International Journal of Allied Practice, Research and Review
Website: www.ijaprr.com (ISSN 2350-1294)

A Review on Protocols to Optimize Communication Security in Underwater Acoustic Sensor Networks

Vikas Raina, Partha Pratim Bhattacharya and V K Jain
College of Engineering and Technology, Mody University of Science & Technology,
Lakshmangarh, Sikar, Rajasthan, India

Abstract - Acoustic waves are mostly used in underwater wireless communication due to its ability to travel larger distance. The implementation of secure communication is very important to prevent unauthorized access. The security can be implemented in many ways and at various levels. This is a review paper aims to present the emerging topics arising from secure communication in Underwater Acoustic Sensor Networks (UASNs). The intent is to motivate researchers to contribute in this field of research.

Keywords - ***Underwater, Acoustic, Wireless Sensor Network, Security Attacks, Countermeasures and Protocols***

I. Introduction

In recent times, the exploration of underwater environments gains the interest of researchers. The willingness to gather information about the various habitats, resources and events is increasing. The design and implementation of efficient UASNs is very important for effective monitoring. The implementation of wireless communication also requires high level of security to prevent malicious attacks and leakage of critical information.

Section 2 presents literature survey, types of security attacks are elaborated in section 3, protocols to mitigate attacks are illustrated in section 4. Finally, conclusion is presented in section 5.

II. Literature Survey

The detection and mitigation of jamming in UASNs is important to optimize the throughput and reduce delay for real time monitoring [1]. The Denial of Service (DoS) is caused due to jamming making Underwater Wireless Sensor Networks (UWSNs) vulnerable [2]. The security of underwater communication utilizing acoustic waves can be achieved by implementing analog mechanism of network coding [3]. The time synchronization of networks can be attained by the utilization of correlation based security [4]. The detection of targets in conjunction with horizontal and vertical synchronization services is important [5]. It is determined that secure synchronization can be achieved by implementing cluster based mechanisms [6]. The detection and prevention of wormholes for secure communication and neighbor discovery is important [7], [8]. The importance and significance of security and end to end authentication is elaborated in [9] and [10]. Robust key generation scheme is very effective [11] and the localization of nodes using trust scheme enhances the security [12]. The implementation and management of powerful trust nodes utilizing effective mechanisms provides optimum results [13]. In [14], different type of attacks at different layer is elaborated with the explanation of efficient protocols able to mitigate the influence of these security attacks.

III. Security Attacks and Countermeasures at Different Layers

The determination of various attacks and the countermeasures to prevent them at different layers of network architecture of UASNs is important. Table 1 illustrates different security attacks in various layers and suggested its counter measures.

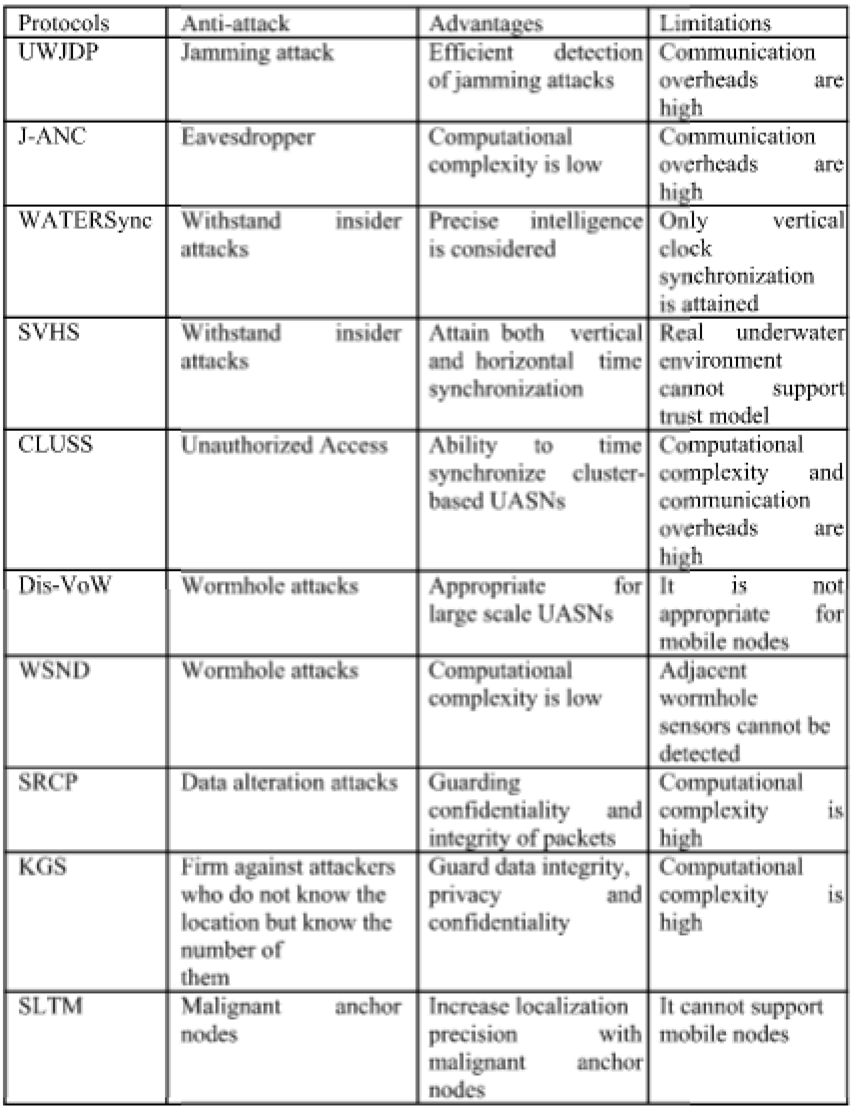
Table 1 Countermeasures to prevent security attacks at different layers [14]

Attacks	Countermeasures	Layer
Flooding	Reduction in the communication range of sensors	Transport
Sinkhole	Implement precise monitoring of traffic, authentication of identity and implementation of multipath routing	Network
Wormhole	Design and implementation of efficient network topologies	
Sybil	Perform authentication of identity of sensor nodes	
Selective Forwarding	Modeling of trust models, reputation and multipath routing	
DoS	Evaluation of consumption of battery power	
Unfairness	Implementation of short packets, Avoiding the use of long packets, reorganize the priority of transmission of data packets	Data link
Exhaustion	Reducing the speed of transmission and retransmission of packets	
Collision	Implementing Forward Error Correction (FEC) code	
Jamming	Implementation of active/sleep schedule, multiple frequencies and different priorities	Physical
Tampering	Model design to prevent physical damage and encryption algorithm to improve security	

IV. Proposed Protocols to Attain Communication Security

There are many protocols proposed to achieve high security in underwater acoustic communication. These are presented in Table 2.

Table 2 Countermeasures to prevent security attacks at different layers [14]



Protocols	Anti-attack	Advantages	Limitations
UWJDP	Jamming attack	Efficient detection of jamming attacks	Communication overheads are high
J-ANC	Eavesdropper	Computational complexity is low	Communication overheads are high
WATERSync	Withstand insider attacks	Precise intelligence is considered	Only vertical clock synchronization is attained
SVHS	Withstand insider attacks	Attain both vertical and horizontal time synchronization	Real underwater environment cannot support trust model
CLUSS	Unauthorized Access	Ability to time synchronize cluster-based UASNs	Computational complexity and communication overheads are high
Dis-VoW	Wormhole attacks	Appropriate for large scale UASNs	It is not appropriate for mobile nodes
WSND	Wormhole attacks	Computational complexity is low	Adjacent wormhole sensors cannot be detected
SRCP	Data alteration attacks	Guarding confidentiality and integrity of packets	Computational complexity is high
KGS	Firm against attackers who do not know the location but know the number of them	Guard data integrity, privacy and confidentiality	Computational complexity is high
SLTM	Malignant anchor nodes	Increase localization precision with malignant anchor nodes	It cannot support mobile nodes

The full form of the abbreviations used for the protocols are Under Water Jamming Detection Protocol (UWJDP) [1], Jamming through Analog Network Coding (J-ANC) [3], Water-quAlity moniToring sEnsor netwoRk Synchronization (WATERSync) [4], Secure Vertical and Horizontal Synchronization (SVHS) [5], CLUster-based Secure Synchronization (CLUSS) [6], Distributed Visualization of Wormhole (Dis-VoW) [7], Wormhole-resilient Secure Neighbor Discovery (WSND) [8], Secure Routing protocol and a set of Cryptographic Primitives (SRCP) [9], Key Generation System (KGS) [11] and Secure Localization algorithm based on a Trust Mechanism (SLTM) [12].

V. Conclusions

This paper has presented the possible attacks and countermeasures to prevent them. The use of effective protocols enhances the security. The security algorithms and mechanisms can be implemented in any layer based on their characteristics and the type of attacks.

Finally, the objective of spreading awareness about the security in UASNs is successfully achieved.

VI. References

1. S. Misra et al., "Jamming in Underwater Sensor Networks: Detection and Mitigation," IET Commun., vol. 6, no. 14, Sep. 2012, pp. 2178-2188.

2. M. Zuba et al., "Vulnerabilities of Underwater Acoustic Networks to Denial-of-Service Jamming Attacks," Security Commun. Net. Feb. 2012, pp. 1-11.

3. H. Kulhandjian, T. Melodia, and D. Koutsonikolas, "Securing Underwater Acoustic Communications through Analog Network Coding," Proc. SECON, June 2014, pp. 1-9.

4. F. Hu, S. Wilson and Y. Xiao, "Correlation-Based Security in Time Synchronization of Sensor Networks," Proc. WCMC. Mar. 2008, pp. 2525-2530.

5. F. Hu et al., "Vertical and Horizontal Synchronization Services with Outlier Detection in Underwater Acoustic Networks," Wireless Commun. Mob. Com., vol. 8, no. 9, Nov. 2008, pp. 1165-1181.

6. M. Xu et al., "A Cluster-Based Secure Synchronization Protocol for Underwater Wireless Sensor Networks," Int. J. Distrib. Sensor Networks, vol. 2014, Apr. 2014, pp. 1-13.

7. W. Wang et al., "Visualisation of Wormholes in Underwater Sensor Networks: A Distributed Approach," Int'l. J. Security Net. vol. 3, no. 1, Jan. 2008, pp. 10-23.

8. R. Zhang and Y. Zhang, "Wormhole-Resilient Secure Neighbor Discovery in Underwater Acoustic Networks," Proc. 29th IEEE INFOCOM., Mar. 2010, pp. 2633-2641.

9. G. Dini and A. L. Duca, "A Secure Communication Suite for Underwater Acoustic Sensor Networks," Sensors Basel, vol. 12, no. 11, Nov. 2012, pp. 15,133-15,158.

10. E. Souza et al., "End-to-End Authentication in Under Water Sensor Networks," Proc. ISCC., July 2013, pp. 299-304.

11. Y. Liu, J. Jing, and J. Yang, "Secure Underwater Acoustic Communication Based on a Robust Key Generation Scheme," Proc. 9th ICSP, Oct. 2008, pp. 1838-1841.

12. Y. Zhang et al., "Node Secure Localization Algorithm in Underwater Sensor Network Based on Trust Mechanism," J. Computer Applications, vol. 33, no. 5, May 2013, pp. 1208-1211.

13. G. Han et al., "Management and Applications of Trust in Wireless Sensor Networks: A Survey," J. Comp. Sys. Sci., vol. 80, no. 3, May. 2014, pp. 602-617.

14. **G. Han et al., "Secure Communication for Underwater Acoustic Sensor Networks," IEEE Communications Magazine, vol. 53, no. 8, August 2015, pp. 54-60.**