Chapter 9
Underwater Wireless Sensor Networks

Usha Jain and Muzzammil Hussain

Abstract In this chapter, we will provide the brief introduction of wireless sensor networks (WSNs) and the detailed introduction of underwater wireless sensor networks (UWSNs). We define the basic issues and different applications related to UWSNs. This chapter provides the description about the difference between the terrestrial WSNs and UWSNs. Later, we discuss the different task of the sensor nodes and deployment architecture of the UWSNs. We elaborate the factors that affect UWSNs design as well as communication architecture of the UWSNs. Here, we explain security issues and provide the detailed description of TCP/IP protocol stack. Later, we define all the protocols for secure communication in UWSNs. One important aspect of this chapter is the study of different simulation tools. We pull together all of the content on simulation of the UWSNs. Finally, we conclude the chapter.

Keywords Underwater wireless sensor networks (UWSNs) · Sensor node · Security attacks · Security protocols · Simulation · Emulation

1 Introduction

A large number of sensor nodes with limited resources and one or more base stations comprise wireless sensor networks (WSNs). Sensor networks are only the reason for revolutionizing the different areas of industry and science. The use of sensor nodes emerges in many more applications like industrial (machine surveillance), underwater, structural monitoring, habitat monitoring of microorganisms, intelligent buildings, facility management, disaster relief operations, medical and health care, agriculture, and many more. Sensor nodes observe the near objects or environments, and report to the base station about the change in observations.

U. Jain (✉) · M. Hussain
Department of Computer Science and Engineering, Central University of Rajasthan, Ajmer, India
e-mail: 2014phdcse03@curaj.ac.in

B. B. Gupta et al. (eds.), *Handbook of Computer Networks and Cyber Security*,
https://doi.org/10.1007/978-3-030-22277-2_9

Wireless sensor networks help in detecting and controlling the critical situations. These networks facilitate many more application areas and try to explore many new ones; but this depends on many characteristic requirements like type of service, quality of service (QoS), faulty tolerance, span time, scalability, flexibility, maintainability, and security [1]. For realizing these characteristic requirements, some mechanisms have been designed such as multihop wireless communication, energy efficient operations, auto configuration, data centric, locality, collaboration, and in-network processing [1].

Wireless sensor networks are different from mobile ad hoc NETworks (MANETs). An ad hoc network is developed for a specific requirement of the application and it is free from the infrastructure. MANET is an ad hoc network with mobility of the sensor nodes and wireless communications in multihop architecture. WSNs are associated with such kind of applications where it is impractical to arrive at the location of the network deployment. The lifetime of the sensor node is the lifetime of the network. In WSNs, once the node runs out of battery or failed due to any reason, it is very difficult in the replacement of the battery or charging of the battery in such a hostile environment. But, in MANETs, the terminal can have more energy with large or powerful battery. WSNs can perform many activities together such as communication, sensing, and computation. This network supports different densities of the network (sparse and dense deployment of the sensor nodes). However, MANETs are unable to handle such kind of the diversity in the deployment of the network. WSNs can easily handle the abrupt changes in the observation, from inactivity to high activity and can help in managing and controlling in the critical situation. While MANETs are used to handle the situation with a specific traffic over the channel in a well-defined manner. WSNs support the scalability of the network from hundreds to thousands or more. On the other hand, it is difficult in case of MANETs. Self-configuration is a common characteristic of the wireless sensor networks and mobile ad hoc networks. But, WSNs strictly follow self-configuration characteristic due to the adequate connectivity of the network and maintaining the trade-offs in energy. WSNs' protocols are data centric where MANETs are not related to data centricity because this network does not follow the redundant deployment. The mobility in WSNs is due to the movement of the sensor nodes according to the specific requirement of the application. The sensor node can be mobile in two situations in WSNs. First, when the sink node is mobile and second, when a node can be used to detect and sense the intrusion inside the network and it has to raise the alarm or send an alert to the base station [2]. However, sensor nodes can dynamically move from one place to another in MANETs.

2 Underwater Wireless Sensor Networks

Underwater wireless sensor networks (UWSNs) are a class of wireless sensor networks in which sensor nodes are placed underwater to study the different areas such as marine life, climate change, natural disasters, and many more others. Sensor nodes are deployed in shallow or deep water to observe the changes and these nodes transmit the report of changes to the sink nodes. There is a need of an efficient communication among underwater devices to make these applications feasible. UWSNs suffer from different challenges like limited bandwidth, more propagation delay, limited battery power, high bit error rate, and others. These networks have more probability of failure because of battery life of sensor nodes and acoustic signal communication [3].

Underwater wireless sensor networks can consist of three types of sensor node: static nodes, semi-static nodes and mobile nodes [4]. Static sensor nodes are anchored to the dock, buoys, or the bottom of the ocean. Semi-static sensor nodes are used for monitoring for a short duration; it may be hours or some days. These nodes are hanged with the buoys and placed by the ship temporarily. Static and semi-static deployment of sensor nodes are mainly energy constrained. Mobile sensor nodes are attached with vehicles like as autonomous underwater vehicles (AUVs), remotely operated vehicles (ROVs), and other underwater vehicles. Mobile nature of sensor nodes helps in covering maximum area in underwater but it raises the problem of network connectivity and localization of nodes. The sensor nodes that are connected with AUVs, suffers less from energy constraint. Sensor nodes in underwater networks are deployed to monitor the changes over a given area [4].

Deployment of sensor networks in underwater environment affects from density of the networks, coverage of the sensor nodes, and number of the sensor nodes. In underwater networks scenario, deployment should be sparse, have good range of connectivity, and deploy a smaller number of nodes [4].

The designing of the UWSNs has some major challenges such as limited bandwidth, impaired channel due to fading and multipath, high propagation delay, high bit error rate, and limited battery power; and sensors are prone of fouling and corrosion [5]. Some disadvantages of underwater communication are as follows:

- When it is needed to buffer the data (before dropping the data) for a long duration, it requires more storage.
- The sink node regularly transmits an enquiry message, if it does not receive any message from other nodes or base station. The regular transmission of enquiry messages raise the problem of power consumption.

2.1 Applications of UWSNs

Deployment of sensor nodes depend upon the applications. UWSNs should be self-organized and self-configurable to adopt the changes in oceanic environment. These characteristics help in performing collaborative tasks of surveillance over a given area. These features explore different applications of underwater wireless sensor networks. The range of applications of UWSNs consists of environment monitoring, exploration monitoring, disaster detection and prevention, undersea navigation, tactical surveillance, mine reconnaissance, and sampling of ocean (Fig. 9.1).

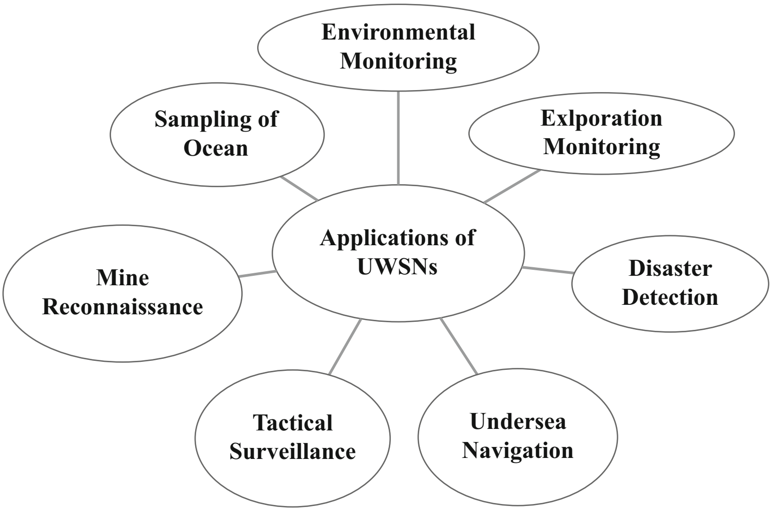

Fig. 9.1 Different applications of underwater wireless sensor networks

- Environment Monitoring: Underwater wireless sensor networks perform monitoring of pollution, currents, winds, biological changes, marine lives of microorganism, and fishes. It helps in understanding of changes of climate and its effect on marine and coastal life. It also provides information of the effect of human activities on ecosystem of underwater area. It helps in prediction of changes in water quality and its effect upon human beings and underwater creatures.
- Exploration Monitoring: Oilfields and reservoirs can be monitored or detected with the help of underwater wireless sensor networks. It can help in the exploration of valuable minerals from the sea or ocean.
- Disaster Detection and Prevention: By calculating the seismic activity, sensor nodes can provide information about tsunami or seaquakes. This information helps in preventing the major losses [6, 7].
- Undersea Navigation: Sensor nodes help in the identification of rocks, hazards of drowning collapse, position of dock, and detection of sandbank in shallow water.
- Tactical Surveillance: Underwater wireless sensor networks can be used in intrusion detection, surveillance, and reconnaissance. It can help in detecting autonomous underwater vehicles (AUV’s), submarines, frigates, and short delivery vehicles [8].
- Mine Reconnaissance: Sensor nodes can help in the detection of change on seabed and mine like objects with the help of autonomous underwater vehicles.
- Sampling of Ocean: With the help of underwater wireless sensor networks, we can find out the idiosyncratic oceanic environment.

Table 9.1 Difference between UWSNs and terrestrial WSNs

Parameters	Underwater wireless sensor networks (UWSNs)	Terrestrial wireless sensor networks (WSNs)
Deployment	Sparsely	Densely
Communication Medium	acoustic or optical	radio
Bandwidth	Low	High
Delay	High	Comparatively less
Power	More	Less
Topology	Highly dynamic	Static or dynamic
Quality of link	High possibility of bit error rate and packet loss	Less
Mobility	Less predictable	Predictable
Memory	More memory (with data caching) due to intermittent nature of UWSNs	Very limited storage
Spatial correlation	Rarely correlated due to more distance between sensor nodes	Highly correlated
Cost	Expensive due to extra protection and complex transceiver	Relatively cheaper

3 Difference Between Terrestrial WSNs and UWSNs

Underwater wireless sensor networks are a set of large number of sensor nodes that are connected to sink(s) to report the changes in deep oceans. Underwater wireless sensor networks have higher probability of link interruption from UWSNs [3, 9]. Comparison table between UWSNs and terrestrial WSNs is as given in Table 9.1. The three primary aspects of link interruption in UWSNs are as follows:

- Network Structure: Due to energy exhaustion or changes in network topology, it is common in UWSNs that sensor node becomes unresponsive or it may be failed. Besides, UWSNs depends upon acoustic medium. Therefore, the variations in communication range affects negatively on the topology generation of the network.
- Underwater Environment: Sound waves of passing ships or creatures in the ocean, and tides or currents in the ocean can create a disturbance in acoustic channel.
- Channel Characteristic Limitations: UWSNs suffers from more transmission delay because of low transmission rate.

4 Underwater Sensor Node

In the previous sections, we have discussed the brief introduction of UWSNs and the basic difference between terrestrial WSNs and UWSNs. In this section, we describe the internal architecture of the sensor node that helps in acoustic communication and define the tasks of underwater sensor node [10]. Underwater sensor node comprises of six parts:

- Controller/CPU: It is responsible for the processing of the data received form sensor nodes and this stored data is used to analyze the situation. It decides what action should be taken, when and where the data should be sent. It is the core unit of the sensor node's architecture.
- Memory: This component is used to store the program and the key values that are used in communication. Different memory types may be used to store the received data.
- Sensor/Actuator and Interface Circuitry: Sensor nodes are used to sense the physical environment and works as an interface that observe the real world. Actuators are responsible for initiating appropriate action after receiving the observed data from the sensor nodes. Interface circuitry is used to make a proper medium for maintaining the data assistance between controller and sensor.
- Acoustic Modem: Physical data are converted in acoustic signal with the help of acoustic modem. After conversion of the signal, it can easily be transmitted over the channel.
- Power Supply: Cabled charging is unavailable in underwater environment. Rechargeable battery or solar cells can be equipped with sensor node. The life of a network depends on the life of the sensor nodes. Therefore, energy saving mechanisms would be used in UWSNs.

5 Communication Architecture for Underwater Wireless Sensor Networks

In this section, we elaborate the communication architecture of the underwater sensor networks. The deployment topology of the network is helpful in determining the energy consumption, and capacity of the network. For the reliable communication in the UWSNs, the topology of the network should be optimized after the deployment. Underwater communication is expensive because the devices that are employed in the communication have high cost. The architecture of the UWSNs can be of three types:

- *Static 2-D UWSNs for Ocean Bottom Monitoring:* In this type of architecture, sensor nodes are deployed on the bottom of the ocean or on seabed. Underwater sink connects with the sensor nodes via acoustic signals. Underwater sink has two transceivers: (a) Horizontal transceiver (used for communication between sink and sensor nodes) and (b) Vertical transceiver (used for communicating with the surface station). The communication between underwater sink and sensor nodes may be commands by the sinks and observed data by the sensor nodes. Surface stations are connected with the surface sinks or onshore sinks through radio frequency signal or satellite transmitter. This architecture helps in underwater environmental monitoring. Energy is the main resource constraint in any kind of WSNs; therefore, the communication would be in such a manner that will reduce the energy consumption and signaling overhead in an excessive amount. Multihop communication in UWSNs can increase the network capacity and reduce the energy consumption with the help of intermediate nodes. However, this multihop communication increases the overhead of routing [11].

- *Static 3-D UWSNs for Ocean Column Monitoring:* This architecture is constituted by sensor nodes whose height from the bottom is controlled by the different techniques such as sensor nodes can be attached with the floating buoys etc. These techniques of deploying the sensor nodes may create some destruction in ship navigation. Sensor nodes can be detected or captured by the enemies and enemies can reprogram the sensor nodes. However, some major challenges with 3-D architecture are the effect of ocean currents on the depth, sensing coverage area, and communication coverage of the senor node [8].
- *3-D UWSNs with AUVs:* Fixed portion of the network is constituted of sensor nodes and mobile portion is composed of autonomous underwater vehicles. This architecture enhances the abilities of the underwater networks to study or control the different situations. The concept of adaptive sampling and self-configuration is most recommended in mobile nature of UWSNs. Due to the scarcity of energy resources, AUVs can use solar energy to endurance of the network. This architecture helps in the study of exploration, environmental monitoring, and tactical surveillance. From the objective of the exploration, oceanographic instruments (like gliders or drifters) are employed. Gliders and drifters are battery powered underwater vehicles that report about the abrupt changes to the onshore station and receives the operational command from the station [11, 12].

6 Secure Communication in UWSNs

Recently, secure communication is an open research issue in UWSNs, because of its unique characteristics. A protocol stack has been defined for the support of UWSNs that helps in understanding their features and singularities. As similar to the terrestrial WSNs, the protocol stack for UWSNs consists of five layers: Physical layer, Data link layer, Network layer, Transport layer, and Application layer [1, 3]. The physical layer handles the selection of frequency, generation of carrier frequencies, detection of signals, modulation, and encryption of data. The data link layer is liable for data multiplexing, frame detection, medium access control, and error detection, and ensures proper connectivity of the network. The network layer is responsible for data-centric approach, and power efficient routing of the data at minimum cost. The transport layer is responsible for controlling the congestion over the channel, reliable communication and proper data flow. The application layer handles the different application software that are developed on the basis of sensing tasks.

Different management planes have been associated to the layer of the protocol stack. These planes are power management, mobility management, task management, quality of service (QoS) management, and security management. The power management plane ensures the minimum power consumption, and manages the functionality of the sensor node to maintain the energy level of the node. The mobility management plane is responsible for detecting and managing the mobility of the sensor nodes and this helps in maintaining the routing data to the sink. The task management plane regularizes the sensing tasks of sensor nodes, and sensor nodes with more residual energy perform the observation and the remaining nodes are focused on data routing and aggregation. QoS management plane is responsible for fault tolerance, optimization of performance, and controlling the errors. Security management deals with access control, authentication, authorization, integrity, confidentiality, and others.

UWSNs suffer from different security attacks due to its large scale and sparse deployment. There is a possibility of attacks on two places: sensor nodes and protocols of networks. Attacks on sensor nodes are less probable because of its sparse deployment and it is very difficult to capture or compromise many nodes in UWSNs. Attacks on protocols are of destructive nature for different layers of network architecture. These types of attacks can compromise whole communication network. Further, we will discuss secure protocols for communication with respect to UWSNs.

In this section, we will discuss the functioning of each layer of the protocol stack briefly and describe the possible security attacks at each layer.

6.1 Physical Layer

In terrestrial WSNs, electromagnetic waves are used for communication, but the use of electromagnetic wave in UWSNs is infeasible. UWSNs suffer from the problem of absorption and dispersion of all electromagnetic frequencies. Hence, the acoustic communication is the most preferable option of communication in UWSNs [13].

The characteristics of UWSNs are only the reason for the development of underwater modems. The underwater modem is designed on the basis of noncoherent frequency shift keying (FSK). The noncoherent schemes have high efficiency in terms of power and low efficiency in terms of bandwidth. This feature of noncoherent modulation scheme proves it inapplicable for multiuser networks [14].

Thus, coherent modulation schemes may be applicable due to the characteristics as long-range communication, and high throughput system. As the powerful digital processing came in existence, phase shift keying (PSK) and quadrature amplitude modulation (QAM) techniques can be applied.

The intermediate solution of noncoherent and fully coherent schemes is differential phase shift keying (DPSK) with proper bandwidth utilization. The DPSK increases the requirement of carrier phase tracking, then it increases the probability of the error in modulation.

The orthogonal frequency division multiplexing (OFDM) is a spread spectrum mechanism that is a suitable solution for UWSNs. In OFDM, signals are transmitted over sub-carriers. OFDM performs better in case of multipath environments and noise spreading over the bandwidth.

Channel estimation helps in efficient communication process in UWSNs. Packet probing is an efficient way for channel estimation; meanwhile, it increases the communication overhead, energy consumption and reduces the capacity of the channel [13, 14].

Secure Communication in Physical Layer The unique characteristics of UWSNs make it vulnerable to security attack. Jamming is a Denial of Service (DoS) attack in physical layer. In jamming attack, an attacker node means jammer node disrupts the communication by sending the unwanted signals on same frequency band. However, UWSNs suffer with limited bandwidth. Hence, UWSNs are vulnerable to jamming attack.

The solutions for jamming attack in UWSNs must be different from the existing solutions in terrestrial WSNs. In 2012, Underwater Jamming Detection Protocol was defined to detect the jamming attack. At the same time, this protocol tries to mitigate this attack [15]. The three phases of the proposed protocol are neighbor discovery, jamming detection, and jammed mapping area. In this protocol, irrelevant packets are injected at high rate to block the channel. The packet delivery ratio, total amount of energy consumption, and packet sending ratio are used to detect the jamming attack in the detection phase. However, in case of channel interruption, the above-discussed metrices cannot be verified. Secondly, this protocol uses exact location of the sensor nodes, which is impractical in terms of UWSNs. Hence, this Underwater Jamming Detection Protocol is not efficiently applicable in UWSNs.

The authors classified the attacker nodes in two categories [16]: the first type of attacker node is dummy signal jammer, which is unknown about the network structure; and the second type of attacker node is deceptive jammer, which pretends as the legitimated nodes and knows about the network protocols. This protocol can harm the network easily and tries to degrade the performance of the network.

The friendly jamming can also be used to detect the unwanted eavesdropping over the channel by the means of Jamming through Analog Network Coding (J-ANC). Artificial noise is mixed with the legitimate link. So, the eavesdropper is unable to decode the received packet easily.

On the basis of the nature of the jammer node, jamming attack can be categorized as three types: (1) Continuous Jamming: Attacker node transmits unwanted packet regularly and tries to exhaust full energy. (2) Pulsed Jamming: Jammer node works alternatively with the legitimate node in both of the mode (sleeping and working mode). Jammer node conserves its energy and interrupts the communication randomly. (3) Reactive Jamming: Jammer node and legitimate node work in same mode at the same time. When the legitimate node sends the packet, at the same time attacker node starts to interrupt the transmission by sending useless packets.

6.2 Data Link Layer

UWSNs have some distinctive features like limited bandwidth and high latency. These features pose more challenges in medium access control in UWSNs. Frequency division multiple access (FDMA) is inapplicable for underwater communication due to channel fading and limited bandwidth. Time division multiple access (TDMA) works efficiently with long-time guard and this long-time guard helps in managing propagation delay and its variance in acoustic channel. Carrier sense multiple access (CSMA) tries to avoid collision in transmission at both of the side sender and receiver. At the receiver side, an additional guard time is added to manage propagation delay within the network. Hence, we can argue that CSMA is not suitable for UWSNs [17].

The contention window-based techniques are also not applicable in UWSNs. The reasons behind inapplicability of these techniques are the delay generated by RTS/CTS control packets, carrier sensed idle due to large propagation delay in acoustic channel and the unpredictability of time of start and finish.

The objective of designing access schemes for UWSNs is avoiding the collision and maximizing the efficiency of the network in acoustic channel. Some existing mechanisms use the sleep and awake time to avoid energy consumption. But, deployment of underwater sensor node is sparse, and then these mechanisms are not applicable in acoustic communication.

Code division multiple access (CDMA) is an applicable technique in UWSNs, because it reduces packet retransmission rate and resolves the problem of selective fading of the frequency generated by the multipath nature of acoustic communication. Rake filters are used to avoid the effect of multipath at receiver side.

Direct sequence spread spectrum CDMA (DSSS CDMA) is an efficient mechanism that can be easily adoptable in case of underwater medium access control. It supports high transmission rate and deals with multiple quality of service requirements. DSSS CDMA works efficiently for shallow water communication due to the Doppler and multipath. In this technique, it is difficult to maintain synchronization among the stations with high delay spread [18].

A multicluster protocol is designed for efficient communication over acoustic signals. Autonomous underwater vehicles join the cluster, and each cluster uses TDMA with long-time guards to preclude the propagation delay. Separate spreading codes of each cluster avoid the interference [19].

Because multipath fading and path loss affects the underwater acoustic communication, it is necessary to manage the bit error rate with error control functionalities. Automatic request repeat (ARQ) technique suffers from high delay, more energy consumption, and overheads of packet retransmission. It is efficient to employ forward error correction (FEC) technique in UWSNs. This technique introduces the redundant bits to avoid bit errors in transmission. Both sender and receiver may suffer from energy drain by finding the redundant bits in the messages. Due to the limited availability of the bandwidth, it is possible to choose redundant bits dynamically on the basis of the available bandwidth measurements in underwater acoustic channel.

Secure Medium Access in Data Link Layer Sensor node can access wireless medium in an efficient manner with the help of data link layer protocols that enable proper time synchronization between sensor nodes. This medium access control layer (MAC) layer manages the sleep and wakeup time of the sensor nodes. WATER is water-quality monitoring sensor network with time synchronization which finds out the detached timestamp data. The timestamp of two neighbor nodes are correlated and on the basis of this correlation, anyone can find out the outlier timestamp data. But, this WATER is not appropriate for dynamic UWSNs because there is a deficiency of the outlier data of neighbor node due to its sparse deployment and high packet drop rate. Another scheme is secure vertical and horizontal synchronization (SVHS) which provides both vertical and horizontal time synchronization.

CLUSS is a cluster-based secure synchronization scheme for UWSNs [20]. The three phases of CLUSS protocol are authentication, intercluster synchronization, and intracluster synchronization. In this protocol, the time accuracy is maintained by proper propagation delay of uplink and downlink. This protocol is energy efficient, time synchronized protocol with very few synchronization errors. With the limited resources, time synchronization should be developed with minimum overhead of computation and communication.

6.3 Network Layer

A path from source node to the destination node is provided by the network layer. Network layer handles the issue of long propagation delay. The routing protocols are divided into three types: proactive routing protocols, reactive routing protocols, and geographical routing protocols.

Proactive Routing Protocols The information of routing is maintained in routing table, each and every time, when the topology is changed, automatically routing table is modified and the information of the modification is broadcasted to all other registered nodes of the network. However, it is not necessary in acoustic communication. Hence, proactive protocols are not applicable in UWSNs [21].

Reactive Routing Protocols In this type of the protocols, sensor node starts to find the route to a destination when it is required. Once, a path is discovered, it is kept secure until it is not required. Like proactive routing protocols, reactive protocols also suffered from overhead of signaling. Due to the high latency, path establishment procedure is not easy. Hence, it is not suitable for UWSNs [22].

Geographical Routing Protocols The location of the sensor node must be known in these types of routing protocols. For the localization of the sensor node, it is necessary to be time synchronized communication among the sensor nodes. For this reason, these protocols are unsuitable in UWSNs.

In 2001, a routing protocol is discussed, in which there is a central authority that works as a manager. The manager maintains the network topology, flow of communication, and manages the resources of the network. This protocol avoids the congestion and maintains the quality of services [23].

A multihop routing protocol based on acoustic propagation model is proposed that conserves the energy in UWSNs [24]. The routes are discovered with the help of neighboring information collected by all the nodes.

The routing protocol for UWSNs may be designed for minimizing the communication and signaling overhead; and it can provide optimal performance with minimum path delay, and preserve energy resources.

Secure Routing in Network Layer The designing of the routing protocols is based on the node's nature. Underwater sensor nodes are mobile. Due to their mobility, the topology of the network changes frequently. Therefore, it is not possible to adopt same routing protocol of terrestrial WSNs in underwater communication. The possible security attacks in network layer are flooding, sinkhole, blackhole, and Sybil wormhole attacks. A distributed visualization of wormhole attack mechanism (Dis-VoW) can detect the wormhole attack using distortion in length of the edges and angles with the neighbor nodes [25]. But, Dis-VoW is not suitable for highly dense UWSNs.

A mechanism, wormhole-resilient secure neighbor discovery (WSND) is proposed that is based on the direction of arrival (DoA) in UWSNs [26]. It is quite easier to implement because there is no need of accurate time of synchronization and it is based on the approximation of the acoustic signals.

The authors present a protocol suite for routing with cryptographic primitives (SRCP) for mobile and fixed sensor nodes in UWSNs. This protocol provides the confidentiality and integrity of UWSNs communication.

6.4 Transport Layer

The responsibility of transport layer includes congestion control and flow control. The designed protocol for transport layer cannot be applicable as it is in UWSNs. In this section, we discuss the challenges for the development of the transport layer protocol.

In terrestrial WSNs, when multiple nodes report about an abrupt change, then it is considered as an event. If a single node reports about the change, it is not considered as an event. This type of event detection may lead to resource wastage, so it is not recommendable in UWSNs. The transport layer protocols are not only required for reliable data transmission, but also for congestion control and flow control in UWSNs. When the network devices try to avoid the overloaded data transmission, it is called flow control, but, when the network prevents the congestion by the abundant amount of data, then it is called congestion control.

The existing TCP are inapplicable in UWSNs, since the flow control in transport layer is based on the accurate estimation of the round-trip time. The rate-based transport protocols are unsuitable for acoustic communication environment, since these mechanisms depend on the feedback control messages. The event-to-sink reliable transport (ESRT) protocol is defined to attain efficient detection of the event with minimum consumption of the power [27]. The sensor nodes are sparsely deployed in underwater environment. Hence, the readings of the underwater nodes are significantly different from each other. The protocol designed for transport layer should be adoptable as the new requirements introduced by the applications.

Reliable Data Transmission in Transport Layer In transport layer, user datagram protocol (UDP) and transmission control protocol (TCP) are two protocols for end-to-end reliable communication and flow control [28]. UDP is unsuitable for UWSNs because it ensures the data transmission in connection-oriented manner. Hence, TCP is applicable in case of UWSNs. Secure data transmission can be assured in two methods: Encryption of data and authentication. In end-to-end authentication protocol for UWSNs, digital signature is used to authenticate, then a secret symmetric key is used to encrypt the whole data that is transmitted over the channel [29].

The authors present a key generation system that is efficient for UWSNs [30]. The key generator system generates a key after analyzing the characteristic of the acoustic channel. Hence, the system is only vulnerable to an attacker, if he/she knows the location of the deep fades.

6.5 Application Layer

The application layer protocols are unexplored research area for UWSNs. The objectives of the application layer are providing the information of lower layers transparently to the management applications, give a language to enquire the UWSNs, and allocate tasks and report about the incidents [31].

Secure Application Layer The secure practical application is the main problem of the application layer. Secure localization is the primary problem in many applications like tactical surveillance, environment monitoring, and others in UWSNs.

The trust-based secure localization algorithm (SLTM) is a beta distribution-based trust model which is used to find legitimate beacon node [32]. To improve the trust, a trust filter mechanism is employed to decrease the instability of the underwater communication medium. However, it is not suitable for UWSNs due to its consideration of static nodes in underwater environment. It is impossible to direct the use of terrestrial WSNs trust model in UWSNs. For UWSNs, an efficient trust model must be developed to resist the different security attacks.

7 Simulation Tools for UWSNs

For UWSNs, the deployment of the testbed is really very expensive, since it involves the complete network structure and communication links to validate a designed mechanism. In this section, we will provide detailed information of available tools of simulation and emulation in UWSNs. Simulator is an analysis tool that is used to set a testbed for validating the designed mechanism. According to the specific applications of UWSNs, simulation and emulation play an important role to understand the functioning of the designed mechanism. Simulators are used for testing and validating of the software or testing in real-time scenario and emulators are also used for verifying and validating the designed protocol without the actual deployment of the network [33–35] (Fig. 9.2).

- SUNSET is a simulation, emulation and real-time testing tool that is used for analyzing UWSNs. It is more flexible and efficient because it provides the facility of real-time scheduler. It deals with five acoustic modems and different sensor nodes. Interference model, debug module, packet conversion modules, and utility modules are incorporated with this SUNSET. The information of delay in packet transmission is provided with the help of timing module. This simulation tool helps in eliminating the distance between actual result and simulation.
- DESERT stands for DEsign, Simulate, Emulate, and Realize Testbeds that is developed with NS-Miracle framework. This tool is used to design cross-layer protocol by supporting application layer, transport layer through the lower layer of the protocol stack. It has mobility supporting module. uwcbr and uwvbr are two modules of application layer to handle flow of traffic. uwudp and uwtcp are two modules of transport layer to provide error and flow control and liable for multiplexing and demultiplexing. Three routing protocols are defined in network layer. Six MAC protocols are provided in data link layer. However, it does not provide better results in experiments.
- SUNRISE is designed from NS-Miracle framework to sense, monitor, and actuate for UWSNs. It enables scalability and analysis of the data. It helps in

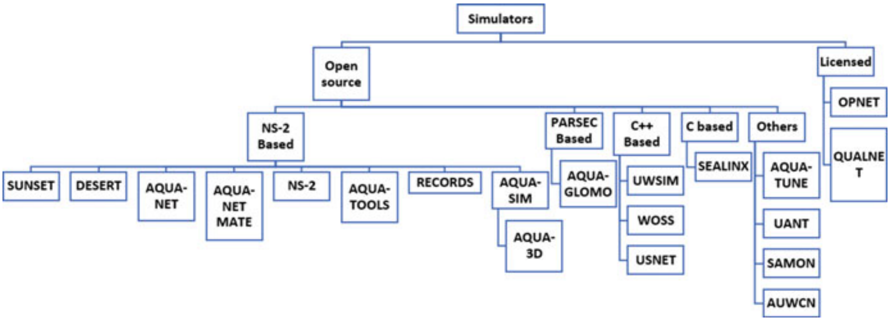

Fig. 9.2 Different simulators for underwater wireless sensor networks

maintaining security and privacy in underwater acoustic communication. However, robot for the underwater application suffers from the battery constrained.

- RECORDS is a framework of remote control in UWSNs. Transmission of remote command becomes possible in multihop communication in the network. It is only designed for static UWSNs [36].
- AQUA-NET is a simulation tool that is designed for protocol stack architecture. It works for embedded systems. It enables optimization of cross-layered architecture.
- AQUA-3D is a robust animator that can analyze the trace files efficiently in UWSNs. It provides prefect visualization of nodes, events, and different objects. There is less probability of compatibility with many simulators for UWSNs.
- SEALINX supports hardware with simultaneous running of modems. It flexibly provides cross-layer communication. It does not support customized the network layer protocol.
- AQUA-SIM is a simulator based on NS-2 that is an open source. Aqua-Sim handles the collision between the packets, propagation model. It contains flexibility and fidelity for UWSNs.
- AQUA-NET MATE is a simulator with virtual channel modem that supports acoustic communication of underwater networks. It supports real-time features and protocol stack layers.
- NS-2 is an open source simulation tool that supports discrete events and it helps in simulation of different protocol. It enables the designing, testing, and validity of the new protocols. It has supported with network animator (NAM) to visualize the connectivity of the medium and nodes' mobility. Sometimes, results obtained by the NS-2 are not enough appropriate as the results of other simulators such as OPNET, OMNET++ and many more.
- UWSIM is a simulator for underwater sensor networks that supports simulation of AUVs. It manages the major challenges like limited bandwidth, frequency, energy resources, and storage capacity of UWSNs properly.
- AQUA-GLOMOSIM simulates the protocols of network layer and physical layer in acoustic communication. Aqua-Glomosim is the upgraded version of Aqua-Glomo. It supports the mobility of the sensor nodes.
- AQUA-TOOLS is a toolkit for channel and physical layer operations in underwater communication. It handles physical layer, data link layer, network layer protocols, and energy constraints.
- WOSS stands for World Ocean Simulation System. It is a simulator that uses Bellhop ray tracing for propagation effects in acoustic communication. It contains full database of the environmental parameters of the world. It simulates the sparsely deployed network that is a complex process.
- USNet is an underwater sensor simulation tool that enables 3-d deployment of the acoustic communication network. This simulation tool deals with threads that can manage many tasks in parallel manner. It simulates the hierarchical architecture of the sensor networks.
- QUAL-NET is a very efficient simulation tool that facilitates simulation by testing, planning, and validating the communication pattern in any type of the

network. It consists of five components that are QualNet Architect (tool for visualization), QualNet Analyzer (Statistical tool for performance analysis of the network), QualNet Packet tracer (analyzer for packet tracing), QualNet File editor, QualNet Command-line Interface. It supports parallel processing and localization of the sensor nodes. It has inbuilt random waypoint mobility model. It is hard to simulate UWSNs in QualNet due to the modeling of characteristics and channel properties of the acoustic communication.

- AQUA-TUNE is a simulator for UWSNs that supports all of the protocol stack. It can set a testbed from 70 h to many days and there is no need for the battery recharging.
- UANT simulates the change in the acoustic channel because it is an underwater acoustic networking simulator. It only deals with two layer that are data link layer and physical layer. It works efficiently in underwater acoustic environment. It was designed with the help of TinyOS and TOSSIM.
- OPNET stands for optimized network engineering tool which can be employed in industrial application for simulation purpose. It supports wireless communication with scalability and customized wireless communication with graphical user interface (GUI) for both 32-bit and 64-bit system. It provides the ability of capturing and visualizing the data flow.
- SAMON simulates the unmanned vehicles by intelligent control. It is a mobile network simulator testbed for sampling in the ocean. It works very efficiently so that the result of simulation and the real-time testing is approximately same. It is very expensive so that it cannot be used in educational purpose.
- AUWCN is an acoustic underwater channel and network simulation tool that works on the physical layer to validate the designed scheme for underwater acoustic channel. It employs Bellhop ray tracing to simulate the physical medium in acoustic communication. It supports the mobility of the sensor node and implements different effects such as Doppler effect, attenuation, and shadow zones.

8 Open Research Issues

As discussed in Sect. 6, UWSNs are vulnerable to different security attacks like jamming, wormhole, Sybil, and many more. To ensure the security of the network, many mechanisms have been proposed for UWSNs. The designed security mechanism does not consider the mobility of the underwater sensor nodes. The protocols are designed on the basis of six aspects: methodology, attacks, node's mobility, energy, outcomes, and challenges. The unique characteristics of UWSNs are responsible for the energy drain, high communication, and computational overheads. For designing an efficient and secure communication protocol, the below mentioned requirements should be considered:

- Security: Security is the major concern in communication. The transmitted data should not be modified by the attacker. It ensures that the transmitted data should be received by only authorized user. As UWSNs are the data centric network, the designed protocol ensures the confidentiality and integrity of the data. Communication should be taken place between two legitimate entities of the network.
- Robustness: The network ensures the proper connectivity and workability in case of any kind of attacks. At the same time, it should efficiently detect the attacker node or try to eliminate it from the network.
- Energy Efficiency: The life of the sensor node is the life of the network. The life of the node depends on the battery of the node. The energy efficient communication protocol maintains the life of the network with the proper communication among mobile nodes.
- Lightweight Protocol: The UWSNs suffers from limited resources in terms of energy, memory, storage, and communication bandwidth. The designed protocol should not be dependent on hardware and software.

9 Conclusion

In this chapter, we have given a brief introduction of wireless sensor networks and detailed introduction of underwater wireless sensor networks. We discussed the difference between the terrestrial WSNs and UWSNs and major challenges in the designing of the UWSNs. We described the deployment architectures of the UWSNs. The protocol stack and secure communication protocols in each layer have been discussed in detail for UWSNs. The simulation and emulation tools have been described properly for the UWSNs. The main objective of this chapter is to encourage the researchers for the development of new efficient and secure communication techniques for communication in underwater environment. This chapter will help in understanding the concept of UWSNs.

References

1. Akyildiz, I. F., Su, W., Sankarasubramaniam, Y., & Cayirci, E. (2002). Wireless sensor networks: A survey. *Computer Networks, 38*(4), 393–422.
2. Yick, J., Mukherjee, B., & Ghosal, D. (2008). Wireless sensor network survey. *Computer Networks, 52*(12), 2292–2330.
3. Akyildiz, I. F., Pompili, D., & Melodia, T. (2005). Underwater acoustic sensor networks: Research challenges. *Ad Hoc Networks, 3*(3), 257–279.
4. Heidemann, J., Stojanovic, M., & Zorzi, M. (2012). Underwater sensor networks: Applications, advances and challenges. *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences, 370*(1958), 158–175.

5. Proakis, J. G., Sozer, E. M., Rice, J. A., & Stojanovic, M. (2001). Shallow water acoustic networks. *IEEE Communications Magazine, 39*(11), 114–119.
6. Soreide, N. N., Woody, C. E., & Holt, S. M. (2001). Overview of ocean based buoys and drifters: Present applications and future needs. In *OCEANS, 2001. MTS/IEEE Conference and Exhibition* (Vol. 4, pp. 2470–2472). Piscataway: IEEE.
7. Cayirci, E., Tezcan, H., Dogan, Y., & Coskun, V. (2006). Wireless sensor networks for underwater surveillance systems. *Ad Hoc Networks, 4*(4), 431–446.
8. Codiga, D. L., Rice, J. A., & Baxley, P. A. (2004). Networked acoustic modems for real-time data delivery from distributed subsurface instruments in the coastal ocean: Initial system development and performance. *Journal of Atmospheric and Oceanic Technology, 21*(2), 331–346.
9. Howe, B. M., & McGinnis, T. (2004, April). Sensor networks for cabled ocean observatories. In *UT'04. 2004 International Symposium on Underwater Technology* (pp. 113–120). Piscataway: IEEE.
10. Sozer, E. M., Stojanovic, M., & Proakis, J. G. (2000). Underwater acoustic networks. *IEEE Journal of Oceanic Engineering, 25*(1), 72–83.
11. Hinchey, M. (2004). Development of a small autonomous underwater drifter. In *Proceedings of IEEE NECECÕ04*.
12. Stojanovic, M., Catipovic, J. A., & Proakis, J. G. (1994). Phase-coherent digital communications for underwater acoustic channels. *IEEE Journal of Oceanic Engineering, 19*(1), 100–111.
13. Karn, P. (1990, September). MACA-a new channel access method for packet radio. In *ARRL/CRRL Amateur Radio 9th Computer Networking Conference* (Vol. 140, pp. 134–140).
14. Misra, S., Dash, S., Khatua, M., Vasilakos, A. V., & Obaidat, M. S. (2012). Jamming in underwater sensor networks: Detection and mitigation. *IET Communications, 6*(14), 2178–2188.
15. Zuba, M., Shi, Z., Peng, Z., & Cui, J. H. (2011, December). Launching denial-of-service jamming attacks in underwater sensor networks. In *Proceedings of the Sixth ACM International Workshop on Underwater Networks* (p. 12). New York: ACM.
16. Freitag, L., Stojanovic, M., Grund, M., & Singh, S. (2002, March). Acoustic communications for regional undersea observatories. In *Proceedings of oceanology international* (pp. 5–8).
17. Freitag, L., Stojanovic, M., Singh, S., & Johnson, M. (2001). Analysis of channel effects on direct-sequence and frequency-hopped spread-spectrum acoustic communication. *IEEE Journal of Oceanic Engineering, 26*(4), 586–593.
18. Kalofonos, D. N., Stojanovic, M., & Proakis, J. G. (2003). Performance of adaptive MC-CDMA detectors in rapidly fading Rayleigh channels. *IEEE Transactions on Wireless Communications, 2*(2), 229–239.
19. Salva-Garau, F., & Stojanovic, M. (2003, September). Multi-cluster protocol for ad hoc mobile underwater acoustic networks. In *OCEANS 2003. Proceedings* (Vol. 1, pp. 91–98). Piscataway: IEEE.
20. Xu, M., Liu, G., Zhu, D., & Wu, H. (2014). A cluster-based secure synchronization protocol for underwater wireless sensor networks. *International Journal of Distributed Sensor Networks, 10*(4), 398610.
21. Jacquet, P., Muhlethaler, P., Clausen, T., Laouiti, A., Qayyum, A., & Viennot, L. (2001). Optimized link state routing protocol for ad hoc networks. In *Multi Topic Conference, 2001. IEEE INMIC 2001. Proceedings IEEE International Technology for the 21st Century* (pp. 62–68). Piscataway: IEEE.
22. Johnson, D. B., Maltz, D. A., & Broch, J. (2001). DSR: The dynamic source routing protocol for multi-hop wireless ad hoc networks. *Ad Hoc Networking, 5*, 139–172.
23. Bose, P., Morin, P., Stojmenović, I., & Urrutia, J. (2001). Routing with guaranteed delivery in ad hoc wireless networks. *Wireless Networks, 7*(6), 609–616.
24. Xie, G. G., & Gibson, J. H. (2001). A network layer protocol for UANs to address propagation delay induced performance limitations. In *OCEANS, 2001. MTS/IEEE Conference and Exhibition* (Vol. 4, pp. 2087–2094). Piscataway: IEEE.

25. Wang, W., Kong, J., Bhargava, B., & Gerla, M. (2008). Visualisation of wormholes in underwater sensor networks: A distributed approach. *International Journal of Security and Networks, 3*(1), 10–23.
26. WANG, R., & ZHANG, Y. (2010). Wormhole-resilient secure neighbor discovery in underwater acoustic networks. *IEEE Transaction on Aerospace and Electronic Systems, 33*(3), 1500–1506.
27. Akan, Ö. B., & Akyildiz, I. F. (2005). Event-to-sink reliable transport in wireless sensor networks. *IEEE/ACM Transactions on Networking (TON), 13*(5), 1003–1016.
28. Dini, G., & Lo Duca, A. (2012). A secure communication suite for underwater acoustic sensor networks. *Sensors, 12*(11), 15133–15158.
29. Souza, E., Wong, H. C., Cunha, ´i., Loureiro, A. A., Vieira, L. F. M., & Oliveira, L. B. (2013, July). End-to-end authentication in under-water sensor networks. In *Computers and Communications (ISCC), 2013 IEEE Symposium on* (pp. 000299–000304). Piscataway: IEEE.
30. Liu, Y., Jing, J., & Yang, J. (2008, October). Secure underwater acoustic communication based on a robust key generation scheme. In *2008 9th International Conference on Signal Processing. ICSP 2008* (pp. 1838–1841). Piscataway: IEEE.
31. Zhang, Y., Jin, Z. G., Luo, Y. M., & Du, X. (2013). Node secure localization algorithm in underwater sensor network based on trust mechanism. *Journal of Computer Applications, 33*(5), 1208–1211.
32. Han, G., Jiang, J., Shu, L., Niu, J., & Chao, H. C. (2014). Management and applications of trust in Wireless Sensor Networks: A survey. *Journal of Computer and System Sciences, 80*(3), 602–617.
33. Egea-Lopez, E., Vales-Alonso, J., Martinez-Sala, A. S., Pavon-Marino, P., & García-Haro, J. (2005, July). Simulation tools for wireless sensor networks. In *Summer simulation multiconference, SPECTS* (pp. 2–9).
34. Korkalainen, M., Sallinen, M., Kärkkäinen, N., & Tukeva, P. (2009, April). Survey of wireless sensor networks simulation tools for demanding applications. In *Fifth International Conference on Networking and Services, 2009. ICNS'09* (pp. 102–106). Piscataway: IEEE.
35. Neves, P. A. C. S., Fonsec, J., & Rodrigue, J. J. P. C. (2007, March). Simulation tools for wireless sensor networks in medicine: A comparative study. In *International Joint Conference on Biomedical Engineering Systems and Technologies, Funchal, Madeira-Portugal* (Vol. 2016).
36. Toso, G., Calabrese, I., Casari, P., & Zorzi, M. (2014, June). RECORDS: A remote control framework for underwater networks. In *2014 13th Annual Mediterranean Ad Hoc Networking Workshop (MED-HOC-NET)* (pp. 111–118). Piscataway: IEEE.