A Comprehensive Study of Security and Research Challenges in Underwater Communication Networks

Merin Mathew
1st yr, M.Tech Communication Engineering,
Department of Electronics & Communication,
Sree Buddha College of Engineering for Women,
Elavumthitta, Pathanamthitta
merinmathew1991@gmail.com

Sudhi Sudharman
Assistant Professor
Department of Electronics & Communication,
Sree Buddha College of Engineering for Women,
Elavumthitta, Pathanamthitta
er.sudhi@gmail.com

***Abstract*-For developments in the field of Underwater Wireless Communication Networks (UWCN), a profound understanding of all the security challenges faced by the underwater systems is required. The UWCN differ from their ground based counterpart in great extents like low bandwidth availability, multipath propagation, high bit error rates, fading etc. Hence new reliable and efficient security techniques have to be developed for underwater communication systems while keeping in mind all the above mentioned challenges. The major attacks on UWCN include wormhole attack, HELLO flood attack, acknowledgement spoofing, selective forwarding, sybil attack and Denial of Service (DoS) attacks like jamming and sinkhole attack. The security measures employed in ground based systems cannot be employed directly in underwater systems due to the differences in the properties of underwater channels from ground based wireless channels, hence they have to be adapted to suit the underwater acoustic environment. The major challenges on researches in underwater networks are secure time synchronization, secure routing and secure localization. It is necessary to design algorithms that can pinpoint the location and time synchronize the network components but are resistant to the security threats present in the network. Overcoming these challenges are essential to secure the underwater communication systems against all possible threats.**

I. INTRODUCTION

Developments of technology over the years have led to dramatic changes in communication in underwater systems. Like the ground based communication systems, underwater systems have also gone wireless. Underwater Wireless Communication Networks (UWCN) consists of a variable number of sensors, anchors, underwater vehicles that are networked and they communicate via acoustics. Major applications of UWCN include data collection, pollution monitoring, offshore exploration, disaster prevention etc. Acoustic transmission is the major difference between the ground based system and the underwater system. The acoustic transmission has a number of inherent disadvantages when compared to the electromagnetic wave transmission in ground based system.

Underwater acoustic communication is characterized by low bandwidth typically in the range of a few KHz to several tens of KHz and supports only low data rates. Propagation delay is longer in underwater systems, the transmission speed of acoustic signals in underwater is around 1500m/s which is a difference of five orders of magnitude lower than the speed of electromagnetic wave in free space. The underwater channel characteristics vary with time and distance due to multipath propagation, fading and scattering, hence bit error rate is also high (typically in the order of 10^{-2}). The above mentioned characteristics imply that underwater communication is more prone to security attacks when compared to ground based systems.

This paper discusses security in UWCNs. It is structured as follows. The following section explains the major attacks. Subsequently, research challenges related to secure time synchronization, localization, and routing are described.

II. SECURITY CHALLENGES

Security is always an important requirement in communication systems. Sensitive data generated by the network should be protected from unauthorized disclosure. Data and control mechanisms likewise should provide integrity and authenticity guarantees. Even with confidentiality and integrity, the network is not achieving its objectives if the services provided by it are not available to authorized users when they need it. In addition to being a security problem, the inability of the network to perform its assigned task may be a safety hazard.

The major drawback of implementing powerful security mechanisms as in ground based system is the draining of the battery. Unlike ground based system all underwater sensor nodes are battery powered and it’s a scarce resource in underwater scenario. Three of the most devastating attacks in UWCNs are explained below. They are sybil attack, wormhole attack and sinkhole attack. These attack lead to Denial of Service (DoS), where the authorized receiver nodes are either denied the data packets or is fed with false information.

A. *Sybil Attack*

In all sensor networks each node is assigned a single identity. All network functions like routing, data forwarding etc. are done with this assumption. Malicious nodes create illegitimate multiple identities either by fabricating or stealing the identities of legitimate nodes. Hence a single node projects that it is present at different locations simultaneously. This is called sybil attack.

Basically, any peer-to-peer network wireless is vulnerable to sybil attack. Sybil attack disrupts routing protocols, data aggregation, fair resource allocation, misbehavior detection, voting, distributed storage etc. It is particularly devastating while choosing the next node to forward the data packets as a node may select a non-existent position of a malicious node. Fig. 1 illustrates a Sybil attack. Here the malicious node (shown in black) broadcast that it is present at multiple non-existent locations (shown in yellow). Neighbor nodes (here node A and B) may select this non-existent identities as the next node to route their data packets.

However, detection of sybil nodes in a network is not so easy. Radio resource testing method can be used to detect the presence of sybil nodes in sensor network and the probability to detect the existence of a sybil node by this method is:

$$Pr(detection) = 1 - (1 - \sum_{all S, M, G} \frac{\binom{s}{S}\binom{m}{M}\binom{g}{G}}{\binom{n}{c}} \frac{S-(m-M)}{c})^{r} \qquad (1)$$

Where, n is the number of nodes in the given set, s is the number of sybil nodes, m malicious nodes, g is taken as the number of good nodes, c is the number of nodes that can be tested simultaneously, of which S is the number of sybil nodes, M are malicious nodes, G are good nodes and r is the number of rounds to iterate the test.

In data aggregation protocols where data from nodes are aggregated, when a malicious sybil node is present it will be able to contribute to the aggregate more than once thus completely corrupting the aggregate data.

Some network resources are allocated on a per node basis using fair resource allocation principle. Sybil attacks are being effectively used for amassing resources by a malicious node unfairly and thus denying the authorized node their entitled share and give the attacker more resources to continue the attack effectively.

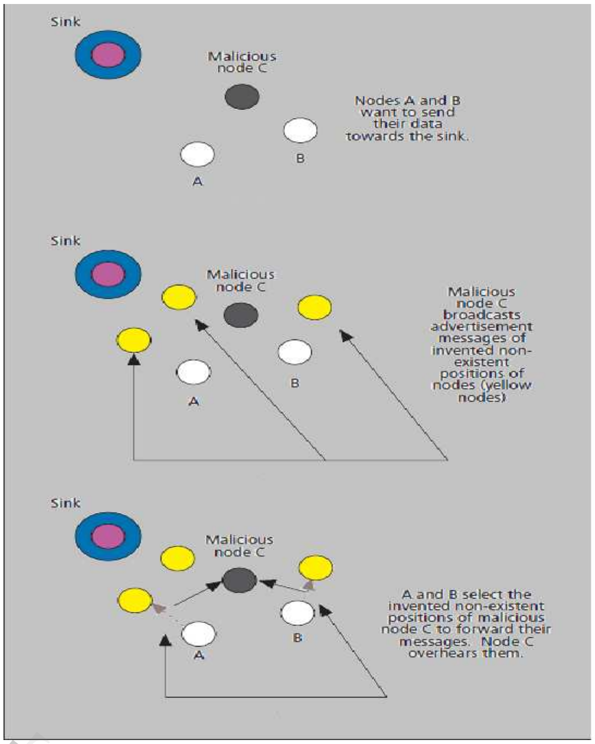
Sink
Malicious node C
Nodes A and B want to send their data towards the sink.
A
B
Sink
Malicious node C
Malicious node C broadcasts advertisement messages of invented non-existent positions of nodes (yellow nodes)
A
B
Sink
Malicious node C
A and B select the invented non-existent positions of malicious node C to forward their messages. Node C overhears them.
A
B

Fig. 1. Sybil attack

In a misbehavior detection algorithm, malicious sybil nodes will put the blame on other nodes and will never getting revoked itself.

Wireless sensor networks uses voting while performing a variable number of tasks. A Sybil attack can cause “stuff the ballot box” .Hence malicious nodes can control the outcome of such voting. Also sybil nodes can vouch for each other when checking for misbehaviors.

A distributed storage scheme may rely on there being three replicas of the same data to achieve a desired threshold of redundancy. If a malicious node in sybil attack mode pretends to be two of the three nodes, the algorithms used may effectively sense that redundancy has been achieved while in reality it has not.

B. *Wormhole Attack*

A wormhole is an out-of-band connection set up by an adversary promising low delay and high bandwidth. Since majority of the routing protocols choose paths with shorter delays, there is high probability for the network to undergo wormhole attack. Thus an enemy node can now monitor all the

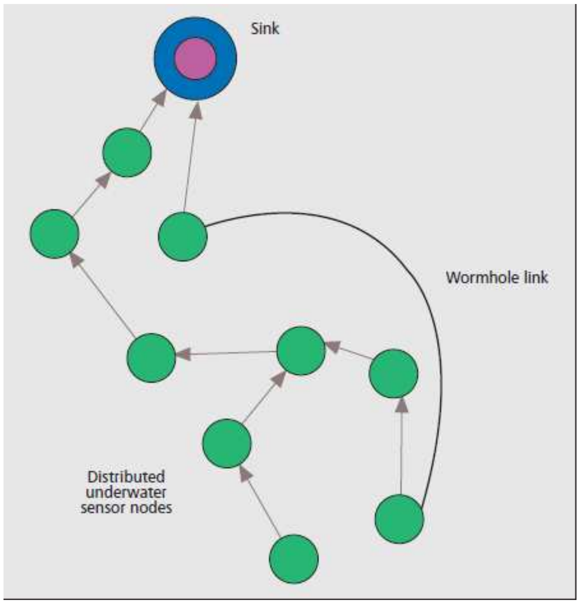

Fig. 2. Wormhole attack

traffic passing through the wormhole effectively. This attack has a tremendous effect on wireless networks, especially against routing protocols. Routing mechanisms can be confused and disrupted when routing control messages are tunneled to wrong direction. The tunnel formed through an attacker is referred as wormhole link. This link can be created either by a malicious node relying messages between two non-neighbor nodes or by a pair of malicious nodes communicating between each other via a fast link.

Fig. 2 shows a network under wormhole attack, here the solid dark connection shows the wormhole link. Since through the wormhole link only two nodes have to be crossed to reach the sink, routing protocols are more likely to select this path for forwarding the data packets.

This attack is particularly challenging to deal with since the adversary does not need to compromise any nodes and it could be performed even at the initial phase when the sensors start to discover the neighboring information. A wormhole receives a message at its “origin end" and sends it to its “destination end”. Mostly a wormhole is passive i.e. it does not send a message without receiving a message and static i.e. it does not move .The two connecting nodes in a wormhole is called as rogue access points. A rogue access point is not authorized by the network and these access points are set up by the enemy in order to capture important data from the network. The attacker has control over the rouge access point and can launch wormhole attack without the knowledge of the network and security keys in the network.

The creation of a wormhole can be by any of the following method:

- Tunneling the packets above the network layer.
- Long range tunneling using high power transmitters
- Tunneling via wired infrastructure.

Once the wormhole attackers have control of a link, they can actively disrupt the network. The wormhole attack can affect network routing, data aggregation, clustering protocols, and location-based wireless security systems. The wormhole attack cannot be defeated by cryptographical measures as wormhole attackers do not create any separate packets; they simply retransmit packets that already exist in the network, which can pass all cryptographic checks.

C. *Sinkhole Attack*

Sinkhole is a more complex attack. Given certain knowledge of the routing protocol in use, the attacker tries to attract the traffic from a particular region through it. In a sinkhole attack, the adversary’s aim is to lure nearly all the traffic from a particular area through a compromised node, creating a metaphorical sinkhole with the adversary at the center. Sinkhole attacks typically work by making a compromised node look especially attractive to surrounding nodes with respect to the routing algorithm. Sinkhole attacks are difficult to counter because routing information supplied by a node is difficult to verify.

As shown in fig. 3 a compromised node attracts all the traffic from its neighbors by telling its neighbor that it has shortest route to reach to the base station. This route is an artificial high quality route.

For example, the attacker can announce a false optimal path by advertising attractive power, bandwidth, or high quality routes to a particular region. Other nodes will then consider the path through this attacker node better than the currently used one, and move their traffic onto it. This results in congestion in the network and increases the energy consumption in the affected area and forms routing holes due to node failures. Since affected nodes depend on the attacker for their communication, the sinkhole attack can make other attacks efficient by positioning the attacker in busy information traffic.

Sinkhole attack is more effective in a flooding based protocol, the attacker listens to requests for routes then replies to the target nodes that it contains the high quality or shortest path to the base station. Once the malicious node has been able to insert itself between the two communicating nodes (for example, sink and sensor node), it is able to do anything with the packets passing between them. It can alter and drop packets that are being forwarded to that node.

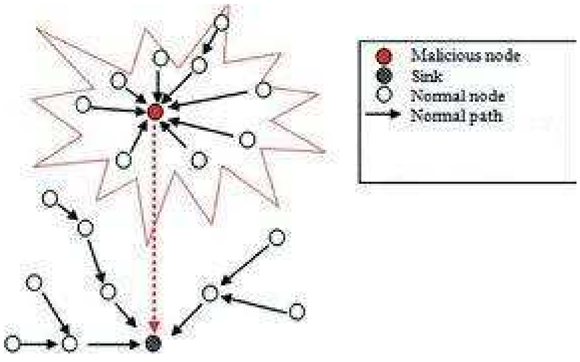

Fig. 3. Sinkhole attack

Hence sinkhole attack denies services to the authorized nodes and leads to DoS. In fact, this attack can affect even the nodes those are considerably far from the base stations. Many other attacks, such as eavesdropping, selective forwarding and black holes, etc., can be empowered by sinkhole attacks.

D. *Comparison between Wormhole and Sinkhole*

Even though both wormhole and sinkhole attacks lure traffic towards the malicious nodes, there are major differences between the two. The basic difference is the setting up of these attacks. In wormhole attacks out-of-band connections, which promises low delay and high bandwidth are being used. However in sinkhole attack no special connection is set up. The existing nodes are used to advertise high quality routes to the network. The main effects of wormhole attack are prevention of path detection algorithm where the out-of- band connections lead to the collapsing of path detection. Also wormhole attacks can lead to other attacks like selective forwarding, acknowledgement spoofing etc. Sinkhole leads to message modification and resource exhaustion as it lures all traffic in the affected area towards it. Both sinkhole and wormhole attacks affects link layer and network layer. Wireless sensor networks are fully vulnerable to both wormhole and sinkhole attacks.

Sinkhole attack detection is more hard compared to wormhole attack as in wormhole attack no nodes are compromised. Also sinkhole attack is more devastating than wormhole attack as it can affect nodes which are far away from the affected region. Most routing protocols are vulnerable to both sinkhole and wormhole attacks. Hierarchical routing where routing is done based on hierarchical addressing is vulnerable to both attacks. Location based routing where the geographical location is considered along with other parameters to decide the node for next hop is resistant to sinkhole attack but is vulnerable to wormhole attack. For network flow and Quality of Service (QoS) aware routing protocols where routes are selected based on energy and bandwidth efficiency and jitter and latency less paths, both wormhole and sinkhole attacks can be present.

TABLE I. COMPARISON BETWEEN WORMHOLE AND SINKHOLE ATTACK

Sl. No	**Parameter**	**Wormhole attack**	**Sinkhole attack**
1	Definition	Use out-of-band connections to lure traffic	Advertise high quality link to lure traffic
2	Effects	Prevention of path detection protocols and enables other attacks	Message modification and resource exhaustion
3	Layers involved	Link layer and network layer	Link layer and network layer
4	Vulnerability of sensor network	Fully vulnerable	Fully vulnerable
5	Detection level	Low	Medium
6	Damage level	Low	High
7	Hierarchical routing	Present	Present
8	Location based routing	Present	Absent
9	Network flow and QoS aware routing	Present	present
10	Defense mechanisms	Packet leash	Geographic forwarding

Packet leashing is done to packets in order to overcome wormhole attacks where each packet is time stamped i.e. each packet now contains the time at it was sent from the source node. Hence any packet reaching a sink from a distant node within a short time is sure to have traversed through an out-of-band wormhole link to arrive faster to the sink. For overcoming sinkhole attack geographic forwarding is used where the data packets are routed only to the neighbors and not to the node advertising high quality routes through it.

III. RESEARCH CHALLENGES

The security threats in an underwater systems can be overcome only when the underwater network is properly time synchronized, all the nodes are properly localized i.e. location of all nodes in the network are known and the packets are routed securely. These three factors are the major research challenges in any sensor network.

A. *Secure Time Synchronization*

Time synchronization is essential in many underwater applications like coordinated sensing tasks. Also, scheduling algorithms such as TDMA require precise timing between nodes to adjust their sleep-wakeup schedules for improving power efficiency. For example, in water quality monitoring, sensors are deployed at different depths because the chemical characteristics of water vary at each level. The design of a delay-tolerant time synchronization mechanism is very important to accurately locate the water contaminant source, set up the sleep-wake up schedules among neighboring nodes appropriately, and log the water quality data correctly into the annual database with accurate timing information.

Achieving precise time synchronization is especially difficult in underwater environments due to the time varying characteristics of UWCNs. For this reason, the time synchronization mechanisms proposed for ground-based sensor networks cannot be applied, and new mechanisms have been proposed. A multilateration algorithm is proposed for localization and synchronization in three-dimensional underwater acoustic sensor networks. It is assumed that a set of anchors, several buoys on the ocean surface, already know their locations and time without error. A group of nearby sensors receives synchronization packets containing the coordinates and packet transmit times from at least five anchor nodes and performs multilateration to obtain their own locations. The sensors learn the time difference between themselves and each anchor node by comparing their local times at which they received the time synchronization packet with the transmit time plus propagation delays; these nodes subsequently become new anchor nodes and thereafter broadcast new synchronization packets to a larger range, and so on[1]. None of the proposed time synchronization schemes consider security, although it is critical in the underwater environment. Time synchronization disruption due to masquerade, replay and message manipulation attacks, can be addressed using cryptographic techniques like private key method and using a central sink to verify the keys.

B. *Secure Localization*

Localization is a very important issue for data tagging where the coordinates or location of all nodes present in network has to be accurately known. Sensor tasks such as reporting the occurrence of an event or monitoring require localization information. Localization can also help in making routing decisions. For example, the underwater sensors in learn the location and speed of mobile beacons and neighbors during the localization phase; the position and motion of mobile beacons are used by the routing protocol to choose the best relay for a node to forward its data. Localization approaches proposed for ground-based sensor networks do not work well underwater because long propagation delays, Doppler effect, multipath, and fading cause variations in the acoustic channel. Bandwidth limitations, node mobility, and sparse deployment of underwater nodes also affect localization estimation. Proposed terrestrial localization schemes based on received signal strength (RSS) are not recommended in UWCNs, since non-uniform acoustic signal propagation causes significant variations in the RSS. Currently employed principles of Time of arrival (ToA) and time difference of arrival (TDoA) measurements require very accurate time synchronization (which is a challenging issue), and angle of arrival (AoA) algorithms are affected by the Doppler shift.ToA based algorithms estimate distances between nodes by measuring the propagation time of a signal. The basic principle is the same as radar or sonar, but is carried out in a distributed way among peering nodes.ToA measurement requires precise time synchronization between a sender and a receiver. Once the measurement is done among neighboring nodes, multilateration algorithms can be applied for each node to calculate its relative position to some reference nodes. If reference nodes are placed on buoys, they are able to use GPS to obtain precise global locations, which can then be used as references to all underwater nodes. Localization schemes are classified into two categories: range-based schemes (using range and/or bearing information) and range-free schemes (not using range or bearing information).While ranged based schemes find out the exact coordinates of nodes, range free schemes give only a coarse estimate on the position of nodes in the network .Range based schemes make use of anchors and mobile beacons to find the distance and bearing information of the sensor nodes present in the underwater network accurately.

C. *Secure Routing:*

Routing is essential for packet delivery in UWCNs. Routing is specially challenging in UWCNs due to the large propagation delays, the low bandwidth, the difficulty of battery refills of underwater sensors, and the dynamic topologies. Therefore, routing protocols should be designed to be energy-aware, robust, scalable and adaptive. The existing routing protocols are usually divided into three categories, namely *proactive, reactive and geographical routing protocols*.

1) Proactive Routing Protocols:

These protocols attempt to minimize the message latency induced by route discovery, by maintaining up to date routing information at all times from each node to every other node. This is obtained by broadcasting control packets that contain routing table information (e.g., distance vectors). These protocols have a large signaling overhead to establish routes for the first time and each time the network topology is modified because of mobility or node failures, since updated topology information has to be propagated to all the nodes. So each node now can establish a path to any node in the network.

2) Reactive Routing Protocols:

A node initiates a route discovery process only when a route to a destination is required. Once a route has been established, it is maintained by a route maintenance procedure until it is no longer desired. These protocols are more suitable for dynamic environments but incur a higher latency and still require source initiated flooding of control packets to establish paths.

3) Geographic Routing Protocols:

These protocols establish source destination paths by leveraging localization information, i.e. each node selects its next hop based on the position of its neighbors and of the destination node. Although these techniques are very promising, it is still not clear how accurate localization information can be obtained in the underwater environment with limited energy expenditure. In fact, fine-grained localization usually requires strict synchronization among nodes, which is difficult to achieve underwater due to the variable propagation delay.

In certain routing protocols, they autonomously establish the underwater network topology, controls network resources and establish network flows. The protocol relies on a centralized network manager running on the surface station. The manager implements network management and routing agents that periodically probe the nodes to estimate the channel characteristics. This information is exploited by the manager to establish efficient data delivery paths in a centralized fashion, which allows avoiding congestion and providing forms of quality of service guarantee. Routing schemes that are to be used for the three-dimensional underwater environment needs to be carefully devised. Especially, in the three-dimensional case the effect of currents should be taken into account, since the intensity and the direction of currents are dependent on the depth of the sensor node. Thus, underwater currents can modify the relative position of sensor devices and also cause connectivity holes, especially when ocean-column monitoring is performed in deep waters.

IV. CONCLUSION

Underwater wireless communication networks (UWCNs) consist of sensors and underwater vehicles that interact, coordinate and share information with each other to carry out sensing and monitoring functions. In the last several years, UWCNs has found widespread range of applications. Underwater communications are characterized by long propagation delay, low bandwidth, sound speed variability, signal attenuation, and many other environmental impairments. Due to these characteristics underwater communication is prone to attacks like sybil attack, wormhole attack, sinkhole attack etc. Open research issues in this area includes development of efficient and secure time synchronization schemes with small computation and communications costs, localization algorithms resistant to wormhole, sybil attacks etc. and finding routing paths devoid of undetected malicious nodes .

REFERENCES

[1] Domingo M.C, Securing Underwater Wireless Communication Networks,IEEE Wireless Communications,Volume 18,Issue 1,2011,pp 22-28.

[2] Akyildiz I.F, D. Pompili and T. Melodia, Underwater Acoustic Sensor Networks: Research Challenges, AdHocNet., March 2010.

[3] Tommaso Melodia and Ian F. Akyildiz, Underwater Sensor Networks:Research Challenges,IEEE Journal of Oceanic Engineering Volume 25(1) (2006) pp 72-83.