Impact of Minimizing the Eavesdropping Risks on Lifetime of Underwater Acoustic Sensor Networks

Alper Ozmen*, Huseyin Ugur Yildiz†, and Bulent Tavli*

*TOBB University of Economics and Technology, 06560, Ankara, Turkey, e-mail: {a.ozmen,btavli}@etu.edu.tr
†TED University, 06420, Ankara, Turkey, e-mail: hugur.yildiz@tedu.edu.tr

***Abstract*—Underwater Acoustic Sensor Networks (UASNs) are often deployed in hostile environments, and they face many security threats. Moreover, due to the harsh characteristics of the underwater environment, UASNs are vulnerable to malicious attacks. One of the most dangerous security threats is the eavesdropping attack, where an adversary silently collects the information exchanged between the sensor nodes. Although careful assignment of transmission power levels and optimization of data flow paths help alleviate the extent of eavesdropping attacks, the network lifetime can be negatively affected since routing could be established using sub-optimal paths in terms of energy efficiency. In this work, two optimization models are proposed where the first model minimizes the potential eavesdropping risks in the network while the second model maximizes the network lifetime under a certain level of an eavesdropping risk. The results show that network lifetimes obtained when the eavesdropping risks are minimized significantly shorter than the network lifetimes obtained without considering any eavesdropping risks. Furthermore, as the countermeasures against the eavesdropping risks are relaxed, UASN lifetime is shown to be prolonged, significantly.**

***Index Terms*—underwater acoustic sensor networks, eavesdropping attack, network lifetime, energy efficiency, optimization.**

I. Introduction

In Underwater Acoustic Sensor Networks (UASNs) sensor nodes gather data periodically from the underwater environment and transfer the captured data to the sink node for further processing [1]. It is impractical to replace the batteries of sensor nodes of UASNs since these nodes can be located in remote or unattended areas. Hence, sensor nodes should dissipate their batteries in a balanced way to prolong the operational lifetime of the UASN.

In UASNs, acoustic communication is preferred rather than radio communication since electromagnetic or optical waves cannot work efficiently in underwater [2]. However, the underwater acoustic channel has poor link quality since it is characterized by low bandwidth, high packet error rates, long propagation delay, *etc.* UASN nodes have high production costs, therefore, sensor nodes should be deployed in large unattended areas [3]. As such reinforcing the security of UASNs becomes an important research challenge, especially for mission-critical applications.

Eavesdropping is a notorious malicious attack type performed to get access to the information exchange between node pairs by silent overhearing without disrupting the network. The eavesdropper can utilize the collected data to infer confidential information [4]. Eavesdropping activities accompany many of the malicious attacks. Detecting the eavesdropper is difficult since the eavesdroppers silently wiretap the acoustic channel without exposing themselves. One possible way to mitigate the risks of eavesdropping is to minimize the number of sensors potentially overhearing the data originated at other nodes which necessitates the decrease of the transmission power of sensor nodes [5] as well as the careful routing of data within the network. However, as the transmission power decreases, the number of hops required to reach the sink node increases, resulting in sensor nodes dissipating more energy for packet forwarding hence decreasing the network lifetime.

A large and growing body of literature has investigated security issues in UASNs. In [2]–[4], UASNs security threats and countermeasure methods are discussed. In [6], a Code-Division Multiple Access (CDMA) based secure communication scheme is proposed for underwater acoustic channels in the presence of eavesdropping. In [7], a tutorial on the received-signal-strength based key generation approaches for the secret underwater communication in UASNs is provided for mitigating eavesdropping attacks. In [8], an analytical framework is derived to calculate the probability of eavesdropping attacks in UASNs by considering the conditions of the underwater acoustic channel. In [9], the security of the underwater acoustic coordinated multi-point transmissions is investigated under eavesdropping attacks. In [10], a secure energy-efficient UASN protocol is proposed, which uses the Janus standard. Moreover, a lightweight key exchange protocol is suggested for establishing symmetric key encryption between the source and the destination nodes to counter eavesdropping attacks. In [11], the location privacy of the sink node is protected via multiple fake paths in UASNs against eavesdropping attacks. In [12], UASNs are secured from eavesdropping attacks such that interferences are created near the source and the destination nodes. In [13], a distributed hybrid attack is proposed that combines both jamming and eavesdropping attacks to investigate the vulnerabilities of UASNs.

To the best of our knowledge, no previous study quantitatively investigates the impact of minimizing the eavesdropping risks on UASNs lifetime. To address this research gap, in this work, we propose two optimization methods that are developed by using Mixed-Integer Programming (MIP) formulations. The first model minimizes the total number of overhearing

(*i.e.*, minimizing the eavesdropping risks) in UASNs while the second model maximizes the lifetime of UASNs under a certain overhearing constraint. Using these MIP models, we numerically explore the effects of reducing the eavesdropping risks on the lifetime of UASNs. Indeed, we aim to extend our earlier work in [14], where the relationship between eavesdropping and network lifetime is explored for terrestrial wireless sensor networks instead of UASNs.

II. System Model

A. Network Model

The UASN considered in this work consists of $|W|$ static sensor nodes and a single sink node where W denotes the set of sensor nodes. Moreover, the set V is defined to cover all nodes in the network, including the sink node. Sensor nodes are uniformly distributed over a volume of $d_e \times d_e \times h$ m^3 where h is the depth of the water. The sink node (*i.e.*, node-0) is floating on the surface of the water and located at one of the corners in the network. Each sensor node has the initial battery energy of E_{bat}. The set $\mathcal{L}$ denotes the set of discrete power levels where we assume that ten discrete power levels (*i.e.*, $|\mathcal{L}| = 10$) are available for transmission. Each sensor node adjusts the transmission power level depending on the node's distance to the target node. $d_c(l)$ is defined as the maximum communication range at power level-l (in m). The operation of the UASN continues (measured in terms of rounds) until the first node runs out of its battery.

B. Underwater Energy Dissipation Model

We adopt the underwater energy consumption model presented in [15]. According to this model, the acoustic attenuation over a distance, $d_c(l)$, is calculated as

$$A(d_c(l)) = d_c(l)^{\kappa} \times \nu^{10^{-3} d_c(l)}, \tag{1}$$

where κ is the spreading factor and $\nu = 10^{\alpha(f)/10}$ is the frequency-dependent term. In this notation, $\alpha(f)$ is the absorption coefficient (in dB/km) and f is the operating frequency. By using Thorp's formula, $\alpha(f)$ is defined as

$$\alpha(f) = \frac{0.11 f^2}{1+f^2} + \frac{44 f^2}{4100+f^2} + 2.75 \cdot 10^{-4} f^2 + 0.003. \tag{2}$$

The transmission energy cost of a single bit at power level-l is expressed as

$$E_T(l) = d_c(l)^k \times \nu^{10^{-3} d_c(l)} \times P_0, \tag{3}$$

where P_0 is the desired power level at the input to the receiver. The reception energy cost of a single bit is independent of the power level used, which can be expressed as

$$E_R = P_r. \tag{4}$$

In this equation, P_r is a constant parameter depending on the receiver node platform. Finally, each node-i adjusts its transmission power level (and its transmission energy accordingly) depending on the distance between node-i and the receiver node-j (*i.e.*, d_{ij}) as specified in the following equation

$$E_{T,ij}^{opt} = \underset{l \in \mathcal{L},\ d_{ij} \le d_c(l)}{\operatorname{argmin}} E_T(l). \tag{5}$$

C. MIP Model for Minimizing the Eavesdropping Risks

In this subsection, we present the MIP model, which minimizes the eavesdropping risks in the network. The eavesdropping risk is modeled as the total number of sensor nodes that overhear other nodes' transmissions in the network, denoted by the variable, ε_{min}. Hence, the objective function of this model is defined as

$$\text{Minimize } \varepsilon_{min}. \tag{6}$$

The constraints of this model are defined in (7)–(15). We define x_{ij}^k to be an integer decision variable that represents the number of packets generated by node-k and flowing over link-(i,j). The flow balancing constraint at each source node ($i = k$), the sink node ($i = 0$), and the relay nodes ($i \neq k$) is expressed as

$$\sum_{\substack{j \in V \\ i \neq j}} x_{ij}^k - \sum_{\substack{j \in W \\ i \neq j}} x_{ji}^k = \begin{cases} 1 & \text{if } i = k \\ -1 & \text{if } i = 0 \\ 0 & \text{o.w.} \end{cases} \quad \forall i \in V, \forall k \in W. \tag{7}$$

For calculating the total number of overhearing in the network, we assume that each sensor node generates a single packet at each round. Loops are eliminated at each source node-k via

$$\sum_{j \in W} x_{jk}^k = 0, \ \forall k \in W. \tag{8}$$

The number of packets generated by node-k and flowing from node-i using the power level-l is expressed with the integer decision variable ω_{il}^k in Const. (9) where β_{ij}^l is the binary parameter equal to 1 if node-i can transmit a packet to the node-j at power level-l, and 0, otherwise.

$$\omega_{il}^k = \sum_{j \in V} x_{ij}^k \beta_{ij}^l, \ \forall (i,k) \in W, \ \forall l \in \mathcal{L}. \tag{9}$$

In Const. (10), ω_{il}^k variables are converted to binary decision variables as $\hat{\omega}_{il}^k$ (*i.e.*, if $\omega_{il}^k > 0$ then $\hat{\omega}_{il}^k$ = 1, else $\hat{\omega}_{il}^k$ = 0).

$$\begin{aligned} \omega_{il}^k &\le M \times \ \hat{\omega}_{il}^k, \ \forall (i,k) \in W, \ \forall l \in \mathcal{L}, \\ \omega_{il}^k &\ge \hat{\omega}_{il}^k, \ \forall (i,k) \in W, \ \forall l \in \mathcal{L}, \end{aligned} \tag{10}$$

where M is a sufficiently large number. The number of packets generated by node-k and transmitted to node-j is represented by the integer decision variable, γ_{kj}, in Const. (11), where δ_{ij}^l is a parameter equal to 1 if a packet can be transmitted from node-i to node-j at power level-l.

$$\gamma_{kj} = \sum_{i \in W} \sum_{l \in \mathcal{L}} \hat{\omega}_{il}^k \times \delta_{ij}^l, \ \forall k \in W, \ \forall j \in V. \tag{11}$$

The integer decision variables, γ_{kj}, are converted to binary decision variables as $\hat{\gamma}_{kj}$ in Const. (12). Indeed, γ_{kj} shows that how many times that node-j can overhear the same packet that is generated by node-k. In other words, if $\gamma_{kj} > 1$, then $\hat{\gamma}_{kj} = 1$.

$$\begin{aligned} \gamma_{kj} &\le M \times \ \hat{\gamma}_{kj}, \ \forall k \in W, \ \forall j \in V, \\ \gamma_{kj} &\ge \hat{\gamma}_{kj}, \ \forall k \in W, \ \forall j \in V. \end{aligned} \tag{12}$$

In Const. (13), the total number of sensor nodes overhearing the packet generated by node-k is represented by the integer decision variable, ζ_k.

$$\zeta_k = \sum_{j \in V} \hat{\gamma}_{kj}, \ \forall k \in W. \tag{13}$$

The total number of overhearing in the UASN is calculated as

$$\varepsilon_{min} = \sum_{k \in W} \zeta_k. \tag{14}$$

Eventually, the boundaries for the decision variables are

$$\begin{aligned} x_{ij}^k \geq 0, \ \forall (i,k) \in W, \forall j \in V, \\ \omega_{il}^k \geq 0, \ \forall (i,k) \in W, \ \forall l \in \mathcal{L}, \\ \gamma_{kj} \geq 0, \ \forall k \in W, \ \forall j \in V, \\ \zeta_k \geq 0, \ \forall k \in W, \\ \hat{\omega}_{il}^k \in \{0,1\}, \ \forall (i,k) \in W, \ \forall l \in \mathcal{L}, \\ \hat{\gamma}_{kj} \in \{0,1\}, \ \forall (k,j) \in W. \end{aligned} \tag{15}$$

D. MIP Model for Maximizing Lifetime of UASNs Under a Certain Level of an Eavesdropping Risk

This subsection introduces the MIP model, which maximizes UASNs lifetime under a certain eavesdropping risk level. The eavesdropping risk level is modeled by defining a limitation on the total number of overhearing in the network. The objective function is to maximize the network lifetime, L (in terms of rounds), which is defined as

$$\text{Maximize } L. \tag{16}$$

Since we assume that each sensor node generates 1 packet at each round, the total number of packets generated by each sensor node during the network lifetime is equal to L. By using this approach, the flow balance constraint for this model is defined as

$$\sum_{\substack{j \in V \\ i \neq j}} x_{ij}^k - \sum_{\substack{j \in W \\ i \neq j}} x_{ji}^k = \begin{cases} L & \text{if } i = k \\ -L & \text{if } i = 0 \\ 0 & \text{o.w.} \end{cases} \quad \forall i \in V, \forall k \in W. \tag{17}$$

Const. (18) limits the energy dissipation of each sensor node to the initial battery energy.

$$\ell_p \sum_{k \in W} \left(\sum_{j \in V} E_{T,ij}^{opt} x_{ij}^k + E_R \sum_{j \in W} x_{ji}^k \right) \leq E_{bat}, \ \forall i \in W. \tag{18}$$

In this constraint, ℓ_p is the packet size (in bits). On the other hand, E_R and $E_{T,ij}^{opt}$ values are already defined in Eqs. (4) and (5), respectively.

The total number of overhearing in the network (*i.e.*, the level of eavesdropping risk) is limited to the constant, ξ, as

$$\sum_{k \in W} \zeta_k \leq \ \xi. \tag{19}$$

Finally, Consts. (8)–(13) and (15) of the MIP model defined in Sec. II-C are also included in this model.

TABLE I: Parameters used in the analysis.

Param.	Description	Value
d_c	Max. commun. range (m)	{100, 200, …, 1000}
d_e	Edge size of the network (km)	{0.4, 0.7, …, 1.9}
E_{bat}	Battery energy (KJ)	25
f	Operating frequency (kHz)	25
h	Depth of the network (m)	300
κ	Spreading factor	1.5
$\lvert\mathcal{L}\rvert$	Num. of discr. power levels	10
ℓ_p	Packet size (bytes)	1024
$\lvert W\rvert$	Number of sensor nodes	{10, 20, 30}
P_0	Power required at the input to the receiver (J/bit)	1×10^{-7}
P_r	Reception constant (J/bit)	0.2×10^{-7}

III. Analysis

In this section, we analyze the relationship between the overhearing limit and the network lifetime. For this purpose, we use the General Algebraic Modeling System (GAMS – http://www.gams.com/) to solve both of the aforementioned MIP models. The parameters that are used while solving the two MIP models are listed in Table I. For a given network topology, the two MIP models are solved in the following order:

1) We solve the MIP model in Sec. II-C to minimize the total number of overhearing in the UASN (*i.e.*, ε_{min}).
2) We solve the MIP model in Sec. II-D by plugging in $\xi = \varepsilon_{min}$ in Const. (19) where ε_{min} is obtained in Step 1. The optimum value of the objective function in (16) is denoted as $L = L_{min}$. In other words, this is the network lifetime obtained when the eavesdropping risk (*i.e.*, the overhearing limit) is minimized.
3) We also solve the MIP model in Sec. II-D by treating ξ as a free decision variable instead of a constant. The optimum value of the objective function in (16) is denoted as $L = L_{max}$. Indeed, this is the network lifetime obtained without any eavesdropping risks. Moreover, the optimum value of the decision variable becomes $\xi = \varepsilon_{max}$ that is the maximum limit of the total overhearing to achieve the maximum lifetime.

Throughout this section, all data points given in Fig. 1 are the averages of 100 randomly generated topologies.

Fig. 1a provides ε_{min} values with respect to the chosen d_e values for the three different network density configurations (*i.e.*, three $|W|$ values). ε_{min} gets the maximum value of 435 for dense networks (*i.e.*, when $|W| = 30$ and $d_e = 0.4$ km values) while ε_{min} takes the minimum vale of 60 for sparse networks (*i.e.*, when $|W| = 10$ and $d_e = 1.9$ km). When d_e is fixed, ε_{min} increases while $|W|$ grows since the total number of overhearings increases as the network becomes denser. On the other hand, as d_e increases when $|W|$ is kept constant, ε_{min} decreases up to a certain d_e value. After a fixed d_e value, ε_{min} converges to specific values.

Fig. 1b presents the percent decrement in the maximum network lifetime (L_{max}) when the total number of overhearing is limited to ε_{min}. The percent decrement in L_{max} is calculated as $100 \times \frac{|L_{max} - L_{min}|}{L_{max}}$. The minimum and maximum percent

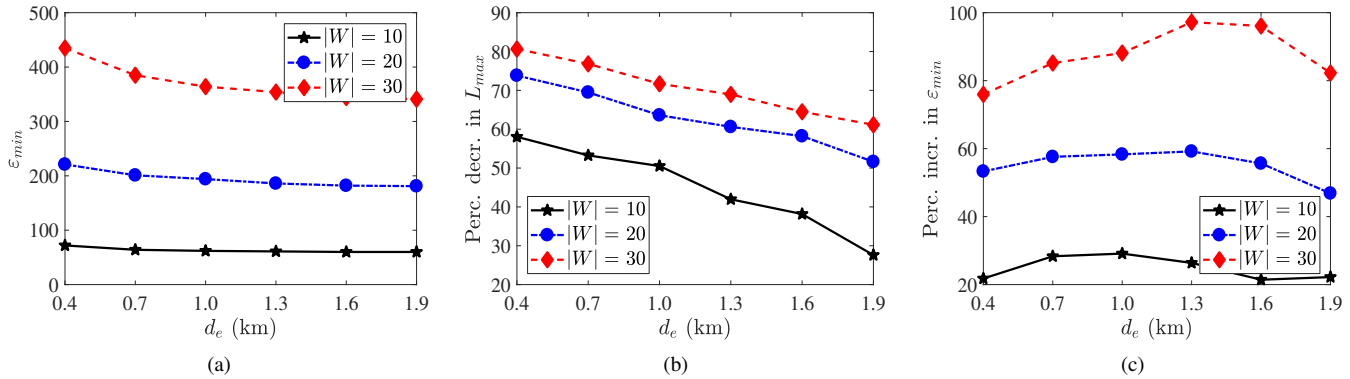

Fig. 1: The min. number of total overhearing – ε_{min} (a), the percent decrement in max. lifetime (L_{max}) when the overhearing limit is minimized (b), and the percent increment in ε_{min} to achieve L_{max} (c) as a function of d_e for three $|W|$ values.

decrements in L_{max} are obtained in the intervals 27.60%–61.14% (for $d_e = 1.9$ km) and 58.04%–80.64% (for $d_e = 0.4$ km), respectively. As $|W|$ increases for a fixed d_e value, the percent decrement in L_{max} increases since sensor nodes cannot find energy-efficient routing paths to minimize the eavesdropping risks while prolonging the network lifetime. For example, when $d_e = 0.4$ km, the percent decrements in L_{max} are obtained as 58.04%, 73.82%, and 80.64% for $|W| = 10$, 20, and 30, respectively. On the other hand, as d_e increases for a constant $|W|$, the percent decrements in L_{max} reduce since limiting the total number of overhearings to ε_{min} has relatively a light impact on the network lifetime as the network becomes sparse. For instance, when $|W| = 30$, the percent decrement in L_{max} reduces from 80.64% to 61.14% as d_e increases.

Fig. 1c shows the percent increment in ε_{min} to obtain L_{max}. The percent increment in ε_{min} is calculated as $100 \times \frac{|\varepsilon_{max} - \varepsilon_{min}|}{\varepsilon_{min}}$. The percent increment in ε_{min} to obtain the L_{max} grows as $|W|$ increases for a constant d_e value. For example, to achieve L_{max}, ε_{min} values should be increased by 21.78%, 53.30%, and 75.95%, for $|W| = 10$, 20, and 30, respectively. On the other hand, when $|W|$ is fixed, the percent increment in ε_{min} to obtain the L_{max} increases up to a certain point then it decreases. The maximum values of the percent increment in ε_{min} are observed as 97.21% (when d_e = 1.3 km and $|W|$ = 30), 59.19% (when d_e = 1.3 km and $|W|$ = 20), and 29.12% (when d_e = 1 km and $|W|$ = 10). The reason behind this result is that ε_{min} values drops much faster than the ε_{max} values when d_e increases up to a specific value.

IV. Conclusion

In this study, we investigate the impact of minimizing the eavesdropping risks on lifetime of UASNs via two MIP models. Our results show that minimizing the eavesdropping risks yield up to 80.64% shorter lifetimes than the lifetimes obtained without any eavesdropping avoidance. Moreover, relaxing the minimum overhearing limit by at most 97.21% yields the maximum network lifetimes (obtained without any eavesdropping consideration). Nevertheless, in sparse networks, the maximum network lifetime decrement due to the minimum overhearing constraint reduces, significantly.

References

[1] G. Yang, L. Dai, and Z. Wei, "Challenges, threats, security issues and new trends of underwater wireless sensor networks," *Sensors*, vol. 18, no. 11, p. 3907, 2018.

[2] G. Han, J. Jiang, N. Sun, and L. Shu, "Secure communication for underwater acoustic sensor networks," *IEEE Commun. Mag.*, vol. 53, no. 8, pp. 54–60, 2015.

[3] M. C. Domingo, "Securing underwater wireless communication networks," *IEEE Wirel. Commun.*, vol. 18, no. 1, pp. 22–28, 2011.

[4] S. Jiang, "On securing underwater acoustic networks: A survey," *IEEE Commun. Surv. Tut.*, vol. 21, no. 1, pp. 729–752, 2019.

[5] J. Kao and R. Marculescu, "Eavesdropping minimization via transmission power control in ad-hoc wireless networks," in *Proc. Ann. IEEE Commun. Soc. Sens. Ad Hoc Commun. Netw.*, vol. 2, 2006, pp. 707–714.

[6] H. Kulhandjian, T. Melodia, and D. Koutsonikolas, "Securing underwater acoustic communications through analog network coding," in *Proc. Ann. IEEE Int. Conf. Sens. Commun. Netw. (SECON)*, 2014, pp. 266–274.

[7] Y. Luo, L. Pu, Z. Peng, and Z. Shi, "RSS-based secret key generation in underwater acoustic networks: advantages, challenges, and performance improvements," *IEEE Commun. Mag.*, vol. 54, no. 2, pp. 32–38, 2016.

[8] Q. Wang, H.-N. Dai, X. Li, H. Wang, and X. Hong, "On modeling eavesdropping attacks in underwater acoustic sensor networks," *Sensors*, vol. 16, p. 721, 2016.

[9] C. Wang and Z. Wang, "Signal alignment for secure underwater coordinated multipoint transmissions," *IEEE Trans. Signal Proces.*, vol. 64, no. 23, pp. 6360–6374, 2016.

[10] H. Ghannadrezaii and J. Bousquet, "Securing a Janus-based flooding routing protocol for underwater acoustic networks," in *Proc. MTS/IEEE Charleston OCEANS*, 2018, pp. 1–7.

[11] X. Feng, Z. Wang, and N. Han, "Protection research of sink location privacy in underwater sensor networks," in *Proc. IEEE INFOCOM WKSHPS*, 2019, pp. 1–6.

[12] Y. Ye, Z. Peng, A. R. K. P, V. A. R., and X. Hong, "Active jamming for eavesdropping prevention in underwater wireless networks," in *Proc. Int. Conf. Underw. Netw. Syst. (WUWNET)*, 2019.

[13] X. Li, Y. Zhou, L. Yan, H. Zhao, X. Yan, and X. Luo, "Optimal node selection for hybrid attack in underwater acoustic sensor networks: A virtual expert-guided bandit algorithm," *IEEE Sens. J.*, vol. 20, no. 3, pp. 1679–1687, 2020.

[14] Y. Karakurt, H. U. Yildiz, and B. Tavli, "The impact of mitigation of eavesdropping on wireless sensor networks lifetime," in *Proc. Signal Proces. Commun. Appl. Conf. (SIU)*, 2018, pp. 1–4.

[15] M. A. Khan, N. Javaid, A. Majid, M. Imran, and M. Alnuem, "Dual sink efficient balanced energy technique for underwater acoustic sensor networks," in *Proc. Int. Conf. Adv. Inform. Netw. Appl. Work. (WAINA)*, 2016, pp. 551–556.