Attacks and Securing Under Water Wireless Communication Networks

K.GopikrishnamaRaju, A. Vijay Kumar, G. Anil Kumar, V. Ravi Kiran
Computer Science Department, B.Tech
JNTUA College of Engineering, Pulivendula.
Email: gopikrishna.kasiraju@gmail.com, avijavijaykumar@gmail.com

Abstract—The unique characteristics of the underwater acoustic communication channel, and the differences between underwater sensor networks and their ground-based counterparts require for the development of efficient and reliable security mechanisms are discussed. Underwater wireless communicationnetworks are particularly vulnerable to malicious attacks due to the high bit error rates, large and variable propagation delays, and low bandwidth of acoustic channels. A complete survey of securing underwater wireless communication networks is presented, and the research challenges for secure communication in this environment are outlined.Acoustic channels have low bandwidth. 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.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 above mentioned characteristics of UWCNs have several security implications. UWCNs suffer from the vulnerabilities which decreases the reliability. So, this article have discussed for security in UWCNs, underlining the specific characteristics of these networks, possible attacks, countermeasures and challenges.

Keywords:UWCN, Acoustic waves, Attacks, Security Requirements

1. INTRODUCTION

Underwater wireless communication networks (UWCNs) are constituted by sensors and autonomous underwater vehicles (AUVs) that interact to perform specific applications such as sensing and monitoring functions [1].Here communication done by acoustic signals. It means instead of electromagnetic waves the acoustic waves are used. Coordination and sharing of information between sensors and AUVs make the stipulation of security challenging. The aquatic channel 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 communication is especially difficult due to the mobility of AUVs and the movement of sensors with water currents. The differences between underwater sensor networks and their ground based counterparts and the unique characteristics of the underwater acoustic channel require the development of efficient and reliable security mechanisms.

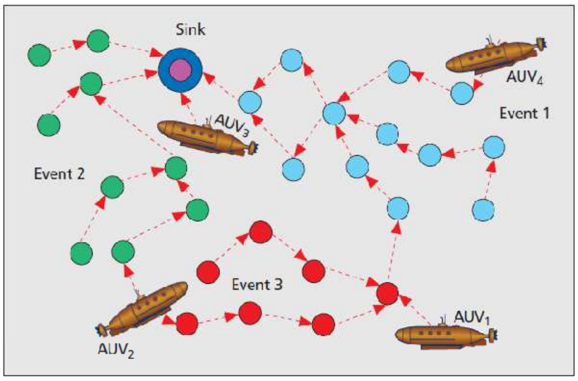

Fig 1: Underwater sensor network with AUVs.

2. LITERATURE SURVEY:

Mari Carmen Domingo, Barcelona Tech University, “**Securing Underwater Wireless Networks**”, IEEE Wireless Communications, February 2011 gave a list of attacks in under water wireless communication and counter measures, complete survey of securing under water wireless communication [1].

F. Akyildiz, D. Pompili, and T. Melodia, **“Underwater Acoustic Sensor Networks: Research Challenges”** gave several fundamental key aspects of underwater acoustic communications are investigated [2]. The characteristics of the underwater channel are detailed. The main challenges for the development of efficient networking solutions posed by the underwater environment are detailed and a cross-layer approach to the integration of all communication functionalities is suggested.

W. Wang et al**., "Visualization of Wormholes in Underwater Sensor Networks: A Distributed Approach,"** propose a distributed mechanism of Visualisation of wormholes (Dis-VoW) to detect wormhole attacks in under-water sensor networks [3]. In Dis-VoW, every sensor reconstructs local network layout using multi-dimensional scaling [5]. It detects the wormholes by visualising the distortions in edge lengths and angles among neighbouring sensors [6].

Y. Liu, J. Jing, and J. Yang, "**Secure Underwater Acoustic Communication Based on a Robust Key Generation Scheme**" describes two parties in the communication, after authentication, generally use a secure symmetric key to encrypt all the data they transmit. Thus, an efficient key generation algorithm is in urgent need to guarding the privacy of the communication data [7]. .

F. Hu, S. Wilson, and Y. Xiao, "**Correlation-Based Security in Time Synchronization of Sensor Networks**"Chemical Water Sensors can be used for such long-term monitoring purpose. In this paper, they propose a scalable, low-energy, delay-tolerant Water-quality monitoring sensor network (WATER) model, which has essential differences from terrestrial radio sensor networks due to its highly variable, long propagation delay and mobility nature [8].

M. Erol and S. Oktug, "**A Localization and Routing Framework for Mobile Underwater Sensor Networks**"they propose a framework to establish localization and routing in mobile underwater sensor networks. Localization and routing are done at two consecutive rounds. Localization messages include localization specific data and additional fields which are used in the routing decision [9].

H. Song, S. Zhu, and G. Cao, "**Attack-Resilient Time Synchronization for Wireless Sensor Networks**". In this paper, they first identify various attacks that are effective to several representative time synchronization schemes, and then focus on a specific type of attack called delay attack, which cannot be addressed by cryptographic techniques. Next they propose two approaches to detect and accommodate the delay attack.

Finally they show the effectiveness of these two schemes through extensive simulations.

Based upon all references this paper highlights the unique characteristics of the underwater acoustic communication channel and explores a complete survey of securing underwater wireless communication networks

3. CHARACTERISTICS & VULNERABILITY

Underwater sensor networks have some similarities with their ground-based equivalent such as their structure, function, computation and energy limitations. They also have some differences, which can be summarized as follows. Electromagnetic waves like Radio waves do not propagate well underwater due to the high energy absorption of water. As a result, the bit error rates of acoustic links are often high, and losses of connectivity arise [1].

Underwater sensors move with water currents, and AUVs are mobile. Although certain nodes in underwater applications are anchored to the bottom of the ocean, other applications require sensors to be suspended at certain depths or to move freely in the underwater medium.Since underwater hardware is more expensive, underwater sensors are sparsely deployed [2].

UWCNs suffer from the following vulnerabilities. High bit error rates cause packet errors. So, critical security packets can be lost. Wireless underwater channels can be eavesdropped on. Attackers may prevent the informationtransmitted and attempt to modify or drop packets.

4. ATTACKS AND COUNTER MEASURES

Both inter vehicle and sensor-AUV communications can be affected by denial-of-service (DOS) attacks. Next, we summarize typical (DOS) attacks, evaluate their dangers, and indicate possible defences to muffle their effects.

4.1. Jamming

A jamming attack consists of interpose with the physical channel by putting up carriers on the frequencies neighbour nodes use to communicate. When the attacker wedges the communication between a sender and a receiver, and later replays the same message with stale information posing as the sender.

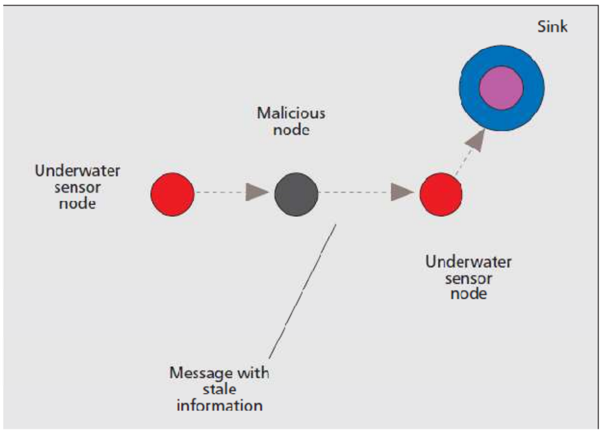

Fig 2: Jamming attack.

4.2. Wormhole Attack

A wormhole is an out-of-band connection created by the antagonist between two physical locations in a network with lower delay and higher bandwidth than ordinary connections. This connection uses fast radio or wired links (Fig. 3) to significantly decrease the propagation delay. 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 refill them into the network [4].

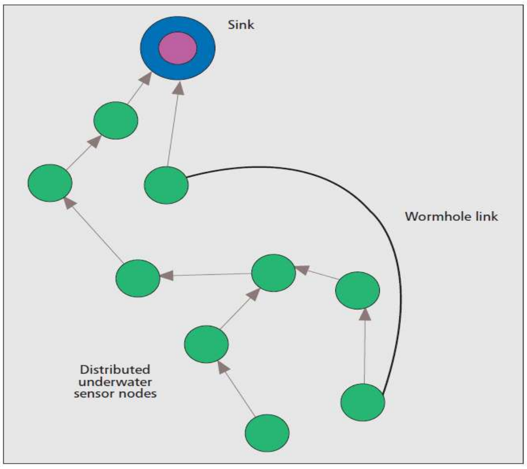

Fig 3. Underwater network with a wormhole link.

4.3. Sinkhole Attack

In a sinkhole attack, a malicious node attempts to allure traffic from a particular area toward it for example, the malicious node can announce a high-quality route by that exchange of routing take place.

4.4. Hello Flood Attack

A node receiving a HELLO packet from a malicious node may interpret that the antagonist is a neighbour this assumption is false, if the antagonist uses high power for transmission. Bidirectional link verification can help protect against this attack, although it is not accurate due to node mobility and the high propagation delays of UWCNs. Authentication is also a possible defence.

4.5. Acknowledgment Spoofing

A malicious node overhearing packets sent to neighbour nodes can use this information to deceive 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 pass into. They cause high bit error rates and loss of connectivity [2]. This way, the routing scheme is manipulated.

4.6. Selective Forwarding

Malicious nodes drop certain messages instead of forwarding them to delay 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.

4.7. Sybil Attack

An attacker with multiple identities can pretend to be in many places at once (Fig. 4). Authentication and position verification are done but it’s pretty tough task as nodes are always mobile.

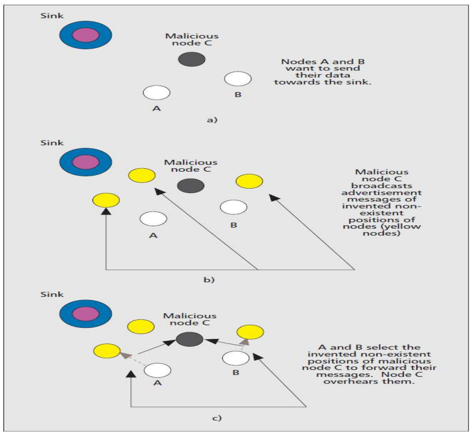
Sink
Malicious node C
Nodes A and B want to send their data towards the sink.
A
B
a)
Sink
Malicious node C
Malicious node C broadcasts advertisement messages of invented non-existent positions of nodes (yellow nodes)
A
B
b)
Sink
Malicious node C
A and B select the invented non-existent positions of malicious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

Fig 4: Sybil attack

5. SECURITY REQUIREMENTS

In UWCNs the following security requirements should be considered.

5.1. Authentication

Authentication is the proof that the data was sent by a legal 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 (renewal) algorithms should be adapted to better address the characteristics of the underwater channel. In [6], a key generation system is proposed that requires only a threshold detector, lightweight computation, and communication costs.

5.2. Confidentiality

Confidentiality means that information is not accessible to unauthorized third parties. Therefore, confidentiality in critical applications such as maritime surveillance (Fig. 5) should be guaranteed.

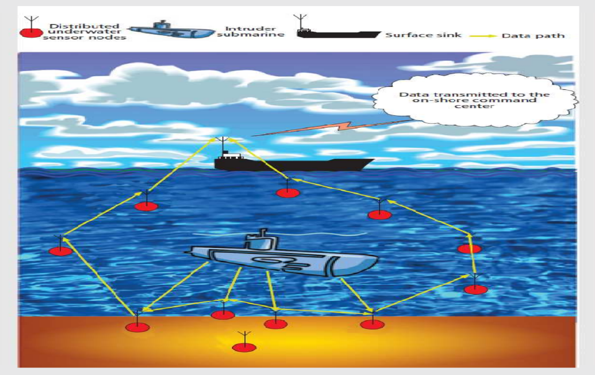
Distributed underwater sensor nodes
Intruder submarine
Surface sink
Data path
Data transmitted to the on-shore command center

Fig 5: Intruder submarine detection

5.3. Integrity

6. CONCLUSION

In this article I have discussed security in UWCNs, underlining the specific characteristics of these networks, possible attacks, and counter measures. Some research issues remain wide open for future investigation.

7. REFERENCES

[1]Mari Carmen Domingo, Barcelona Tech University, "Securing Under Water Wireless Networks", IEEE Wireless Communications, February 2011.

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

[3] W. Wang et al., "Visualization of Wormholes in Underwater Sensor Networks: A Distributed Approach," Int'l. J. Security Net., vol. 3, no. 1, 2008, pp. 10–23.

[4] 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 MARI CARMEN
DOMINGO. Mahgoub, Eds., CRC Press, 2004.

[5] 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.

[6] R. Zhang and Y. Zhang, "Wormhole-Resilient Secure Neighbor Discovery in Underwater Acoustic Networks," Proc. IEEE INFOCOM, 2010.

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

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

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

[10] M. C. Domingo and R. Prior, "Design and Analysis of a GPS-Free Routing Protocol for Underwater Wireless Sensor Networks in Deep Water," Proc. UNWAT, 2007.

It ensures that information has not been altered by any antagonist. Many underwater sensor applications for environmental preservation, such as water quality monitoring [7], rely on the integrity of information.

5.4. 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.