ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 4, April 2018

Security in Underwater Wireless Communication

[1] L.Vetrivendan,[2] Dr.R.Viswanathan, [3]K.Punitharaja
[1][3] Assistant Professor, [2]Associate Professor
[1][2][3] Galgotias University

Abstract: Underwater wireless communication networks are particularly vulnerable to malicious attacks due to the high bit error rates, large and variable propagation delays, and low bandwidth of acoustic channels. The unique characteristics of the underwater acoustic communication channel and the differences between underwater sensor networks and their ground-based counterparts require the development of efficient and reliable security mechanisms. In this paper a complete survey of security for UWCNs is presented, and the research challenges for secure communication in this environment are outlined.
Index Terms- Bandwidth, Security, Underwater sensors.

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. Coordination 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 [1].

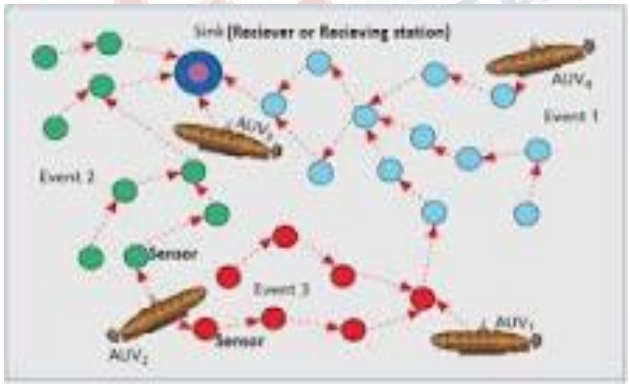

Figure 1: Underwater sensor network with AUV

Underwater wireless communication autonomous underwater vehicles (AUVs) that move to perform specific applications cherish underwater watching (Fig. 1) Coordination and sharing of knowledge between sensors and AUVs build the supply of security difficult. The aquatic atmosphere is especially susceptible to malicious attacks because of the high bit error rates, massive and variable propagation delays, and low information measure of acoustic channels. Achieving reliable entomb vehicle and sensor-AUV communication is very tough because of the quality of AUVs and therefore the movement of sensors with water currents. This paper discusses security in UWCNs. it's structured as follows. the subsequent section explains the particular characteristics of UWCNs compared with their ground based counterparts. Next, the doable attacks and countermeasures square measure introduced. later on, security necessities for UWCNs square measure delineated. Later, the analysis challenges involving secure time synchronization, localization, and routing square measure summarized. Finally, the paper is all over

CHARACTERISTICS AND VULNERABILITIES OF UWCN

Underwater detector networks have some similarities with their ground-based counterparts love their structure, function, computation and energy limitations. Radio waves don't propagate well underwater thanks to the high energy absorption of water. Therefore, underwater communications area unit supported acoustic links characterised by massive propagation delays. The propagation speed of acoustic signals in water (typically 1500 m/s) is 5 orders of magnitude less than the nonparticulate radiation propagation speed in free house. Acoustic channels have low information measure [1]. The link quality in underwater communication is severely full of multipath, fading, and also the refractive properties of the sound channel. As a result, the bit error rates of acoustic links are usually high, and losses of property

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 4, April 2018

arise. Underwater sensors move with water currents, and AUVs are mobile. the long run development of geographical routing is extremely promising in UWCNs thanks to its measurability and restricted communication properties. However, it cannot admit the worldwide Positioning System (GPS) as a result of it uses radiolocation waves within the one.5 GHz band that don't propagate in water. Wireless underwater channels will be eavesdropped on. Attackers could intercept the knowledge transmitted and conceive to modify or drop packets. Malicious nodes will produce out of band connections via quick radio (above the water surface) and wired links, that are cited as wormholes. Since sensors are mobile, their relative distances vary with time. The dynamic topology of the underwater detector network not solely facilitates the creation of wormholes however it conjointly complicates their detection. The higher than mentioned characteristics of UWCNs have many security implications. UWCNs suffer from the subsequent vulnerabilities. High bit error rates cause packet errors. Consequently, vital security packets are often. Underwater device networks have some similarities with their ground based counterparts cherish their structure, function, computation and energy limitations. However, they even have variations, which may be summarized as follows. Radio waves don't propagate well underwater because of the high energy absorption of water. Therefore, underwater communications square measure supported acoustic links characterised by massive propagation delays. The propagation speed of acoustic signals in water (typically 1500 m/s) is 5 orders of magnitude not up to the nonparticulate radiation propagation speed in free area. Acoustic channels have low information measure. The link quality in underwater communication is severely suffering from multipath, fading, and therefore the refractive properties of the sound channel. As a result, the bit error rates of acoustic links square measure usually high, and losses of property arise underwater sensors move with water currents, and AUVs square measure mobile. the long run development of geographical routing is extremely promising in UWCNs because of its quantifiability and restricted sign properties. However, it cannot believe the world Positioning System (GPS) as a result of it uses measuring system waves within the one.5 GHz band that don't propagate in water. Since underwater hardware is dearer, underwater sensors area unit sparsely deployed. Underwater communication systems have a lot of tight power necessities than terrestrial systems as a result of acoustic communications area unit a lot of power - hungry, and typical transmission distances in UWCNs area unit greater; thus, higher transmit power is needed to confirm coverage. The dynamic topology of the underwater sensing element network not solely facilitates the creation of wormholes however it additionally complicates their detection. Since power consumption in underwater communications is more than in terrestrial radio communications, and underwater sensors square measure sparsely deployed, energy exhaustion attacks to empty the batteries of nodes cause a heavy threat for the network lifespan.

ATTACKS ON UWCNS AND COUNTERMEASURES

Jamming

An electronic jamming attack consists of meddlesome with the physical channel by putt up carriers on the frequencies neighbour nodes use to speak. Since underwater acoustic frequency bands area unit slender, UWCNs area unit prone to narrowband electronic jamming. Localization is tormented by the replay attack once the offender jams the communication between a sender and a receiver, and later replays identical message with stale info motility because the sender. unfold spectrum is that the commonest defence against electronic jamming. Frequency hopping unfold spectrum (FHSS) and direct sequence unfold spectrum (DSSS) in beneath water communications area unit drawing attention for his or her smart performance under noise and multipath interference [2]. These schemes square measure immune to interference from attackers, though not infallible. associate assailant will jam a good band of the spectrum or follow the precise hopping sequence once associate FHSS theme is employed. In ground-based device networks, different sensors situated on the sting of the realm underneath traditional background signal and report intrusion to outside nodes. which will cause from now on traffic to be rerouted round the packed region. However, this resolution can't be applied to UWCNs, since nodes underwater square measure sometimes sparsely deployed, which implies there wouldn't be enough sensors to delimit the packed region accurately and reroute traffic around it. Another resolution projected for ground-based detector networks against electronic countermeasures is to use various technologies for communication resembling in fared or optical. However, this resolution can't be applied either, since optical and infrared waves square measure severely attenuated below water.

Wormhole Attack

A hollow is associate degree out-of-band association created by the someone between 2 physical locations in a very network with lower delay and better information measure than normal connections. in a very hollow attack

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 4, April 2018

the malicious node transfers some chosen packets received at one finish of the hollow to the opposite finish victimisation the out-of-band association, and re-injects them into the network. The result is that false neighbour relationships area unit created, as a result of 2 nodes out of every other's vary will mistakenly conclude that they're in proximity of 1 another because of the wormhole's presence [3]. This attack is devastating. Routing protocols select routes that contain hole links as a result of they seem to be shorter; therefore, the resister will monitor network traffic and delay or drop packets sent through the hole.

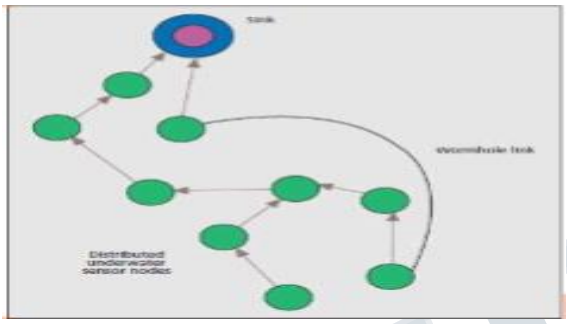

Figure 2: Underwater network with a wormhole link

One planned methodology for hollow detection in ground based device networks consists of estimating the important physical distance between 2 nodes to visualize their neighbour relationship. If the measured distance is longer than the nodes' communication varies, it's assumed that the nodes square measure connected through a hollow. However, correct distance estimation depends on precise localization (geographical packet leashes, hollow detection mistreatment position info of anchors), tight clock synchronization (temporal packet leashes), or use of specific hardware (directional antennas). In underwater communications correct localization and time synchronization square measure still difficult. Since a hollow contracts the virtual layout at sure regions, some nodes isolated seem to be neighbours, and these contradictions may be detected visualizing the virtual layout. Sinkhole Attack

In a swallow hole attack, a malicious node tries to draw in traffic from a selected space toward it; as an example, the malicious node will announce a high-quality route. Geographic routing and authentication of nodes exchanging routing data area unit attainable defences against this attack, however geographic routing continues to be associate degree open analysis topic in UWCNs.

Sybil Attack

An assaulter with multiple identities will faux to be in several places promptly. Geographic routing protocols area misled as a result of AN resister with multiple identities will claim to be in multiple places promptly Authentication and position verification are ways against this attack, though position verification in UWCNs is problematic because of quality.

SECURITY REQUIREMENTS

In UWCNs the following security requirements should be considered.

Authentication

Authentication is that the proof that the information was sent by a legitimate sender. it's essential in military and safety critical applications of UWCNs. Authentication and key institution ar powerfully connected as a result of once 2 or additional entities verify every other's believability, they will establish one or additional secret keys over the open acoustic channel to exchange data securely; conversely, associate degree already established key may be accustomed perform authentication [4]. A key generation system is planned that needs solely a threshold detector, light-weight computation, and communication prices. It exploits reciprocity, deep fades (strong harmful interference), randomness extractor, and sturdy secure fuzzy data reconciliatory. This way, the secret's generated victimization the characteristics of the underwater channel and is secure against adversaries UN agency recognize the quantity of deep fades however not their locations.

Confidentiality

Confidentiality implies that data isn't accessible to unauthorized third parties. Therefore, confidentiality in vital applications similar to maritime police work ought to be warranted.

Integrity

It ensures that data has not been altered by any human. several underwater device applications for environmental preservation, equivalent to water quality observation, deem the integrity of knowledge [5].

Availability

The data ought to be on the market once required by a certified user. Lack of convenience thanks to denial-of-service attacks would particularly have an effect on time-critical aquatic exploration applications akin to prediction of seaquakes.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 4, April 2018

SECURITY CHALLENGES

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

Secure Time Synchronization

Time synchronization is important in several underwater applications resembling coordinated sensing tasks. Also, programing algorithms resembling time division multiple access (TDMA) need precise temporal order between nodes to regulate their sleep-wake up schedules for power saving. Achieving precise time synchronization is particularly tough in underwater environments because of the characteristics of UWCNs. For this reason, the time synchronization mechanisms planned for ground-based sensing element networks cannot be applied, and new mechanisms are planned [5]. A multilateration algorithmic program is planned certain localization and synchronization in 3D underwater acoustic detector networks. it's assumed that a collection of anchors, many buoys on the ocean surface, already recognize their locations and time while not error. The sensors learn the time distinction between themselves and every anchor node by examination their native times at that they received the time synchronization packet with the transmit time and propagation delays; these nodes afterward become new anchor nodes and thenceforth there once broadcast new synchronization packets to a bigger vary, and so on. Time synchronization disruption because of masquerade, replay and message manipulation attacks, may be addressed victimisation crypto graphical techniques. However, countering alternative potential attacks similar to delays (deliberate delaying the transmission of your time synchronization messages) and DoS attacks needs the employment of alternative methods. The countermeasures against delay attacks projected sure ground-based sensing element networks don't seem to be applicable to UWCNs. If a constant of the window of information is below a threshold, it's associate degree outlier worth. If the abnormal proportion of information in one window (outlier percentage) is systematically (10 consecutive windows) on top of a planned threshold, the corresponding neighbour is flagged as a malicious node generating corporate executive attacks. Node quality thanks to water currents conjointly modifies the propagation delays. so as to raised distinguish between causeless and malicious timestamp alterations, the authors in improve the projected theme by victimization as a second step a applied math name and trust model to sight outlier timestamps, and determine nodes generating corporate executive attacks. it's supported quantitative measurements associate degreed on the idea that distinctive an corporate executive wrongdoer needs long-run behaviour observations. the subsequent open analysis problems for secure time synchronization ought to be addressed [6].

• Because of the high and variable propagation delays of UWCNs, the time needed to synchronize nodes ought to be investigated.
• Efficient and secure time synchronization schemes with tiny computation and communications prices got to be designed to defend against delay and hollow attacks [7].

Secure Localization

Localization could be a vital issue for knowledge tagging. detector tasks comparable to coverage the incidence of an occasion or observation need localization info. Localization also can facilitate in creating routing choices. maybe, the underwater sensors in learn the situation and speed of mobile beacons and neighbours throughout the localization phase; the position and motion of mobile beacons square measure employed by the routing protocol to decide on the simplest relay for a node to forward its knowledge. Localization approaches planned for ground-based detector networks don't work well underwater as a result of long propagation delays, Doppler shift, multipath, and weakening cause variations within the acoustic channel. information measure limitations, node quality, and thin preparation of underwater nodes conjointly have an effect on localization estimation [8]. planned terrestrial localization schemes supported received signal strength (RSS) don't seem to be suggested in UWCNs, since non-uniform acoustic signal propagation causes important variations within the RSS. Time of arrival (ToA) and time distinction of arrival (TDoA) measurements need terribly correct time synchronization (which could be a difficult issue), and angle of arrival (AoA) algorithms square measure tormented by the propagation. Localization schemes are often classified into:

Range-based schemes

The location of nodes within the network is calculable through precise distance or angle measurements [9].

Anchor-based schemes

Anchor nodes are deployed at the bed or ocean surface at locations determined by GPS. The propagation delay of sound signals between the device or AUV and therefore the anchors is employed to figure the gap to multiple anchor nodes.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 4, April 2018

Distributed positioning schemes

Positioning infrastructure isn't obtainable, and nodes communicate solely with one-hop neighbours and cipher their locations victimization multilateration. Underwater detector positioning (USP) has been projected in as a distributed localization theme for thin 3D networks, reworking the 3D underwater positioning downside into a second downside employing a distributed no chronic projection technique. Using sensor depth information [9] the neighbouring reference nodes are mapped to the

•Schemes that use mobile beacons/anchors:

They use mobile beacons whose locations area unit invariably glorious. ascendible Localization with quality prediction (SLMP) has been planned in as a class-conscious localization theme. At the start, solely surface nodes grasp their locations, and anchor nodes will be localized by these surface buoys. Anchor nodes area unit hand-picked as reference nodes due to their glorious locations; with the advance of the placement method a lot of standard nodes area unit localized and become reference nodes. throughout this method, each node predicts its future quality pattern per its past glorious location data. the longer term location is calculable supported this prediction. Range-free schemes (not victimisation vary or bearing information): they need been designed as straightforward schemes to reason solely coarse position estimates some localization specific attacks (replay attack, Sybil attack, worm hole attack) have antecedent been delineating. planned broadcast authentication strategies would cause high communication overhead and latency in UWCNs.

Open analysis problems for secure routing are:

•There may be a got to develop reputation-based schemes that analyse the behaviour of neighbours and reject routing methods containing stingy nodes that don't collaborate in routing.

•Quick and powerful cryptography and authentication mechanisms against outside entrants ought to be devised for UWCNs as a result of the time needed for intruder detection is high thanks to the long and variable propagation delays, and routing methods containing unseen malicious nodes is elite within the meanwhile for packet forwarding [10].

• Sophisticated mechanisms ought to be developed against business executive attacks equivalent to selective forwarding, Sybil attacks, hi flood attacks, and acknowledgment spoofing.

• There is a necessity to develop new techniques against sinkholes and wormholes, and improve existing ones. With Dis-VoW a hollow attack will still be hide by manipulating the buffering times of distance estimation packets. The wormhole-resilient

CONCLUSIONS

In this paper I actually have mentioned security in UWCNs, underlining the precise characteristics of those networks, attainable attacks, and countermeasures the most analysis challenges involving secure time synchronization, localization, and routing have conjointly been surveyed. These analysis problems stay 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," 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 Behaviour 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," Proc. ICSP, 2008.

[5] Domingo, Mari Carmen. "Securing underwater wireless communication networks." IEEE Wireless Communications 18, no. 1 (2011).

[6] Cui, Jun-Hong, Jiejun Kong, Mario Gerla, and Shengli Zhou. "The challenges of building mobile underwater wireless networks for aquatic applications." Ieee Network 20, no. 3 (2006): 12-18.

[7] Loo, Jonathan, Jaime Lloret Mauri, and Jesus Hamilton Ortiz, eds. Mobile ad hoc networks: current status and future trends. CRC Press, 2016.

[8] Jaruwatanadilok, Sermsak. "Underwater wireless optical communication channel modeling and performance evaluation using vector radiative transfer

theory." IEEE Journal on Selected Areas in Communications 26, no. 9 (2008).

[9] Cong, Yanping, Guang Yang, Zhiqiang Wei, and Wei Zhou. "Security in underwater sensor network." In Communications and Mobile Computing (CMC), 2010 International Conference on, vol. 1, pp. 162-168. IEEE, 2010.

[10] Gkikopouli, Andrianna, George Nikolakopoulos, and Stamatis Manesis. "A survey on underwater wireless sensor networks and applications." In Control & Automation (MED), 2012 20th Mediterranean Conference on, pp. 1147-1154. IEEE, 2012.