanism of DSDV

1.2) Optimized Link State Routing Protocol (OLSR):
OLSR protocol has been discussed in various studies [30, 31, 32, 33, 34, 35, 36] which have implemented it under several model circumstances. It has information of all the present links between USVs. It occupies the constancy of link state algorithm because it is a maximization of link state algorithm.

OLSR minimizes the overhead because it uses only selected nodes, called MPRs which stands for multipoint relay. The knowledge of all the existing links is established by periodic transfer of topology control packets between nodes of network. Using MPRs for transmission of messages also limits the amount of transfers needed to spread a message across all the nodes and the maximum time required for the transmission. As [27] states "This protocol is very helpful for networks where a large number of nodes are interacting with another set of large number of nodes and the source, destination pairs are changing over time". OLSR is best fitted for crowded networks as the optimization done using MPRs only acts as an advantage when there is a lot of traffic. But one drawback of this algorithm is that no exception is made for small networks, so if a small network is using this protocol it will still do the same amount of work, which might not even be required. This restricts the scalability of this protocol and it works efficiently only in dense networks.

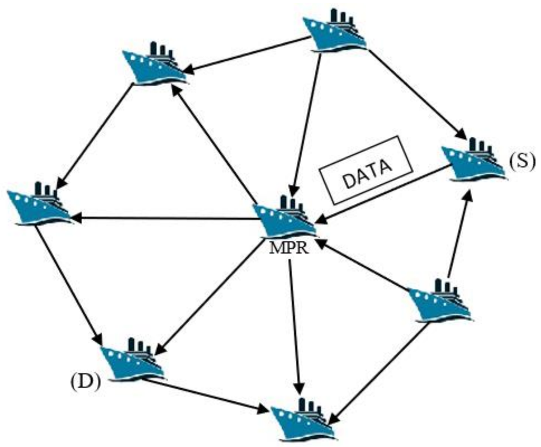

FIGURE 5. Mechanism of OSLR

2) Reactive Routing protocols:

Reactive routing protocols are also named as "On Demand routing protocols" because they do not retain information in table and the route finding process is only started when one node wants to communicate with other node. The path is determined by exploring the maximum routing paths available, due to which this type of protocols undergo a high delay and response time particularly when the system is fragmented. This algorithm finds the route by using two packets: Route Request packets (RREQ) and Route Reply packets (RREP). RREQ is used by source node by flooding it in the network and only the target node or destination node replies to this RREQ using RREP, thus when the RREP reaches the source the communication is initiated. Thus, this algorithm can be used for networks with a huge bandwidth [37] like SANET.

The main advantages of these protocols are:

1) Reduces overhead.
2) Suitable for systems with large data transfer capacity.

And the disadvantages are:

1) High reaction time due to the discovery process in route discovery.
2) High congestion can make the network cluttered.

Examples of these algorithms are DSR and AODV.

2.1) Dynamic Source Routing (DSR):

According to [38] “The dynamic source routing protocol or DSR is a simple and efficient routing protocol designed mainly for wireless interlocking networks and is based on a method known as source routing”. Since DSR is reactive in nature, a discovery process is started only on demand or when the communication is required. While crafting DSR, the intention was to make a routing protocol that has very little running cost but can respond to network changes very quickly.

DSR provides the possibility to find multiple paths to a destination by exchanging RREQ packets. Each intermediate node that passes the packet to next node adds its own address to the list in the packet. A one way response packet or RREP containing addresses of all the intermediate nodes is produced, when the RREQ packet arrives at the destination node. Then the final path is the path that requires the minimum count of hops to reach the destination node.

The DSR protocol is comprised of two main schemes, Route Discovery and Route Maintenance.

The node produces a path error message and is transmitted to the root node when a measurable number of transfers fail, and the message comprises of problem reference. Now the root node needs another path to destination node that it already doesn’t have in its memory. It initiates a route exploration process again to find a better path. And since DSR does not need any regular update messages, it avoids the loss of bandwidth.

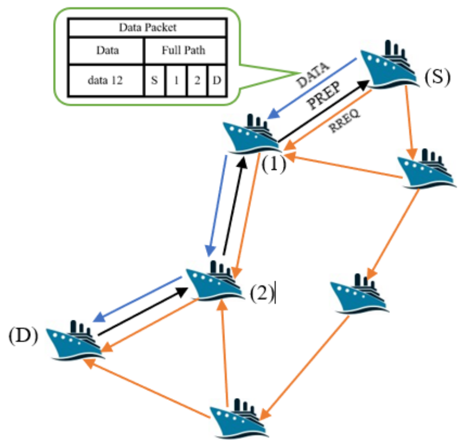

FIGURE 6. Mechanism of DSR

2.2) Ad Hoc On Demand Vector Algorithm (AODV):

As stated in [39] AODV algorithm enables dynamic, self-starting and multi hop routing between the participating mobile nodes. It only finds routes when the need of communication arises. It maintains these nodes as long as the communication continues. Similar to DSR, AODV protocols use the flooding of RREQ across the network to identify the path differentiating characteristic of this protocol is its association of sequence number with every route entry. An intermediate node can reply to RREQ if it has the path to the target node whose respective sequence number is equal to or larger than the one present in the RREQ or if it is the destination node. Or else, it retransmits the route request, Nodes store and audit the Route request's IP address and Broadcast ID.

If they receive a RREQ from a IP address that they have already processed, they do not transfer it. When the root node collects route reply, it initiates sending the information or data to the destination or final node. The root node revises its routing table and starts using the more efficient route if it receives a route reply with a greater sequence number than it already possesses. When a network collapses when the path is still effective, the node previous to the broken link transmits a RERR to the root node. In AODV the routes to destination are maintained only till the communication is active, when the communication stops all the links are deleted.

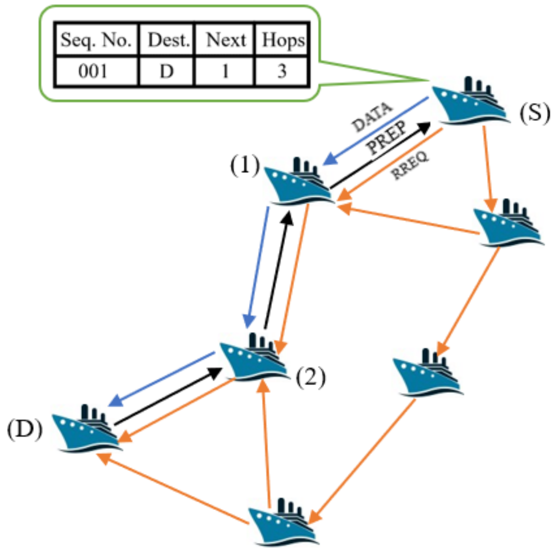

FIGURE 7. Mechanism of AODV

3) Hybrid Protocols:

To knuckle down the disadvantages previously mentioned routing approaches, hybrid protocols were designed which is a merge between PRP and RRP protocols containing the advantages or benefits of both. PRP requires overhead to sustain a network and RRP needs ample amount of time to establish the possible paths. So, to fix these problems, hybrid protocols take up the notion of separate areas or zones where proactive approach is used inside the zones, thus lessening the overhead, and for the intercommunication of zones, reactive strategy is used. This protocol is best fitted for large networks. The paths are initially created using proactive approach and after that demand is served using reactive approach.

The main advantages of these Protocols are:

1) It contains the benefits of both PRP and RRP.
2) It is convenient for crowded networks.
3) Low overhead.
4) Less time delay in finding routes.

The main disadvantages of these protocols:

1) Time to find the route depends on slope of traffic volume.

Examples of Hybrid protocols is ZRP.

3.1) Zone Routing Protocol (ZRP):

According to [40] "Zone Routing Protocol or ZRP is a hybrid routing protocol merging two types of routing protocols, Reactive and Proactive". It utilizes the benefits of both to make the route finding process increasingly proficient and quick..

In ZRP, the entire topology is divided into different zones and RRP or PRP are used inside the zone or between the zone based on their strengths and weaknesses. Each zone is distinguished based on the distance between nodes using a predefined radius r and hence each node contains a set of nodes.

AUVs in the same zone use intra zone routing that uses proactive methodology to communicate. And if a communication between zones is to be made, then a data packet must be transmitted from one zone to another, inter zone routing is used which is based on reactive approach. It reduces the need for hubs to keep the entire network proactive.

ZRP also explains a strategy called BRP (Border cast Resolution protocol) to regulate gridlock between zones.

If communication is to be made between the AUVs and the source unmanned vehicle S, and there is no path to target node D that is present in different zone, BRP is used to flood the Route Request (RREQ) across nodes. ZRP enhances the organisation of nodes.

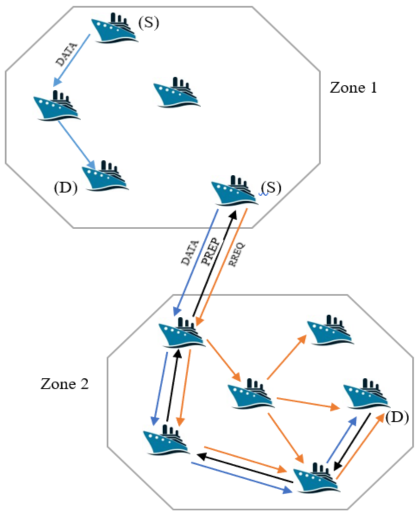

FIGURE 8. Mechanism of ZRP

TABLE 2. Comparison between routing protocols

Feature	OLSR	AODV	DSDV	DSR	ZRP
Protocol Type	Link State	Table driven and Source routing	Distance vector	Source routing	Table driven and Source routing
Route maintained in	Routing Table	Routing Table	Routing Table	Route cache	Routing Table Route cache
Route discovery	Via control message link sensing	On demand	Via control message	On demand	Via control message On demand
Multiple route discovery	Yes	No	No	Yes	Yes
Multicast	Yes	Yes	Yes	No	Yes
Broadcast	Limited by MPR set	Yes	Full	Yes	Partially
Reuse of routing information	Yes	No	Yes	No	Yes
Route reconfiguration	Link state Mechanism/ Routing Message Transmission in advance	Erase route then source notification or local route repair	Sequence number adopted	Erase route the source notification	Sequence Number and erase route the source notification
Limited overhead	Concepts of MPRs	No	Concept of Sequence numbers	Concept of route cache	Concept of Sequence numbers and route cache
Advantages	Minimize the overhead, improve the transmission quality	Adaptable to highly dynamic topologies, reduced control overhead	Avoid extra traffic, reduce the amount of space in the routing table	Multiple routes, reduced bandwidth overhead	Enhances the organization of nodes
Disadvantages	Require more processing power and bandwidth	Scalability problems, large delay caused by the route discovery process	High control overhead, wastage of bandwidth	Scalability problems due to source routing and flooding, large delay	Inadequate for high mobility

CHALLENGES AND ISSUES IN SANET

1) GPS Localization [4]**:**
In any ad hoc network it is crucial for each USV to know its current state with respect to other USVs. But, GPS localization and time synchronization in SANET is not easy, since high frequency waves used by Global Positioning System (GPS) cannot travel well below water and are quickly absorbed by the water surface. It is no longer possible to use the regular GPS free methodology utilized in ad hoc services used on land, of measuring the Time-Difference-of-Arrival (TDoA) [22] between a Radio frequency and an acoustic Signal since normally used radio frequency fails to operate under water. Moreover, the flow of water, temperature difference and pressure influence the speed of acoustic waves.
An alternate way of transmitting signals in the water is use of EM waves, it is outlined to be rapid and productive communication. EM ways are considered to be better than acoustic waves mainly because of their high bandwidth, but certain elements confine the usage of EM waves such as their need to be transmitted differently depending on the water type [1].

2) Security:
In any ad hoc network, safety of data transfer is the biggest challenge. It needs revisiting every time a new concept is announced to update and upgrade the security services. The data that is being transferred and the nodes in use should be secure from any malicious attack that can grow even more if the node is a basic point. As discussed above SANET nodes are restricted in power, calculation and correspondence abilities which makes SANET even more vulnerable to security threats. Moreover, an ad hoc system that is self-organizing like SANET needs more security than just cryptography, security attacks can still be made even if an efficient cryptosystem is guarding the network. The biggest threat is denial of service attack, which can happen if the battery of the nodes start draining due to extra computation and communication, or if the network of a node is interrupted. These attacks can take place irrespective of the presence of cryptographic protections.

3) Peer to peer communication:
According to [5] “A fleet of autonomous underwater vehicles (AUVs) require coordinated synchronization and accident avoidance using peer to peer communications (P2P)”. But the AUVs operating underwater have a very limited operational range especially while transmitting heavy data. The range of operation of AUVs can be extended but at the expense of speed of transmission of data which can prove to be a little risky sometimes, since it won’t be possible to get the data and warning on time. However, there are two other problems underwater that the propagation time is much larger than transportation time and scattering of waves. Scattering is the change in direction of motion of particle because of a collision with another particle [1]. Higher the turbidity, higher is the scattering effect. According to [23] “These three conditions are necessary to be implemented in order for an ad hoc network to be successful underwater: a) Presence of a stable connection link, b) A reliable routing protocol, c) A protocol for sharing of communication link”. Therefore, peer to

peer communication among nodes is a major challenge in SANET, if they won't be able to communicate with each other effectively and collaborate to transfer data, the whole meaning of this network stands useless. The route of transfer of data is solely decided by the nodes.

4) Energy supply efficiency:

As the energy consumption of USV's is too high, so it has become a challenge to provide them the required energy constantly and efficiently in order for them to keep working at a required rate.

Sustainable improvements are underway in renewable energy advancements by overusing resources like solar energy [21]. This power produced cannot satisfy the energy needs for data transfer and the long distance movement of USVs. The first possible substitute is to cooperate with other USVs to reach the required energy limit. The second substitute is ideal positioning of recharge stations.

To address the energy concerns a new investigation is drafted to combine cloud computing prototype with SANETs. But, another challenge that comes with cloud computing is of security, because the data can be transferred between USVs. Various safety mechanisms are required to overcome this challenge. Cloud computing prototypes are being investigated only. They are yet to be applied [5].

So, the nodes must be designed with low power consumption in mind to maximize the network life, their every design aspect should be concentrated towards minimizing the energy requirement. Another solution that can be implemented is using lithium batteries. Lithium batteries because they are a smart substitute to AA batteries which suffer from physical deterioration and leakage currents. But using batteries in the USVs might not be a good idea, because in order to change the batteries in USVs they will have to be retrieved from the bottom of the sea, which can be a time consuming and costly process [10].

5) Routing challenges:

Routing protocols in SANET are dissimilar to other ad hoc networks because the deployment of SANET is different therefore it makes for a challenge to propose a routing protocol and algorithm that can update the routing tables in SANET when the deployment changes. Moreover, the routing protocols that have been designed are for nodes having low mobility (MANET) or very high mobility (FANET), a little or no research is done towards making the routing protocols efficient for nodes having medium mobility. Both the medium mobility and medium density are significant challenges in developing a routing approach to ensure a reliable transfer of information. According to [24], "Currently, there are two routing protocols developed for sublunary sensor networks namely, proactive and reactive". Both of them have some issues and challenges. In proactive approach, a broad signalling is provoked in order to create paths, every time the topology is changed because of constant node movement. Whereas reactive protocols are more appropriate for dynamic conditions and cause a significant delay in sending information bundles to create routes. The extremity of these difficulties is enhanced when the nodes move in 3D space (i.e. underwater). Therefore, there is a grave need to introduce new protocols that can implement new techniques in above mentioned situations.

FUTURE RESEARCH TOPICS:

SANET has become a critical area of examination and research in current years. This technology can provide formidable aid to existing services and can provide new implementations. However, it still has many issues and challenges to overcome to become a successfully established network. Specific technical issues that need to be focused upon are frequent disconnections, restricted transfer speed and inadequate energy capacity. There is a need of advancement in routing protocols that focuses on bandwidth optimization, latency reduction, security problem, fault tolerance, stronger connection to prevent frequent link disconnections when there is high mobility and also integrates all the required sensors in a single unit. Examination of basic SANET environment like density and movability structure of AUVs can also be done. Security of data transfer is one of the biggest and difficult issues not only in SANET but in all the variants of ad hoc networks, extensive research needs to be done on the generation and transmission of security codes.

CONCLUSION:

The main concepts of SANETs have been analysed in this paper. The contrasts among SANETs and other variants of ad hoc networks in premises of versatility, node density, topology transition and power utilization are highlighted. The basic purpose is to serve customers and the potential use of SANETs in seismic monitoring, environment monitoring, underwater robots and military domains is presented. Then the main problems associated with SANET system such as transmission problems, security and routing challenges are shown. In SANETs, routing is thought of as one of the leading components to guarantee correct performance of the network therefore, several routing protocols have been discussed thoroughly. By the evidences, reactive protocols are mostly used in SANET. We have highlighted AODV and DSR under this category because they do not need to store routing information for a long time. A brief study that discusses and validates all the major routing protocols is presented.

Finally, the less explored challenges of SANET are identified and listed under future research challenges. As a final conclusion we can say SANET can generate a large amount of different systems and the various applications of this system are exposed. Furthermore, the crucial factors that need to be considered in SANET are: Energy consumption, Capacity and Dependability of network, which require to be analysed comprehensively to ensure right quality of service.

REFERENCES

[1] M. Garcia, S. Sendra, M. Atenas and J. Lloret, "Underwater Wireless Ad-hoc Networks: A Survey," p. 2, 2011.

[2] Taher and H. Mohammed, "Sea Ad hoc Network (SANET) Challenges and Development," *International Journal of Applied Engineering Research,* p. 1, 2018.

[3] W. Lou, W. Liu, Y. Zhang and Y. Fang, ""SPREAD: Improving network security by multipath routing in mobile ad hoc networks.," *Wireless Networks,* vol. 15, no. 3, 2010.

[4] T. Eissa, S. Razak and M. Ngadi, "Towards providing a new lightweight authentication and encryption scheme for MANET," *Wireless Netwoks,* vol. 17, no. 4, 2011.

[5] S. Mutly and G. Yilmaz, "A distributed cooperative trust based intrusion detection framework for MANETs," *ICNS 2011, The Seventh International Conference on Networking and Services,* 2011.

[6] K. Hartann and C. Steup, "The vulnerability of UAVs to cyber attacks-An approach to the risk assessment".

[7] I. Bekmezci, S. ,. Koray and S. Temel, "Flying Ad-Hoc Networks (FANETs): A survey," *Elsevier,* p. 1, 2013.

[8] J. Kong, J.-h. Cui, D. Wu and G. Mario, "BUILDING UNDERWATER AD-HOC NETWORKS AND SENSOR NETWORKS FOR LARGE SCALE REAL-TIME AQUATIC APPLICATIONS," *MILCOM 2005,* p. 1, 2005.

[9] "Wikipedia," [Online]. Available: https://en.wikipedia.org/wiki/Ocean-bottom_seismometer.

[10] J. Heidemann, Y. Li, A. Syed, J. Wills and W. Ye, "Underwater Sensor Networking: Research Challenges and Potential Applications," 2005.

[11] "Wikipedia," [Online]. Available: https://en.wikipedia.org/wiki/Vehicular_ad-hoc_network.

[12] "JavaTPoint," [Online]. Available: https://www.javatpoint.com/mobile-adhoc-network.

[13] S. Misra and S. Bhardwaj, "Secure and robust localization in a wireless ad," *Transactions on Vehicular Technology,* no. 58, pp. 1480-1489, 2009.

[14] "Research challenges in intelligent transportation network," *IFIP Keynote,* 2008.

[15] W. Li and H. Song, “ART: An attack-resistant trust management scheme for securing vehicular ad hoc networks,” *Trans. Intell. Transp. Syst.,* vol. 17, no. 4, pp. 960-969, 2016.

[16] H. -S. Ahn and C. -H. Won, “DGPS/IMU integration-based geolocation system: airborne experimental test results,” *Aerospace Science and Technology,* no. 13, pp. 316-324, 2009.

[17] A. K. Wong, T. K. Woo, A. T. -L. Lee, X. Xiao, V. W. -H. Luk and K. W. Cheng, “An AGPS-based elderly tracking system,” *International Conference on Ubiquitous and Future Networks,,* 2009.

[18] J. Clapper, J. Young, J. Cartwright and J. Grimes, “Unmanned Systems Roadmap 2007–2032,” *Dept. of Defense,* 2007.

[19] A. Purohit, F. Mokaya and P. Zhang, “Collaborative indoor sensing with the sensorfly aerial sensor network,” *Proceedings of the 11th International Conference on Information Processing in Sensor Networks,* pp. 145-146, 2012.

[20] R. Al-Zaidi, J. C. Woods, M. Al-Khalidi and H. Hu, “Building novel VHF-based wireless sensor networks for the Internet of marine things,” *Sensors J.,* vol. 18, no. 5, pp. 2131-2144, 2018.

[21] O. S. Oubbati, M. Atiquzzaman, P. Lorenz, M. H. Tareque and M. S. Hossain, “Routing in Flying Ad Hoc Networks: Survey, Constraints, and Future Challenge Perspectives,” 2019.

[22] A. Savvides, C. -C. Han and M. B. Srivastava, “Dynamic Fine- Grained Localization in Ad-Hoc Networks of Sensors,” *ACM MOBICOM,* pp. 166-179, 2001.

[23] K. Y. Foo, P. R. Atkins, T. Collins, S. A. Pointer and C. P. Tiltman, “Sea trials of an underwater, ad hoc, acoustic network with stationary assets,” *IET Radar, Sonar and Navigation,* 2007.

[24] A. Abdullah and M. Ayaz, “Underwater Wireless Sensor Networks: Routing Issues and Future Challenges,” 2009.

[25] Y. Kim, J. Kim, Y. Wang, K. Chang, J. Park and Y. Lim, “Application Scenarios of Nautical Ad-hoc Network for Maritime Communications,” *OCEANS 2009,* p. 2, 2009.

[26] S. A. Ade and P. A. Tijare, “Performance Comparison of AODV, DSDV, OLSR and DSR Routing Protocols in Mobile Ad Hoc Networks,” *International Journal of Information Technology and Knowledge Management,* vol. 2, no. 2, pp. 545-548, 2010.

[27] T. Clausen and P. Jacquet, “Optimized link state routing protocol (OLSR),” *RFC,* 2003.

[28] “ Computer Science & Electronics Journals,” [Online]. Available: https://www.csjournals.com/.

[29] N. S. Mohamad, “Performance Evaluation of AODV, DSDV & DSR Routing Protocol in Grid Environment,” *International Journal of Computer Science and Network Security,* vol. 9, no. 7, 2009.

[30] S. Makkar, Y. Singh and R. Singh, “Performance investigation of OLSR and AODV routing protocols for 3 D FANET environment using NS3,” *J. Commun. Eng. Syst.,* vol. 8, no. 2, pp. 1-10, 2018.

[31] A. Leonov, G. Litvinov and D. Korneev, “Simulation and analysis of transmission range effect on AODV and OLSR routing protocols in flying ad hoc networks (FANETs) formed by mini-UAVs with different node density,” *Proc. Syst. Signal Synchronization, Generating Process. Telecommun,* pp. 1-7, 2018.

[32] Y. Jiao, W. Li and I. Joe, “OLSR improvement with link live time for FANETs,,” *Advanced Multimedia and Ubiquitous Engineering,* pp. 521-527, 2017.

[33] A. Nayyar, “Flying adhoc network (FANETs): Simulation based performance comparison of routing protocols: AODV, DSDV, DSR, OLSR, AOMDV and HWMP,” *Proc. Int. Conf. Adv. Big Data, Comput. Data Commun. Syst. (icABCD),* pp. 1-9, 2018.

[34] K. Singh and A. K. Verma, “Experimental analysis of AODV, DSDV and OLSR routing protocol for flying adhoc networks (FANETs),,” *Proc. IEEE Int. Conf. Elect., Comput. Commun. Technol. (ICECCT),* pp. 1-4, 2015.

[35] K. Singh and A. K. Verma, “Applying OLSR routing in FANETs,” *Proc. IEEE Int. Conf. Adv. Commun. Control Comput. Technol. (ICACCCT),* pp. 1212-1215, 2014.

[36] D. S. Vasiliev, D. S. Meitis and A. Abilov, “Simulation-based comparison of AODV, OLSR and HWMP protocols for flying ad hoc networks,” *Proc. Int. Conf. Next Gener. Wired/Wireless Netw. Cham,* pp. 245-252, 2014.

[37] A. M. Sagheer and H. M. Taher, “Identity Based Cryptography for Secure AODV Routing Protocol,” *TELFOR,* pp. 198-201, 2012.

[38] D. Johnson, Y. Hu and D. Maltz, “The dynamic source routing protocol (DSR) for mobile Ad-hoc networks for IPv4,” *RFC 4728,* 2007.

[39] C. Perkins, E. Belding-Royer and S. Das, “Ad-Hoc On-Demand Distance Vector (Aodv) Routing,” *RFC 3561,* 2003.

[40] Z. J. Haas and M. R. Pearlman, "ZRP: A hybrid framework for routing in ad hoc networks," *Ad Hoc Networking,* pp. 221-253, 2001.