International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 06 Issue: 12 | December - 2022 Impact Factor: 7.185 ISSN: 2582-3930

Advanced Security Techniques for Underwater Wireless Communication: An Overview

Faizan Khan
VIT Bhopal University, Bhopal

ABSTRACT

Underwater wireless communication refers to the communication system taken into consideration underwater but limited to acoustic, radio frequency and optical wireless communication. Underwater wireless communication networks are vulnerable to the malicious attacks due to high bit error rates, large and vulnerable propagation delays and low bandwidth of acoustic channels. This paper offers an overview on the security attacks, requirements and security challenges.

Keywords: Underwater wireless communication network (UWCN); security challenges; security requirements; security attacks.

1. INTRODUCTION

Underwater wireless communication Networks (UWCNs) are constituted by Sensors and Autonomous Underwater Vehicles (AUVs) that move to perform specific application like underwater monitoring and sharing of information between sensors and AUVs makes the security challenging. The aquatic environment is vulnerable to malicious attack due to high bit error rates, large and variable propagation delays and low bandwidth of acoustic channel.

Achieving inter vehicle and sensor AUV communication becomes difficult due to the mobility of AUVs and movement of sensors. The special characteristic of underwater acoustic channel and dissimilarity between Underwater sensor network and their ground based counterparts requires the development of efficient security mechanism.[1]

2. ATTACKS ON UNDERWATER WIRELESS COMMUNICATION NETWORKS

1. **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]

2. **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.[2]

3. **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.[2]

4. **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.[4]

5. **Wormhole**

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. 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.[3]

6. **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.[4]

3. SECURITY REQUIREMENTS

In UWCNs the following security requirements should be considered

1. **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. Traditional solutions for key generation and update algorithms should be adapted to better address the characteristics of the underwater channel. A key generation system is proposed that requires only a threshold detector, lightweight computation, and communication costs.[4]

2. **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.

3. **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.

4. **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.

4. SECURITY CHALLENGES

1. 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. Tri-Message is a time synchronization protocol designed for high-latency networks with a synchronization precision that increases with distance. A multilateration algorithm is proposed in for localization and synchronization in 3D underwater caustic sensor networks. It is assumed that a set of anchors, several buoys on the ocean surface, already know their locations and time without error[5]

2. Localization security

Location estimation is a vital component in source detection and tracking applications. The underwater sensor nodes get the location information and speed of mobile nodes during the localization phase, which would be used to select the best relay node to forward data. Without the location information, the sink node cannot identify where the received data comes from. Due to the characteristics of underwater channel, localization protocols proposed for WSNs cannot work in underwater applications. Some localization-specific attacks e.g. Sybil attack, black hole attack and wormhole attack can cause great damages by utilizing or modifying the localization information. Most of existing localization protocols do not take security issues into account when designing. The secure localization scheme should be able to determine the location of sensors even in the presence of Sybil and wormhole attacks, and the scheme should be able to node mobility in UWSNs. To defend against injecting false localization information in UWSNs, effective and efficient cryptographic algorithms need to be developed.[6]

3. Routing security

Routing is essential for packet delivery in UWCNs. For example, the Distributed Underwater Clustering Scheme (DUCS) 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 difficulties of battery refills of underwater sensors, and the dynamic topologies. Therefore, routing protocol should be designed to be energy-aware, robust, scalable and adaptive. Many routing protocols have been proposed for underwater wireless sensor network .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.[6]

5. CONCLUSION

This paper gives the overall view of the necessity of underwater wireless communication. Despite much development in this area of the underwater wireless communication, there is still an immense scope so more research as major part of the ocean bottom yet remains unexploded.

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.

6. FUTURE WORK

Underwater Sensor Networks is a very recent technology that tries to follow the same steps than terrestrial wireless networks in a very different and challenging network environment.

The research issues remain wide open for future investigation, and find the best technique is range free distributed positioning scheme because its provide the large scale range and range free technique at present time.

7. REFERENCES

1. Lakshmanan, Vetrivendan & Ramasamy, Viswanathan. (2018). Security in Underwater Wireless Communication. 10.13140/RG.2.2.19774.95040.

2. Pravin M. Pandav, Prof. N. J. Padole "STUDY OF UNDERWATER WIRELESS COMMUNICATION SYSTEM AND VULNERABILITIES, SECURITY" International Journal of Advanced Innovative Technology in Engineering (IJAITE), Vol. 1, Special Issue 2, July-2016

3. Kumar, Dr Rajeev. (2019). Security Analysis and Issues in Underwater Wireless Sensor Auditory and Multipath Network. The International journal of analytical and experimental modal analysis. 11. 2269-2271

4. Yildiz, Huseyin. (2019). Prolonging the Lifetime of Underwater Sensor Networks Under Sinkhole Attacks. 1-5. 10.1145/3366486.3366516.

5. Ekta Deshmukh , Rajendra Singh Yadav , Nandini Upadhyay "Securing underwater wireless communication networks," in IJARCCE, Smart And Innovative Technologies In Engineering And Sciences Gyan Ganga College of Technology Vol. 5, Special Issue 3, November 2016

6. Guang Yang, Lie Dai, Guannan Si, Shuxin Wang, Shouqiang Wang,
Challenges and Security Issues in Underwater Wireless Sensor Networks, Procedia Computer Science,Volume 147,2019, Pages 210-216, ISSN 1877-0509