A Secure Communication Suite for Cluster-based Underwater Surveillance Networks

Md. Rafiqul Islam*, Saiful Azad*, Md. Monzur Morshed†

*Department of Computer Science, American International University - Bangladesh, Banani, Dhaka, Bangladesh
†TigerHATS, Dhaka, Bangladesh

{rafiqulislam,sazadm684}@aiub.edu, monzur@tigerhats.org

***Abstract*—Surveilling the water territory of a country by installing an Underwater Surveillance Network (USN) is one of the prominent applications developed for underwater communication. The primary responsibility of a USN is to detect trespassers within the premises and to notify the activities to the responsible authority for further actions. Alike any surveillance network, a USN also possesses several security threats and may undergo several passive and/or active attacks. In this paper, we propose a noble secure communication suite which is resistible against most kind of known attacks. Our propose protocol aimed at gaining confidentiality, integrity and authenticity of the messages being exchanged within the cluster while taking into the consideration of the peculiarities of the underwater communication. Moreover, since our proposed scheme is designed for a cluster-based USN where routing layer activities are not eminent, it is embedded within a media access control (MAC) protocol.**

***Index Terms*—Underwater surveillance sensor networks, Media access control, Public key, Private key, Cluster, Hash algorithm, Authentication key.**

I. Introduction

In recent years, Underwater Acoustic Communication is gaining immense attention from the militaries, industries and researchers due to its many potential applications and unlimited possibilities. Consequently, many applications are already developed for such network architecture and many of them are yet to be discovered. Surveilling the water territory of a country via USN where underwater sensors are deployed within the area of interest is considered as one of the prominent among the proposed applications. Consequently, several USNs are proposed in different literatures [1]–[3]. In [1], [2], a USN is proposed which is comprising of bottom mounted fixed sensor nodes. All the nodes involved in the surveillance are capable of detecting the movement of any intruder within the surveilling area and informing the activities to a bouy or a ship. In [3], a next generation Coastal Patrol and Surveillance Network is proposed where Automatic Underwater Vehicles (AUVs) are installed to patrol an area of interest. When an AUV detects an intruder within the area, it starts following it and endeavors to inform the activities to a shore based control center employing delay-tolerant routing technique. Latter type of USN is not likely utilizing the current AUVs available in operation. Therefore, the earlier USN architecture is considered in this paper which is illustrated in Section II in details.

Alike any surveillance network in any network architecture, USN also undergo several security threats [4]. For instance, let us consider that a ship or a submarine of an adversary which is equipped with an acoustic modem eavesdrops to learn the messages being exchanged within a cluster. Sometime later, it may employ the knowledge which is acquired from eavesdropping to alter the messages and/or to inject fake messages within the cluster. It may also falsify its identity and can enter into the premises. In these circumstances, it is necessary to take security measures more sharply to prevent any attack from the adversaries. There are a couple of approaches which are proposed for terrestrial networks to combat this kind of threats. However, they are not suitable for USNs because of the differences between both the architectures.

Underwater communication is more challenging than terrestrial communication since communication is performed through acoustic waves which experience longer propagation delays and higher bit error rate than radio waves in terrestrial networks [5], [6]. Moreover, acoustic communication is more energy hungry because of its nature [7]. Consequently, underwater sensors must not dissipate energy in transmitting and receiving unnecessary packets. These aspects must be taken into consideration while designing a secure communication suite for a USN. Though a couple of USNs are proposed in the literatures, a few among them are designed considering the security aspects of USNs. In [8], [9], authors proposed and tested a secure communication suite with the objectives to preserving the confidentiality and the integrity of the messages which are exchanged. Nevertheless, since keys are not exchanged securely, they may still experience spoofing attack.

In this paper, we propose a secure communication suite which is resistible against most kind of known attacks. Our propose protocol aimed at gaining confidentiality, integrity and authenticity of the messages being exchanged within the cluster while taking into the consideration of the peculiarities of the underwater communication. Moreover, since our proposed scheme is designed for a cluster-based USN where routing layer activities are not eminent, it is embedded within a media access control (MAC) protocol.

The rest of the paper is organized as follows. In Section II, we illustrate the system model considered while designing the proposed suite. Our proposed secure communication suite is demonstrated in Section III. Discussions on the proposed

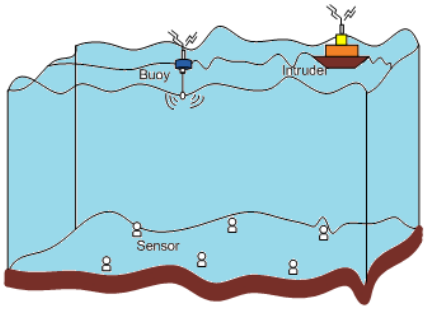

Figure 1. A Cluster-based Underwater Surveillance Network architecture.

scheme is given in Section IV and this paper ends with a concluding remarks in Section V.

II. System Model

A USN is subjected to several threats and possible attacks as it is demonstrated in Section I which must be taken care of for secure communication. The secure communication suite which is proposed in this paper is designed for a cluster-based single-hop USN where all the cluster-members are bottom mounted and a cluster-master is installed at the surface of the water. Every cluster is headed by the cluster-master. A cluster-based USN architecture is depicted in Fig. 1. Alike [8], every node in the network is equipped with ample number of sensors to detect the activities of any intruder which enters into the premises of that node and with an acoustic modem to support communication. Moreover, every cluster-member is considered to have computational resources comparable to those of a low configured computer (e.g., a PC/104 embedded computer [10]). Therefore, computationally expensive cryptographic algorithms, like AES [8], DES/3DES [11], RSA [12], [13], CMAC [11], etc. can be installed in underwater sensors, whereas, they are unlikely for terrestrial wireless sensor networks.

Since the area to be patrolled is large, a cluster-member would be able to inspect only a portion of the surveillance area. Multiple sensors need to be deployed to cover up the entire area of interest. Again, if a single cluster is not adequate to cover up the entire surveillance area, multiple clusters can be deployed. Each cluster-member reports the sensed data to the cluster-master which is connected to a shore-based control center via wireless link or via satellite communication. Therefore, our intentness in this paper is to secure the communication between the cluster-members and the cluster-master or vice versa. Any terrestrial wireless secure communication suite can be employed to secure the communication between the cluster-masters and the shore-based control center which is out of the scope of this paper.

III. The Secure Communication Suite

Cryptography is the primary means to support private communication in the public world. The key goals of any secure communication suite is to attain confidentiality, integrity and authentication and our proposed suite is no exception. Since we designed our suite for a cluster-based network which is described in Section II, we incorporate it with a MAC protocol[1]. It has been argued in different literatures that random access MAC protocols (e.g., ALOHA [14], [15], CSMA-ALOHA [16]) attain higher throughput performance than hand-shake based MAC protocols (e.g., MACA-MN [17], DACAP [18]) in underwater network architecture. Consequently, we have chosen a random access MAC protocol, namely ALOHA to incorporate our secure communication suite. Moreover, random access protocols are also preferred in USNs because of their timely message transmission capability. Our proposed also can be embedded within a routing protocol after slight modification. The proposed secure communication suite is detailed in following two Subsections.

A. Authentication Key Exchange

Before the nodes are deployed in a USN, certain information is pre-stored according to the responsibilities of the nodes. For instance, a cluster-member must store a private-key of its own and a public-key of the cluster-master. Conversely, a cluster-master must store a private-key of its own and a secret message which is utilized in authentication key exchange procedure.

After the installation of the nodes in a USN, a cluster-master generate an *Authentication Key Required (AKR)* message which includes the identification of the cluster-master, ID_{cm} and the afore mentioned secret message, S_M. Then *AKR* message is encrypted employing the private-key of the cluster-master and the cipher, C_{ain} is generated as,

$$M_{akr} = (ID_{cm}||S_M) \tag{1}$$

$$C_{akr} = E\left(K_{(pr,cm)}, M_{akr}\right) \tag{2}$$

where $K_{(pr,cm)}$ is the private-key of the cluster-master. This message is encapsulated afterward by appending a header and a trailer to form a frame by ALOHA protocol and then broadcasts in the network. After receiving the frame, encrypted message is decrypted and M_{akr} is unearthed as follows,

$$M_{akr} = D\left(K_{(pb,cm)}, C_{akr}\right) \tag{3}$$

where $K_{(pb,cm)}$ is the public-key of the cluster-master. If a new member, i wishes to join the cluster, it replays with an *Authentication Key Transfer (AKT)* message where it echoes the S_M received from the cluster-master. It also includes its public-key, $K_{(pb,i)}$, and an authentication key of i, $K_{(auth,i)}$. The *AKT* message is then encrypted using the public-key of the cluster-master and a cipher, C_{akt} is produced as,

$$M_{akt} = \left(S_M||K_{(pb,i)}||K_{(auth,i)}\right) \tag{4}$$

$$C_{akt} = E\left(K_{(pb,cm)}, M_{akt}\right) \tag{5}$$

$K_{(auth,i)}$ in Eq. 4 is produced using one-way hash function as follows.

$$K_{(auth,i)} = H\left(ID_i, K_{(pr,i)}, NP\right) \tag{6}$$

[1]In a cluster-based network, since all the nodes are within the communication range of each other or within the communication range of the cluster-master, routing layer activities may not eminent which inspires us to embed our proposed scheme within a MAC protocol.

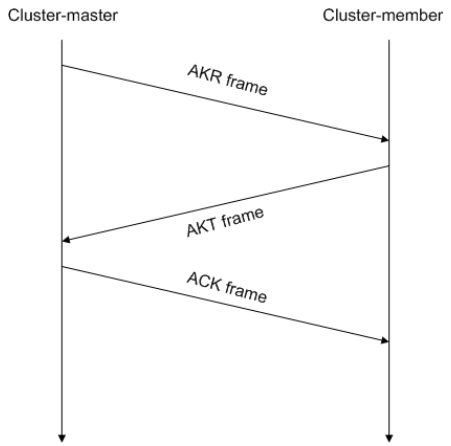

Figure 2. Message exchange scheme to acquire the authentication key of every cluster-member by.the cluster-master.

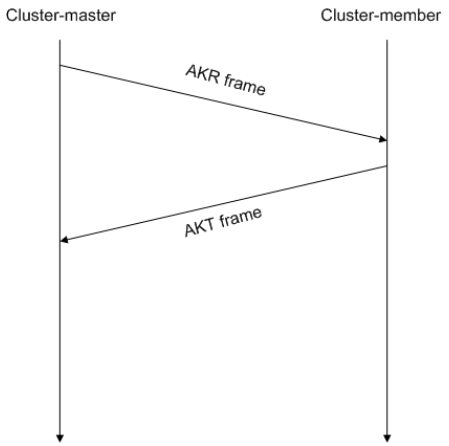

Figure 3. Message exchange scheme to notify the availability of a cluster-member.

where ID_i is the identification of the member i, $K_{(pr,i)}$ is the private-key of i and NP is the network parameter. Alike, the *AKR* message, the *AKT* message is also encapsulated by appending a header and a trailer to create a frame which is then transferred after a random waiting time to avoid the collisions. After receiving the frame, the cluster-master retrieves M_{akt} using its private-key as follows,

$$M_{akt} = D\left(K_{(pb,cm)}, C_{akt}\right) \tag{7}$$

Afterward, the cluster-master stores $K_{(pb,i)}$ in a public-key table and $K_{(auth,i)}$ in an authentication key table with other related information for future reference. As it is mentioned before, underwater channels experience higher bit error rate, therefore, an *ACK* message is transmitted to notify the sender about the reception of the *AKT* message. If the *AKT* message sender fails to receive that *ACK* message, after a random waiting time it retransmits the message again. An *ACK* message will be only transmitted to confirm the membership of a novice group member and it is avoided in all other cases to save energy. Moreover, surveillance messages must be delivered in timely fashion and reliable delivery is not the concern. An *ACK* message is also encrypted using the public-key of the *AKT* message sender. Fig. 2, illustrates the message exchange scheme between a new cluster-member and a cluster-master to acquire the authentication key and the public-key of the member.

When a cluster-member which is already a member of the cluster receives an *AKR* message, it also replies the message to notify its availability to the cluster-master. However, all the fields (e.g., S_M, $K_{(pb,i)}$ and $K_{(auth,i)}$) are filled with zeros. A flag in ALOHA header is set to notify the cluster-master between the presence and the absence of information and hence, sender's identity (whether, it is a new member or it is an old member). This message exchange scheme is depicted in Fig. 3. Missing of couple of consecutive *AKT* messages let the cluster-master in presuming that the node is not currently in operation and information of that member is erased from the public-key table as well as from the authentication key table.

B. Data Exchange

Whenever a node detects an intruder within its premises, it generates a *detection* message to notify the cluster-master regarding the detection. A *detection* message includes time of the detection with other related information. From the generated message, a hash code, h_k is calculated as follows,

$$h_k = H\left(K_{(auth,i)}||M_d\right) \tag{8}$$

where $K_{(auth,i)}$ is the authentication key of i and M_d is the *detection* message. Afterward, h_k is affixed with the original message and a cipher, C_d is produced as follows,

$$C_d = E\left(K_{(pb,cm)}, M_d||h_k\right) \tag{9}$$

where $K_{(pb,cm)}$ is the public key of the cluster-master. This message is then appended with a header and trailer and formed a frame and injected in the network. A node keep transmitting *detection* messages as long as it can detect the intruder within its premises. On the other hand, when cluster-master receives a *detection* message, it unwraps the message and decrypts it as below,

$$(M_d||h_k) = D(K_{(pb,cm)}, C_d) \tag{10}$$

After that the cluster-master calculates another hash code, h'_k employing Eq. 8 and using M_d and $K_{(auth,i)}$ which is fetched from the authentication key table. A scenario of

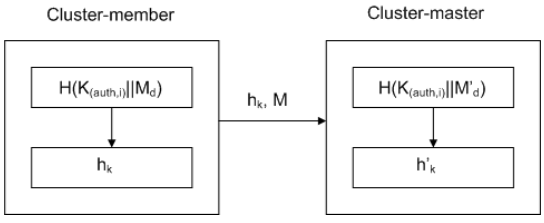

Figure 4. A scenario of integrity checking by employing hashing function and by generating hash code.

integrity checking by employing hashing function and by generating hash code is given in Fig. 4. If both hash codes are analogous, i.e., $h'_k = h_k$, the cluster-master can presume that the message is received unaltered. Conversely, it is considered that the message has been altered and dropped immediately. From the received message, a cluster-master realizes the activities of an intruder and it immediately notifies the activities to the shore-based control center for taking further actions.

IV. Discussions

The motivation behind designing this proposed suite is to attain secure communication between a cluster-master and all the cluster-members of a USN architecture. A communication can be claimed secure if it can preserve confidentiality of the message, conserve integrity of that message and confirm that the message has been generated and sent from an authentic node. We designed our communication suite keeping these objectives in mind. Moreover, the peculiarities of the underwater channel is also considered. For instance, our proposed scheme is incorporated with a random access MAC protocol, namely ALOHA because of its superior performance in underwater scenario over most of the hand-shake based MAC protocols which are usually preferred in terrestrial wireless networks. Moreover, to handle higher bit-error rate of underwater channels, *ACK* messages are incorporate in the ALOHA protocol where necessary.

Secure communication without authentication is unlikely [19]. Therefore, we incorporate an authentication procedure in our proposed suite. Every cluster-member must originates $K_{(auth,i)}$ and share it with its cluster-master. After receiving $K_{(auth,i)}$, the cluster-master stores it in an authentication key table with other related information. This key is utilized by a node in a USN to generate h_k which is affixed with a message to attain following advantages: 1) it assures the authentication of the sender, and 2) it also checks the integrity of the message.

When h_k is generated using Eq. 6 by a cluster-member, it exploits $K_{(auth,i)}$ with other related information. As $K_{(auth,i)}$ is involved while generating h_k, an analogous h_k could be possible to regenerate only if someone know $K_{(auth,i)}$. After receiving a *detection* message, whenever a cluster-master could reproduce an analogous h_k utilizing the $K_{(auth,i)}$ of the sender, it can presume that the message has been transferred from an authentic cluster-member.

The similar h_k which ensures the authentication of a cluster-member also ensures the integrity of the message since M_d is involved in generation of h_k. Consequently, if the message is altered by any adversary, a cluster-master would not able to regenerate an analogous h_k which is an evidence that the message has been altered before delivery. The cluster-master would be able to regenerate h_k if and only if when the message is not altered and hence, integrity of the message is conserved using h_k.

Since only the encrypted messages are exchanged between a cluster-master and all the cluster-members, it can be claimed that the confidentiality of the message is preserved. An adversary would be able to decrypt the message only when the public-key and the private-key are compromised. This is pretty unlikely in this scheme since almost all the keys are pre-stored before a sensor is installed in the USN network except the public-key of a cluster-member; which is again transferred through an encrypted message described in Subsection III-A in details.

Aforementioned, different techniques are combined together in our proposed scheme to secure the communication of a USN. Moreover, incorporating all these within the ALOHA protocol completes the suite and make it compatible for underwater surveillance activities via USNs.

V. Conclusions

In this paper, we propose a noble secure communication suite for underwater surveillance network which is resistible against most kind of known attacks. Our proposed scheme is capable in preserving the confidentiality, conserving the integrity and assuring the authenticity of the messages while exchange within a cluster. The peculiarities of the underwater communication channel is also considered while the suite is designed. Since the USN considered in this paper is a cluster-based USN where routing layer activities are not eminent, it is embedded in ALOHA protocol. The proposed secure communication suite seals the loopholes exist in other available suites designed for USNs.

References

[1] M. Goetz, S. Azad, P. Casari, I. Nissen, and M. Zorzi, "Jamming-resistant multi-path routing for reliable intruder detection in underwater networks," in *Proc. of ACM WUWNet*, Seattle, Washington, USA, Dec. 2011.

[2] E. H. Cherkaoui, S. Azad, P. Casari, L. Toni, N. Agoulmine, and Z. M, "Packet error recovery in multipath underwater networks using reed-solomon codes," in *Proc. of MTS/IEEE Oceans*, Virginia, USA, 2012.

[3] S. Azad, P. Casari, and M. Zorzi, "Coastal patrol and surveillance networks using AUVs and delay-tolerant networking," in *Proc. of MTS/IEEE OCEANS*, Yeosu, South Korea, May 2012.

[4] Y. Cong, G. Yang, Z. Wei, and W. Zhou, "Security in underwater sensor network," in *Proc. of IEEE International Symposium on Computers and Mobile Computing*, Shenzen, China, 2010.

[5] I. Akyildiz, D. Pompili, and T. Melodia, "Underwater acoustic sensor networks: research challenges," *Elsevier's Ad Hoc Networks*, vol. 3, no. 3, 2005.

[6] M. Chitre, S. Shahabudeen, and M. Stojanovic, "Underwater acoustic communications and networking: Recent advances and future challenges," *Marine Tech. Soc. Journal*, vol. 42, no. 1, pp. 103–116, spring 2008.

[7] A. Radosevic and J. G. Proakis and M. Stojanovic, "Statistical Characterization and Capacity of Shallow Water Acoustic Channels," in *Proc. of IEEE OCEANS*, Bremen, May 2009.

[8] G. Dini and A. L. Duca, "A secure communication suite for underwater acoustic sensor networks," *SENSORS*, no. 12, pp. 15 133–15 158, 2012.

[9] ——, "Seflood: A secure network discovery protocol for underwater acoustic networks," in *Proc. of IEEE Symposium on Computers and Communications*, Jul. 2011, pp. 636–638.

[10] "Pc/104 consortium." [Online]. Available: http://www.pc104.org/

[11] Y. P. Kim, J. An, S. H. Park, O. Yi, J. Kwon, and C.-H. Kim, "Data encryption and authentication mechanism based on block cipher mode for underwater acoustic sensor networks," in *Proc. of International Conference on Information Science and Technology*, Shanghai, China, 2012.

[12] W. Stallings, *Cryptography and Network Security*, 4th ed. Pearson, 2006.

[13] C. Kaufman, R. Perlman, and M. Speciner, *Network Security: Private Communication in a Public World*. New Delhi, India: Perentice-Hall of India, 2007.

[14] F. Guerra, P. Casari, and M. Zorzi, "MAC protocols for monitoring and event detection in underwater networks employing a FH-BFSK physical layer," in *Proc. of IACM UAM*, Nafplion, Greece, Jun. 2009.

[15] ——, "World Ocean Simulation System (WOSS): a simulation tool for underwater networks with realistic propagation modeling," in *Proc. of ACM WUWNet 2009*, Berkeley, CA, Nov. 2009.

[16] S. Azad, P. Casari, C. Petrioli, R. Petroccia, and M. Zorzi, "On the impact of the environment on mac and routing in shallow water scenarios," in *Proc. of IEEE/OES OCEANS*, Santander, Spain, 2011.

[17] N. Chirdchoo, W.-S. Soh, and K. C. Chua, "MACA-MN: A MACA-based MAC protocol for underwater acoustic networks with packet train for multiple neighbors," in *Proc. of IEEE VTC Spring*, Singapore, May 2008.

[18] B. Peleato and M. Stojanovic, "Distance aware collision avoidance protocol for ad hoc underwater acoustic sensor networks," *IEEE Commun. Lett.*, vol. 11, no. 12, pp. 1025–1027, Dec. 2007.

[19] A. J. Menzes, P. C. V. Oorschot, and S. A. Vanstone, *Handbook of Applied Cryptography*. Boca Raton, FL, USA: CRC press, 1996.