Underwater Wireless Communication:Its Necessity and Security

Ms. JUHI DIXIT[1], Asst.Prof. & Research Scholar
Department of Electronics and Communication Engineering
AMITY UNIVERSITY, M.P
juhiec21@gmail.com

Nripesh Gupta[2]
B.Tech (ECE), Amity School of Engineering and Technology
Amity University Madhya Pradesh, Gwalior, India
Email Id: nikky97gupta@gmail.com

Abstract
Underwater wireless communication systems are especially helpless against malicious assaults because of the high piece blunder rates, variable spread deferrals, and low data transfer capacity of acoustic channels. The one of kind qualities of the submerged acoustic communication channel and the contrasts between underwater sensor networks and their ground-based partners require the improvement of proficient and dependable security components. In this article, a total overview of security for UWCNs is introduced, and the exploration challenges for secure communication in this condition are outlined.

Index Terms- Underwater wireless communication networks (UWCNs), autonomous underwater vehicles (AUVs), Global Positioning System (GPS), Frequency hopping spread spectrum (FHSS), direct sequence spread spectrum (DSSS), Underwater sensor positioning (USP)

I. INTRODUCTION
Underwater wireless communication networks (UWCNs) are constituted by sensors and autonomous underwater vehicles (AUVs) that interact to perform specific applications such as underwater monitoring. Co-ordination and sharing of information between sensors and AUVs make the provision of security challenging. The aquatic environment is particularly vulnerable to malicious attacks due to the high bit error rates, large and variable propagation delays, and low bandwidth of acoustic channels. Achieving reliable inter vehicle and sensor-AUV communication is especially difficult due to the mobility of AUVs and the movement of sensors with water currents.
The unique characteristics of the underwater acoustic channel and the differences between underwater sensor networks and their ground based counterparts require the development of efficient and reliable security mechanisms

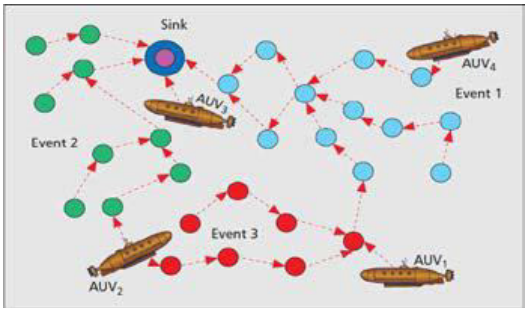

Fig: 1 Underwater Sensor Network with AUV

The following section explains the specific characteristics of UWCNs in comparison with their ground-based counterparts. Next, the possible attacks and countermeasures are introduced. Subsequently, security requirements for UWCNs are described. Later, the research challenges related to secure time synchronization, localization, and routing are summarized. Finally, the paper is concluded.

II. CHARACTERISTICS AND VULNERABILITIES OF UWCN
Underwater sensor networks have some similarities with their ground-based counterparts such as their structure, function, computation and energy limitations. Radio waves do not propagate well underwater due to the high energy absorption of water. Therefore, underwater communications are based on acoustic links characterized by large propagation delays. The propagation speed of acoustic signals in water (typically 1500 m/s) is five orders of magnitude lower than the radio wave propagation speed in free space. Acoustic channels have low bandwidth [1]. The link quality in underwater communication is severely affected by multipath, fading, and the refractive properties of the sound channel. As a result, the bit error rates of acoustic links are often high, and losses of connectivity arise. Underwater sensors move with water currents, and AUVs are mobile. The future development of geographical routing is very promising in UWCNs due to its scalability and limited signaling properties. However, it cannot rely on the Global Positioning System (GPS) because it uses radar waves in the 1.5 GHz band that do not propagate in water. Wireless underwater channels can be eavesdropped on. Attackers may intercept the information transmitted and attempt to modify or drop packets. Malicious nodes can create out-of band connections via fast radio (above the water surface) and wired links, which are referred to as wormholes. Since sensors are mobile, their relative distances vary with time. The dynamic topology of the underwater sensor network not only facilitates the creation of wormholes but it also complicates their detection. The above mentioned characteristics of UWCNs have several security implications. UWCNs suffer from the following vulnerabilities. High bit error rates cause packet errors. Consequently, critical security packets can be. Since underwater hardware is more expensive, underwater sensors are sparsely deployed. Underwater communication systems have more stringent power requirements than terrestrial systems because acoustic communications are more power - hungry, and typical transmission Distances in UWCNs are greater; hence, higher transmit power is required to ensure

coverage. Energy exhaustion attacks to drain the batteries of nodes pose a serious threat for the network lifetime.

III. ATTACKS ON UWCNS AND COUNTER MEASURES

A. *Jamming*

A jamming attack consists of interfering with the physical channel by putting up carriers on the frequencies neighbor nodes use to communicate. Since underwater acoustic frequency bands are narrow, UWCNs are vulnerable to narrowband jamming. Localization is affected by the replay attack when the attacker jams the communication between a sender and a receiver, and later replays the same message with stale information posing as the sender. Spread spectrum is the most common defense against jamming. Frequency hopping spread spectrum (FHSS) and direct sequence spread spectrum (DSSS) in underwater communications are drawing attention for their good performance under noise and multipath interference [2]. These schemes are resistant to interference from attackers, although not infallible. An attacker can jam a wide band of the spectrum or follow the precise hopping sequence when an FHSS scheme is used.

In ground-based sensor networks, other sensors located along the edge of the area under normal background noise and report intrusion to outside nodes. That will cause any further traffic to be rerouted around the jammed region. However, this solution cannot be applied to UWCNs, since nodes underwater are usually sparsely deployed, which means there would not be enough sensors to delimit the jammed region accurately and reroute traffic around it. Another solution proposed for ground-based sensor networks against jamming is to use alternative technologies for communication such as in fared or optical. However, this solution cannot be applied either, since optical and infrared waves are severely attenuated under water.

B. *Wormhole Attack*

A wormhole is an out-of-band connection created by the adversary between two physical locations in a network with lower delay and higher bandwidth than ordinary connections. In a wormhole attack the malicious node transfers some selected packets received at one end of the wormhole to the other end using the out-of-band connection, and re-injects them into the network. The effect is that false neighbor relationships are created, because two nodes out of each other's range can erroneously conclude that they are in proximity of one another due to the wormhole's presence [3]. This attack is devastating. Routing protocols choose routes that contain wormhole links because they appear to be shorter; thus, the adversary can monitor network traffic and delay or drop packets sent through the wormhole.

One proposed method for wormhole detection in ground-based sensor networks consists of estimating the real physical distance between two nodes to check their neighbor relationship. If the measured distance is longer than the nodes' communication range, it is assumed that the nodes are connected through a wormhole. However, accurate distance estimation depends on precise localization (geographical packet leashes, wormhole detection using position information of anchors), tight clock synchronization (temporal packet leashes), or use of specific hardware (directional antennas). In underwater communications accurate localization and time synchronization are still challenging. Since a wormhole contracts the virtual layout at certain regions, some nodes far away appear to be neighbors, and these contradictions can be detected visualizing the virtual layout.

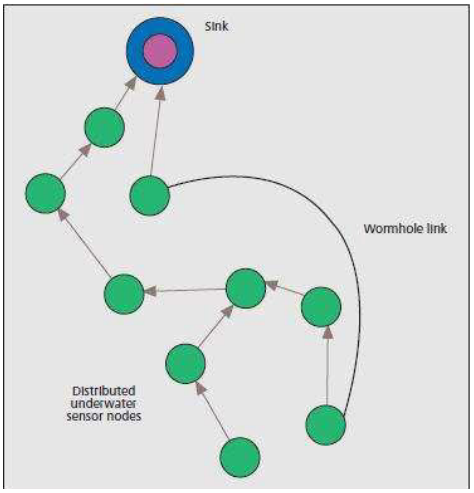

Fig: 2 Underwater Network with a Wormhole link

C. *Sinkhole Attack*

In a sinkhole attack, a malicious node attempts to attract traffic from a particular area toward it; for example, the malicious node can announce a high-quality route. Geographic routing and authentication of nodes exchanging routing information are possible defenses against this attack, but geographic routing is still an open research topic in UWCNs.

D. *Acknowledgment Spoofing*

A malicious node overhearing packets sent to neighbor nodes can use this information to spoof link layer acknowledgments with the objective of reinforcing a weak link or a link located in a shadow zone. Shadow zones are formed when the acoustic rays are bent and sound waves cannot penetrate. They cause high bit error rates and loss of connectivity. This way, the routing scheme is manipulated. A solution to this attack would be encryption of all packets sent through the network.

E. *Sybil Attack*

An attacker with multiple identities can pretend to be in many places at once. Geographic routing protocols are also misled because an adversary with multiple identities can claim to be in multiple places at once Authentication and position verification are methods against this attack, although position verification in UWCNs is problematic due to mobility.

F. *Selective Forwarding*

Malicious nodes drop certain messages instead of forwarding them to hinder routing. In UWCNs it should be verified that a receiver is not getting the information due to this attack and not because it is located in a shadow zone. Multipath routing and authentication can be used to counter this attack, but multipath routing increases communication overhead.

IV. SECURITY REQUIREMENTS

In UWCNs the following security requirements should be considered.

A. *Authentication*

Authentication is the proof that the data was sent by a legitimate sender. It is essential in military and safety-critical applications of UWCNs. Authentication and key establishment are strongly related because once two or more entities verify each other's authenticity, they can establish one or more secret keys over the open acoustic channel to exchange information securely; conversely, an already established key can be used to perform authentication [4].

A key generation system is proposed that requires only a threshold detector, lightweight computation, and communication costs. It exploits reciprocity, deep fades (strong destructive interference), randomness extractor, and robust secure fuzzy information reconciliatory. This way, the key is generated using the characteristics of the underwater channel and is secure against adversaries who know the number of deep fades but not their locations.

B. *Confidentiality*

Confidentiality means that information is not accessible to unauthorized third parties. Therefore, confidentiality in critical applications such as maritime surveillance should be guaranteed.

C. *Integrity*

It ensures that information has not been altered by any adversary. Many underwater sensor applications for environmental preservation, such as water quality monitoring, rely on the integrity of information [5].

D. *Availability*

The data should be available when needed by an authorized user.

Lack of availability due to denial-of-service attacks would especially affect time-critical aquatic exploration applications such as prediction of seaquakes.

V. SECURITY CHALLENGES

The security issues and open challenges for secure time synchronization, localization, and routing in UWCNs are summarized in the following sections

A. *Secure Time Synchronization*

Time synchronization is essential in many underwater applications such as coordinated sensing tasks. Also, scheduling algorithms such as time division multiple access (TDMA) require precise timing between nodes to adjust their sleep-wake up schedules for power saving. Achieving precise time synchronization is especially difficult in underwater environments due to the 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 [5]. A multilateration algorithm is proposed in for localization and synchronization in 3D 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. 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 there after broadcast new synchronization packets to a larger range, and so on. Time synchronization disruption due to masquerade, replay and message manipulation attacks, can be addressed using cryptographic techniques. However, countering other possible attacks such as delays (deliberate delaying the transmission of time synchronization messages) and DoS attacks requires the use of other strategies. The countermeasures against delay attacks proposed in for ground-based sensor networks are not applicable to UWCNs.

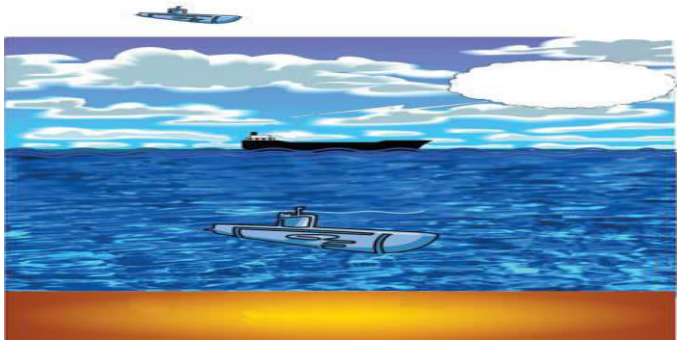

Fig: 3 Intruder Submarine Detection

If a coefficient of the window of data is below a threshold, it is an outlier value. If the abnormal percentage of data in one window (outlier percentage) is consistently (10 consecutive windows) higher than a predetermined threshold, the corresponding neighbor is flagged as a malicious node generating insider attacks. Node mobility due to water currents also modifies the propagation delays. In order to better distinguish between unintended and malicious timestamp alterations, the authors in improve the proposed scheme by using as a second step a statistical reputation and trust model to detect outlier timestamps, and identify nodes generating insider attacks. It is based on quantitative measurements and on the assumption that identifying an insider attacker requires long-term behavior observations. The following open research issues for secure time synchronization need to be addressed [8].

• Because of the high and variable propagation delays of UWCNs, the time required to synchronize nodes should be investigated.

• Efficient and secure time synchronization schemes with small computation and communications costs need to be designed to defend against delay and wormhole attacks.

B. *Secure Localization*

Localization is a very important issue for data tagging. 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 [7].

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. 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. Localization schemes can be classified into:

1) Range Based Scheme

The location of nodes in the network is estimated through precise distance or angle measurements [6].

•Anchor-based schemes:

Anchor nodes are deployed at the seabed or sea surface at locations determined by GPS. The propagation delay of sound signals between the sensor or AUV and the anchors is used to compute the distance to multiple anchor nodes.

•Distributed positioning schemes:

Positioning infrastructure is not available, and nodes communicate only with one-hop neighbors and compute their locations using multilateration.Underwater sensor positioning (USP) has been proposed in as a distributed localization scheme for sparse 3D networks, transforming the 3D underwater positioning problem into a 2D problem using a distributed no degenerative projection technique. Using sensor depth information [9] the neighboring reference nodes are mapped to the

•Schemes that use mobile beacons/anchors:

They use mobile beacons whose locations are always known. Scalable Localization with mobility prediction (SLMP) has been proposed in as a hierarchical localization scheme. At the beginning, only surface nodes know their locations, and anchor nodes can be localized by these surface buoys. Anchor nodes are selected as reference nodes because of their known locations; with the advance of the location process more ordinary nodes are localized and become reference nodes. During this process, every node predicts its future mobility pattern according to its past known location information. The future location is estimated based on this prediction.

2) Range Free Scheme

They have been designed as simple schemes to compute only coarse position estimates some localization specific attacks (replay attack, Sybil attack, and wormhole attack) have previously been described. Open research issues for secure localization are:

• Effective cryptographic primitives against injecting false localization information in UWCNs need to be developed.

• It is necessary to design resilient algorithms able to determine the location of sensors even in the presence of Sybil and wormhole attacks.

• Techniques to identify malicious or compromised anchor nodes and to avoid false detection of these nodes are required.

• Secure localization mechanisms able to handle node mobility in UWCNs need to be devised.

3) Secure Routing

Routing is essential for packet delivery in UWCNs. For example, the Distributed Underwater Clustering Scheme (DUCS) [17] does not use flooding and minimizes the proactive routing message exchange. 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. Many routing protocols have been proposed for underwater wireless sensor networks. However, none of them has been designed with security as a goal. Routing attacks can disable the entire network's operation. Spoofing, altering, or replaying routing information affects routing. Important routing attacks (selective forwarding, sinkhole attack, Sybil attack, wormhole attack, HELLO flood attack, acknowledgment spoofing) have been previously described. Although the attacks against routing in UWCNs are the same as in ground-based sensor networks, the same countermeasures are not directly applicable to UWCNs due to their difference in characteristics. Proposed broadcast authentication methods would cause high communication overhead and latency in UWCNs. Multipath routing would cause high communication overhead as well. Routing is specially challenging in UWCNs due to the large propagation delays, low bandwidth, difficulty of battery refills of underwater sensors, and dynamic topologies. Therefore, routing protocols should be designed to be energy-aware, robust, scalable and adaptive. Open research issues for secure routing are:

•There is a need to develop reputation-based schemes that analyze the behavior of neighbors and reject routing paths containing selfish nodes that do not cooperate in routing. The proper functioning of these schemes is challenging because they do not work well in mobile environments, the time required to detect compromised nodes increases substantially in UWCNs due to the long propagation delays, and they must be adapted to tolerate short-term disruptions.

•Quick and powerful encryption and authentication mechanisms against outside intruders should be devised for UWCNs because the time required for intruder detection is high due to the long and variable propagation delays, and routing paths containing undetected malicious nodes can be selected in the meantime for packet forwarding.

•Sophisticated mechanisms should be developed against insider attacks such as selective forwarding, Sybil attacks, HELLO flood attacks, and acknowledgment spoofing.

•There is a need to develop new techniques against sinkholes and wormholes, and improve existing ones. With Dis-VoW [2] a wormhole attack can still be concealed by manipulating the buffering times of distance estimation packets. The wormhole-resilient neighbor discovery in [5] is affected by the orientation error between sensors.

VI. CONCLUSION

In this paper I have discussed security in UWCNs, underlining the specific characteristics of these networks, possible attacks, and countermeasures. The main research challenges related to secure time synchronization, localization, and routing have also been surveyed. These research issues remain wide open for future investigation.

REFERENCES

[1] I. F. Akyildiz, D. Pompili, and T. Melodia, "*Underwater Acoustic Sensor Networks: Research Challenges," Ad Hoc Net*. vol. 3, no. 3, Mar. 2005.

[2] A. D. Wood and J. A. Stankovic, *"A Taxonomy for Denial-of-Service Attacks in Wireless Sensor Networks*,"[1] chapter in *Handbook of Sensor Networks: Compact Wireless and Wired Sensing Systems*, M. Ilyas and I. Mahgoub, Eds., CRC Press, 2004.

[3] L. Buttyán and J.-P. Hubaux, *Security and Cooperation in Wireless Networks: Thwarting Malicious and Selfish Behavior*[2] *in the Age of Ubiquitous Computing*, Cambridge Univ. Press, 2008.

[4] Y. Liu, J. Jing, and J. Yang, *"Secure Underwater Acoustic Communication Based on a Robust Key Generation Scheme,"*[3] *Proc. ICSP*, 2008.

[5] F. Hu, S. Wilson, and Y. Xiao, *"Correlation-Based Security in Time Synchronization of Sensor Networks," Proc. IEEE WCNC*, 2008.

[6] C. Tian *et al*., "*Localization and Synchronization for 3D Underwater Acoustic Sensor Networks,"* in *Ubiquitous Intelligence and Computing*, LNCS, Springer, 2007, pp. 622–31.

[7] M. Erol and S. Oktug, *"A Localization and Routing Framework for Mobile Underwater Sensor Networks,"* Proc. *IEEE INFOCOM*, Apr. 2008.

[8] H. Song, S. Zhu, and G. Cao, "*Attack-Resilient Time Synchronization for Wireless Sensor Networks," Ad Hoc Net*., vol. 5, no. 1, 2007, pp. 112– 25.

[9] W. Cheng *et al*., *"Underwater Localization in Sparse 3D Acoustic Sensor Networks," Proc. IEEE INFOCOM*, 2008.

[10] N. Chirdchoo, W.-S. Soh, and K. Chua, "MU-Sync: A Time Synchronization Protocol for Underwater Mobile Networks," *Proc. WUWNet*, 2008.

[11] Y. Zhou *et al*., "A Range-free Localization Scheme for Large Scale Underwater Wireless Sensor Networks," *J Shanghai Jiaotong Univ. (Science)*, vol. 14, no. 5, 2009, pp. 562–68.

.