Authentication in Underwater Wireless Sensor Networks

An Annotated Bibliography

M. Phillip Lowney Jr.
University of Massachusetts Dartmouth

September 9, 2017

References

[1] I. F. Akyildiz, D. Pompili, and T. Melodia, "Underwater acoustic sensor networks: research challenges," *Ad Hoc Networks*, vol. 3, no. 3, pp. 257–279, May 2005. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1570870505000168

[2] I. F. Akyildiz, P. Wang, and S.-C. Lin, "SoftWater: Software-defined networking for next-generation underwater communication systems," *Ad Hoc Networks*, vol. 46, pp. 1–11, Aug. 2016. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1570870516300579

> The authors explain the current state-of-the-art for underwater communication systems, and why hardware-based network architecture is severly limiting and inflexible. Software-defined networking (SDN) is then introduced as the "next-generation networking paradigm." A SDN underwater communication architecture called SoftWater is proposed, and it is explained in detail why it will be a major improvement upon the current state of underwater networking. Several important features are covered, including adaptivity, infrastructure-as-a-service, optimal throughput, convergence of heterogeneous networks, and high energy efficiency. The authors draw differences between their networking scheme and the recently introduced software-defined

acoustic modems, noting that they "lack the capability to enable the programmable network layer functions," however the adaptability of the SoftWater architecture allows for them to be integrated into it's programmable data plane. The design of the architecture is covered thoroughly, as well as it's management tools. The final section proposes a full networking solution using SoftWater, and explains why it is superior to any scheme available to date. Research challenges are then summarized. The authors all have Ph. D. Degrees, and have written several relavent papers; many of which are used as self-references.

[3] C.-F. Cheng and L.-H. Li, "Data gathering problem with the data importance consideration in Underwater Wireless Sensor Networks," *Journal of Network and Computer Applications*, vol. 78, pp. 300–312, Jan. 2017. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1084804516302399

Two fundamental methods of gathering data are explained: Multi-hop transmission, and Autonomous Underwater Vehicles (AUVs). A thorough explanation of both methods, including advantages and disadvantages, are given, as well as a review of the most relevant works of research in both methods. The authors propose an algorithm which combines both methods in a way which will take advantage of the speed of multi-hop transmission, and the efficiency of AUVs simultaneously. The article explains how the importance level of data is measured and determined, and then thoroughly describes the proposed algorithm. In the results section, it can be seen that out of several similar algorithms, the proposed algorithm has the best network lifetime. The performance of the throughput of data, the effect of network stratification, and the effect of collection region size are also analyzed.

[4] M. C. Domingo, "Securing underwater wireless communication networks," *IEEE Wireless Communications*, vol. 18, no. 1, pp. 22–28, Feb. 2011.

The article starts with a concise explanation of characteristics that make Underwater wireless communication networks (UWCNs) prone to attacks and failures. The subsequent sec-

tions detail known attacks, giving thorough descriptions and using clear explanations and minimalistic graphics. Proposed solutions to each attack are listed, as well as possible fallacies within the proposed schemes. The author then details the security requirements of UWCNs, and lists research challenges and areas which still need to be addressed. Quick and powerful authentication and encryption is continually listed as a requirement that is needed but not quite fulfilled. The author has a Ph.D. in telematics engineering, and has published several papers in mobile ad-hoc networks, wireless sensor networks, heterogeneous networks and distributed algorithms.

[5] X. Du, C. Peng, and K. Li, "A secure routing scheme for underwater acoustic networks," *International Journal of Distributed Sensor Networks*, vol. 13, no. 6, p. 1550147717713643, June 2017. [Online]. Available: http://dx.doi.org/10.1177/1550147717713643

[6] S. Farrell and C. Adams, "Internet X.509 Public Key Infrastructure Certificate Management Protocols." [Online]. Available: https://tools.ietf.org/html/rfc2510

[7] D. Galindo, R. Roman, and J. Lopez, "A Killer Application for Pairings: Authenticated Key Establishment in Underwater Wireless Sensor Networks," in *Proceedings of the 7th International Conference on Cryptology and Network Security*, vol. 5339. NICS Lab, 2008, pp. 120–132. [Online]. Available: https://www.nics.uma.es/pub/papers/Galindo2008aa.pdf

This article looks into authentication and key establishment with the primary concern being saving in communication. As a result, it is argued that symmetric key authentication is a better choice than public key infrastructure. Non-interactive identity-based key agreement (NIKE) is explained, giving an example which uses identity-based cryptography (IBC), comparing it to elliptic curve authenticated key exchange, which employs public key cryptography. In analysis, IBC is found to exchange far less bits than PKC, leading to a low-bandwidth solution. The article then looks into a comparison of NIKE with symmetric key-based key-management systems (KMS). Symmetric KMS is found to have multiple security flaws,

which are backed up with examples of how adversaries may be able to breach the authenticity of communication.

[8] G. Han, J. Jiang, L. Shu, and M. Guizani, "An Attack-Resistant Trust Model Based on Multidimensional Trust Metrics in Underwater Acoustic Sensor Network," *IEEE Transactions on Mobile Computing*, vol. 14, no. 12, pp. 2447–2459, Dec. 2015. [Online]. Available: http://ieeexplore.ieee.org.libproxy.umassd.edu/document/7038144/

[9] G. Han, J. Jiang, N. Sun, and L. Shu, "Secure communication for underwater acoustic sensor networks," *IEEE Comunications Magazine*, vol. 53, no. 8, pp. 54 – 60, Aug. 2015. [Online]. Available: http://ieeexplore.ieee.org.libproxy.umassd.edu/abstract/document/7180508/

The authors present a survey on the state of the art for security measures in UWSNs. At each layer of the network model, attacks paired with their respective countermeasures are described. Much of the findings are presented in easy to read tables.

[10] J. Jiang, G. Han, C. Zhu, S. Chan, and J. J. P. C. Rodrigues, "A Trust Cloud Model for Underwater Wireless Sensor Networks," *IEEE Communications Magazine*, vol. 55, no. 3, pp. 110–116, Mar. 2017.

The authors introduce trust management as an intrusion-tolerant solution for UWSNs. An overview of trust management is given as well as a brief description of several trust management mechanisms. Cloud-based trust is used in their proposed scheme, called Trust-Cloud Model (TCM). It is described as a network model and a cloud model, with various methods of trust evidence collection to create a scheme which allows for accurate, transferable trust for each node in the network. In the evaluation of the simulations, TCM outperforms similar schemes in comparisons of malicious node detections and successful data transmission.

[11] C. Lal, R. Petroccia, K. Pelekanakis, M. Conti, and J. Alves, "Toward the Development of Secure Underwater Acoustic Networks," *IEEE Journal of Oceanic Engineering*, vol. PP, no. 99, pp. 1–13, July 2017. [Online]. Available: http://ieeexplore.ieee.org.libproxy.umassd.edu/document/7970108/

The article explores the attack vector on all of the layers of the network model, providing relavent proposed solutions to each type of attack. It is drawn that there is no fully accepted security protocol for underwater acoustic networks. Requirements for a more secure underwater network are described in great detail, with explanations of what each concept is, why it is relavant, and what it entails. The remainder of the article describes a network architecture with unique security features at each layer, all of which consider the characteristics of underwater communication. It is evaluated using metrics of fault-tolerance, overhead, and security.

[12] Y. Liu, J. Jing, and J. Yang, "Secure underwater acoustic communication based on a robust key generation scheme," in *ICSP2008*, vol. 9. Beijing, China: IEEE, Oct. 2008, pp. 1838–1841. [Online]. Available: http://ieeexplore.ieee.org.libproxy.umassd.edu/abstract/document/4697498/

The article points out that traditional key generation is unfeasible underwater due to characteristics of the acoustic channel. Rather, the authors use the unique characteristics of the channel as well as some well-known properties in a key generation scheme to create a secure, unique key between two nodes in a network.

[13] T. Melodia, H. Kulhandjian, L.-C. Kuo, and E. Demirors, "Advances in underwater acoustic networking," *Mobile Ad Hoc Networking: Cutting Edge Directions*, vol. 852, 2013. [Online]. Available: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.307.5052rep=rep1type=pdf

[14] C. Neuman, S. Hartman, T. Yu, and K. Raeburn, "The Kerberos Network Authentication Service (V5)." [Online]. Available: https://tools.ietf.org/html/rfc4120

[15] M. Sharif-Yazd, M. R. Khosravi, and M. K. Moghimi, "A Survey on Underwater Acoustic Sensor Networks: Perspectives on Protocol Design for Signaling, MAC and Routing," *Journal of Computer and Communications*, vol. 05, no. 05, pp. 12–23, Mar. 2017. [Online]. Available: http://www.scirp.org/journal/PaperDownload.aspx?DOI=10.4236/jcc.2017.55002

A brief overview of the challenges and caveats of UWSNs are presented, compared, as usual, to surface WSNs. A propogation model is defined, presenting equations which represent

acoustic channel attenuation, underwater environment noise, signal to noise ratio, and underwater propogation velocity. The next section reviews challenges faced at each layer of the open system interconnection model. Table 3 on page 16 lists challenges faced in the physical layer, as well as reasons and effects. MAC protocols are discussed as an important concern of the link layer, as well as advantages and disadvantages of contention-based techniques versus channelization techniques. At the network layer, routing protocols and topologies are discussed. Flooding and multipath routing techniques are emphasized as the most widely used for UWSNs. Not much information is presented on the transport layer, besides that UDP has a lower processing delay. Topology control problem of wireless networks is suggested as a research topic. Application layer issues are presented as a very hot topic for current research, especially when combining UWSNs with other new topics such as internet of things, big data, and software defined networks. Multiple relevant sources are given for all of the above topics, making this paper an invaluable research companion for the state of the art in UWSNs.

[16] E. Souza, H. C. Wong, I. Cunha, L. F. M. Vieira, and L. B. Oliveira, "End-to-end authentication in Under-Water Sensor Networks," in *2013 IEEE Symposium on Computers and Communications (ISCC)*, July 2013, pp. 000 299–000 304.

The authors examine digital signature schemes, and how they perform in UWSNs, an authentication method which had not been previously worked on in the underwater domain. Elliptic Curve Cryptography schemes are used for their quick and efficient generation methods. Message Authentication Codes are used, rather than link-layer authentication because of signature length. A model for determining authentication cost in terms of energy is given, and in performance evaluation the ratio between transmission and signing costs is considered. It is concluded that short and aggregate signature schemes have better performance in UWSNs.

[17] W. Stallings, *Data and computer communications*, 8th ed. Upper Saddle River, N.J: Pearson/Prentice Hall, 2007.

[18] ——, *Cryptography and network security: principles and practice*, seventh edition ed. Boston: Pearson, 2014.

[19] P. Xie, J.-H. Cui, and L. Lao, "VBF: vector-based forwarding protocol for underwater sensor networks," *Networking 2006. Networking technologies, services, and protocols; performance of computer and communication networks; mobile and wireless communications systems*, pp. 1216–1221, 2006. [Online]. Available: http://www.springerlink.com/index/M371255X96GK9767.pdf

This is the specification for the vector-based forwarding (VBF) routing protocol which is now widely accepted as a standard for underwater wireless sensor networks (UWSN). There is a light introduction which draws similarities and differences between UWSNs and terrestrial sensor networks, explains challenges unique to UWSNs, and clearly states the problem that is being solved by their contributions. The next section describes the operation of VBF as an overview which includes the contents of each packet, and the methods of routing initiation by query packets. The subsequent section proposes an algorithm that uses self-adaptation to save energy in a dense network. A mathematical model for node desirability with respect to the routing vector is defined and used in the explanation of the self-adaptation algorithm. The remainder of the paper evaluates the performance of VBF in terms of success rate, energy consumption, and average delay, under scenarios which vary node mobility speed and number of nodes in the network. The results show that "in VBF, node speed has little impact" on the three metrics quantified for this evaluation, and "[the experiment] demonstrates that VBF could handle node mobility very effectively." There is another technical report by the authors which gives results of simulations showing the impact of more specific aspects of the protocol, given in the paper as [8]. The conclusion remarks on reasons that cause VBF to stand out amongst other geographic routing protocols, namely that it does not need the exact positioning of nodes to be available. Two of the authors are from the University of Connecticut, an institution which is highly active in the field of UWSNs, and the other from University of California, Los Angeles. The authors have

made several invaluable contributions to UWSNs as well as computer networks in general.

[20] M. Xu, G. Liu, D. Zhu, and H. Wu, "A Cluster-Based Secure Synchronization Protocol for Underwater Wireless Sensor Networks," *International Journal of Distributed Sensor Networks*, vol. 10, no. 4, p. 398610, Apr. 2014. [Online]. Available: http://journals.sagepub.com/doi/10.1155/2014/398610