Prolonging the Lifetime of Underwater Sensor Networks Under Sinkhole Attacks

Huseyin Ugur Yildiz
TED University
Department of Electrical and Electronics Engineering
Ankara, Turkey
hugur.yildiz@tedu.edu.tr

ABSTRACT

Severe characteristics and convergecast nature of underwater acoustic channels make underwater sensor networks (USNs) vulnerable to malicious attacks. One of the most malicious attacks in USNs is the sinkhole attack, where an adversary first captures a sensor node and then lures the surrounding network traffic by using false routing information. Later, the captured node can forward the captured network traffic to the intruder or drop the packets. Sinkhole attacks negatively affect the lifetime, end-to-end latency, and energy-efficiency of USNs since lured nodes spend energy in an unbalanced manner and the forwarding process introduces additional latency. In this work, we investigate the lifetime, end-to-end latency, and energy consumption performances of USNs under sinkhole attacks within an integer programming (IP) model which maximizes USNs lifetime. Our results show that if half of the nodes in the network are lured by a sinkhole node, the network lifetime decreases at a minimum of 71%; the end-to-end latency and energy consumption are increased at least by 89% and 77% as compared to the performance metrics which are obtained in the case of no sinkhole attacks.

CCS CONCEPTS

• **Networks → Network performance modeling**; **Ad hoc networks**; *Network design principles*; *Network algorithms*; • **Theory of computation → Network optimization**; **Linear programming**.

KEYWORDS

underwater sensor networks, sinkhole attacks, integer programming, network lifetime, end-to-end latency, energy-efficiency

1 INTRODUCTION

Underwater Sensor Networks (USNs) are constructed by using numerous battery-limited sensor nodes which can perform various sensing and monitoring operations (*e.g.*, pollution monitoring, offshore exploration, tactical surveillance, *etc.*) in marine environment [1]. In a routine USN operation, sensor nodes periodically capture data related to their surroundings and report their findings to the central sonobuoy (*i.e.*, the sink node) by using multi-hop communication techniques. Since underwater sensor nodes have limited energy budget, sensor nodes should consume their battery energies in a balanced manner to prolong the network lifetime.

USN nodes generally use acoustic (sound) waves for communication due to the fact that electromagnetic waves have high attenuation in underwater environment [4]. Moreover, acoustic channels have long propagation latency since the speed of sound in underwater is five orders of magnitude lower than electromagnetic waves. Furthermore, acoustic channels have high bit error rates since the quality of the acoustic link is poor. Due to the harsh conditions of the aquatic environment and convergecast (many-to-one) traffic type of USNs, data communication can be eavesdropped, modified, forwarded or dropped by an intruder [5]. Hence, USNs security is considered as an important research challenge.

In recent years, there has been an increasing amount of literature on the security issues in USNs. For the interested readers, [3, 5, 8] provide surveys on the emerging issues of security threats and secure communications in USNs. One of the most dangerous security threats in USNs is called *denial-of-service (DoS)* attack [3]. DoS is a low-cost attack which makes network resources unavailable to the intended nodes. Furthermore, DoS attacks disrupt the communication performance of sensor nodes by forcing nodes to waste their limited battery supplies thus reducing the availability of the whole network. DoS attacks can be performed at different layers of USNs. In the physical layer, jamming is the primary type of DoS attacks [15]. In the upper layers, wormhole [10], flooding [4], and sinkhole attacks [2, 11] are widely performed. In this work, we focus on *sinkhole* attacks. In a sinkhole attack, a captured node attracts the surrounding network traffic by announcing a high-quality fake route to the central sonobuoy with the aim of dropping the sensed data. The captured node can also perform forwarding on the captured data. In this case, the captured node relays the captured messages towards the intruder who is located at the central sonobuoy by using a virtual tunnel [12]. Besides the security concerns, sinkhole attacks disrupt the energy-efficiency of USNs since captured nodes consume an excessive amount of energy to launch attacks and perform forwarding [7]. Moreover, in a sinkhole attack, the end-to-end latency (*i.e.*, the time taken for a flow to travel from source to destination) performance of USNs is negatively affected while performing forwarding [14].

In the literature, very little attention has been paid to sinkhole attacks in USNs. In [2], a reputation based channel aware routing protocol called R-CARP is proposed for USNs. The performance of R-CARP is investigated under normal conditions and different forms of sinkhole attacks in terms of energy per bit, packet delivery ratio, and latency. In [11], various forms of sinkhole attacks are investigated and an algorithm is developed to detect and cut off potential malicious nodes. The performance of the algorithm is measured in terms of throughput. To the best of our knowledge, none of these works provide an extensive analysis of the lifetime as well as end-to-end latency and energy consumption of USNs under sinkhole attacks. The contribution of this paper is twofold. First, we develop an integer programming (IP) model that maximizes USNs lifetime under sinkhole attacks. Second, by solving the IP model to optimality, we investigate the impact of the number of nodes that are lured by a sinkhole node on the lifetime, end-to-end latency, and energy consumption of USNs.

2 SYSTEM MODEL

2.1 Physical Layer Model

In the physical layer model, we adopt the underwater propagation mechanism provided in [9, 13]. The path loss observed in any link pair-(i, j) is calculated as

$$\overline{A_{ij}(f)} = \overline{A_0} + 10\kappa \log_{10}(d_{ij}) + d_{ij} \times 10^{-3} \times \overline{a(f)}, \tag{1}$$

where $\overline{A_0} = 30$ dB is the normalizing constant, $\kappa = 2$ is the spherical spreading factor, f is the central operation frequency of the underwater modem (in kHz), and d_{ij} is link distance (in m). The absorption coefficient, $\overline{a(f)}$ (in dB/km), is empirically calculated as

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

The approximation for the power spectral density of the ambient noise is given as

$$\overline{N(f)} \approx 50 - 18\log_{10}(f). \tag{3}$$

By using the passive sonar equation, the signal-to-noise ratio (SNR) at the receiver is expressed as

$$\overline{\gamma_{ij}(f)} = \overline{\mathrm{SL}} - \overline{N(f)} - \overline{A_{ij}(f)}, \tag{4}$$

where $\overline{\mathrm{SL}}$ is the acoustic transmission power (in dB re 1μPa). The relationship between the acoustic transmission power (*i.e.*, $\overline{\mathrm{SL}}$) and the electrical transmission power (*i.e.*, P_t – in W) is defined as

$$P_t = 2\pi \times z_d \times 0.67 \times 10^{-18} \times 10^{0.1 \times \overline{\mathrm{SL}}}. \tag{5}$$

In this equation, z_d is the depth of the ocean (m). For the sake of simplicity, we employ the binary phase shift keying (BPSK) modulation. The average bit error probability for the BPSK modulation is calculated as

$$p_{ij}^b = \frac{1}{2} - \frac{1}{2}\sqrt{\frac{10^{0.1\times\overline{\gamma_{ij}(f)}}}{1+10^{0.1\times\overline{\gamma_{ij}(f)}}}}. \tag{6}$$

2.2 Network Model

Our USN consists of a single central sonobuoy (node-1) which does not have any limitations on the battery, a single captured sensor node which acts as the sinkhole node (node-2), and N ordinary sensor nodes (node-3 to node-N+2). Sensor nodes and the sinkhole node are arbitrarily distributed within a rectangular region of $d_{net} \times d_{net} \times H$ m^3. The central sonobuoy is at the center of the square region, $d_{net} \times d_{net}$ m^2 and located on the ocean surface. Ordinary sensor nodes are equipped with WHOI Micromodem [6]. The central operating frequency, data rate, transmission power, reception power, and transmission range of this modem platform are given as $f = 25$ kHz, $R_b = 5$ kbps, $P_t = 8$ W, $P_r = 1$ W, and $R_{max} = 2.5$ km, respectively.

We adopt the traditional definition of the network lifetime, the time until the first node exhausts its initial battery energy. We partition the network lifetime as the equal duration of rounds where a single round lasts 100 s (*i.e.*, $T_R = 100$ s). Before the network becomes operational, the intruder captures an arbitrary sensor node as the sinkhole node. As the network becomes operational, each ordinary sensor node initiates a flow by generating a data packet which has the size 1024 bits (*i.e.*, $L_D = 1024$ bits). The sinkhole node first lures α percent of nodes randomly such that lured nodes convey their generated flow to the sinkhole node. Then, the sinkhole node forwards the captured data to the intruder who is located at the central sonobuoy. On the other hand, the remaining nodes transmit their data to the central sonobuoy. In both cases, multi-hop communication techniques are used.

For each successful flow transmission, an acknowledgment (ACK) packet is transmitted. The size of an ACK packet is 64 bits (*i.e.*, $L_A = 64$ bits). Retransmission is required if both data and ACK packets are not successfully received. In order for flow transmission to be successful, the expected number of transmission is calculated as $\lambda_{ij} = \frac{1}{p_{ij}^d \times p_{ji}^a}$. In this equation, $p_{ij}^d = (1 - p_{ij}^b)^{L_D}$ and $p_{ji}^a = (1 - p_{ji}^b)^{L_A}$ are probabilities for successfully transmitting data and ACK packets, respectively. In a single round, the transmitter node-i consumes

$$e_{ij}^t = [(L_D/R_b)P_t + (L_A/R_b)P_r] \times \lambda_{ij}, \tag{7}$$

of energy on the average where $(L_D/R_b)P_t$ is the energy required for transmitting L_D bits of packet and $(L_A/R_b)P_r$ is the energy dissipation for receiving the ACK packet, respectively. Contrarily, the receiver node-j consumes

$$e_{ji}^r = [(L_D/R_b)P_r + (L_A/R_b)P_t] \times \lambda_{ji}. \tag{8}$$

of energy on the average. The total latency of each link is

$$\tau_{ij}^d = [L_D/R_b + L_A/R_b + 2d_{ij}/c] \times \lambda_{ij}, \tag{9}$$

where $2d_{ij}/c$ is the propagation latency and $c = 1.5$ km/s is the speed of sound in underwater [13].

2.3 IP Formulation for Maximizing the Lifetime of USNs Under Sinkhole Attacks

The IP formulation which maximizes the lifetime of USNs under sinkhole attacks is presented in (10). The objective function of the IP model is the maximization of the network lifetime, $L_R \times T_R$ (in s) which is provided in (10a). In this objective function definition, L_R is a free variable that represents the network lifetime in terms of rounds. The IP model has the following decision variables:

- h_{ij}^k: The total number of flows that belong to node-k which are transmitted over link-(i, j) during the network lifetime (integer).
- g_{21}^k: The total number of captured flows of node-k by the sinkhole node and forwarded to the intruder during the network lifetime (integer).
- H_1^k: The total number of flows (generated by node-k) that are collected at the central sonobuoy (integer).
- H_2^k: The total number of flows (generated by node-k) that are collected at the sinkhole node (integer).
- e_i: The total energy dissipated by sensor node-i during the network lifetime (in J).
- L_R: The network lifetime in terms of rounds.

In (10b)–(10s), constraints of the IP model are defined.

$$\text{Maximize } L_R \times T_R \tag{10a}$$

subject to:

$$\sum_{j=1}^{N+2} h_{kj}^k = L_R,\ \forall k \in \{3,\ldots,N+2\} \tag{10b}$$

$$\sum_{j=1}^{N+2} h_{ij}^k = \sum_{j=3}^{N+2} h_{ji}^k,\ \forall (i,k) \in \{3,\ldots,N+2\}, \forall i \neq k \tag{10c}$$

$$\sum_{j=3}^{N+2} h_{j1}^k = H_1^k,\ \forall k \in \{3,\ldots,N+2\} \tag{10d}$$

$$\sum_{j=3}^{N+2} h_{j2}^k = H_2^k,\ \forall k \in \{3,\ldots,N+2\} \tag{10e}$$

$$H_2^k = g_{21}^k,\ \forall k \in \{3,\ldots,N+2\} \tag{10f}$$

$$\sum_{j=1}^{N+2} h_{kj}^k = 0,\ \forall k \in \{1,2\} \tag{10g}$$

$$\sum_{j=3}^{N+2} h_{jk}^k = 0,\ \forall k \in \{3,\ldots,N+2\} \tag{10h}$$

$$H_1^k \leq (1-a_k) \times M,\ \forall k \in \{3,\ldots,N+2\} \tag{10i}$$

$$H_2^k \leq a_k \times M,\ \forall k \in \{3,\ldots,N+2\} \tag{10j}$$

$$\sum_{k=3}^{N+2} \left(H_1^k + H_2^k\right) = N \times L_R, \tag{10k}$$

$$\sum_{k=2}^{N+2} \left(\sum_{j=1}^{N+2} (h_{ij}^k + g_{ij}^k)\tau_{ij}^d + \sum_{j=3}^{N+2} h_{ji}^k \tau_{ji}^d \right) \leq L_R \times T_R, \quad \forall i \in \{2,\ldots,N+2\} \tag{10l}$$

$$\sum_{k=2}^{N+2} \left(\sum_{j=1}^{N+2} (h_{ij}^k + g_{ij}^k)e_{ij}^t + \sum_{j=3}^{N+2} h_{ji}^k e_{ji}^r \right) = e_i, \quad \forall i \in \{2,\ldots,N+2\} \tag{10m}$$

$$e_i \leq \xi,\ \forall i \in \{2,\ldots,N+2\} \tag{10n}$$

$$h_{ij}^k = 0 \text{ if } d_{ij} > R_{max},\ \forall (i,j,k) \in \{1,\ldots,N+2\} \tag{10o}$$

$$h_{ij}^k \geq 0,\ \forall (i,j,k) \in \{1,\ldots,N+2\} \tag{10p}$$

$$g_{ij}^k \geq 0,\ \forall k \in \{3,\ldots,N+2\} \text{ if } i=2, j=1 \tag{10q}$$

$$e_i \geq 0,\ \forall i \in \{2,\ldots,N+2\} \tag{10r}$$

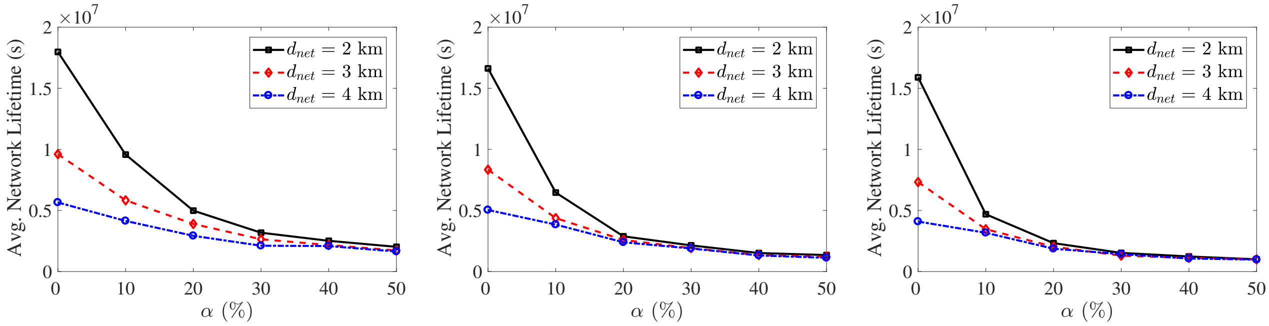
$$\{H_1^k, H_2^k\} \geq 0,\ \forall k \in \{3,\ldots,N+2\} \tag{10s}$$

Const. (10b) is the source flow generation constraint. Since a single flow is generated by node-k in each round, the total amount of flows generated by node-k during the network lifetime is L_R. Const. (10c) balances the flows that belong to node-k at each relay node-i. Consts. (10d) and (10e) calculate the total amount of flows (which are generated by node-k) that are collected at central sonobuoy (*i.e.*, H_1^k) and the sinkhole node (*i.e.*, H_2^k), respectively. Const. (10f) enforces the sinkhole node to forward all the captured data that belongs to the source node-k to the intruder who is located at the central sonobuoy. In this constraint, g_{21}^k is the virtual flow that is used for the forwarding operation. Const. (10g) ensures that the central sonobuoy and the sinkhole node cannot generate flows. Const. (10h) is the loop elimination constraint where the generated flows are prohibited to be routed to the source nodes. In Consts. (10i) and (10j), flows are forced to be terminated either at the central sonobuoy or the sinkhole node. In these constraints, we use the parameter, a_k, which takes 1 if the source node-k is lured by the sinkhole node. Otherwise, if $a_k = 0$, node-k terminates its flows at the central sonobuoy. Note that, M is sufficiently a large number. Const. (10k) equates the total amount of collected flows at both the central sonobuoy and the sinkhole node to the total number of generated flows by all sensor nodes (*i.e.*, $N \times L_R$). Const. (10l) bounds the total latency of node-i to the network lifetime. Const. (10m) calculates, e_i, the energy dissipation of node-i. Const. (10n) states that each node cannot spend more than the initial battery energy (*i.e.*, $\xi = 1$ MJ). Since the sinkhole node (node-2) is a captured sensor node, it is also subjected to the constraints defined in (10l)–(10n). However, the central sonobuoy is not subjected to these constraints. Const. (10o) enforces the maximum transmission range limitation. Finally, Consts. (10p)–(10s) show the boundaries of the decision variables.

3 ANALYSIS

In this section, we solve the IP model to optimality by using GAMS CPLEX 12 solver and provide the optimal solutions. We consider 9 network density combinations by varying N and d_{net} values. N values are taken as 20, 30, and 40; d_{net} values are chosen as 2 km, 3 km, and 4 km. On the other hand, the depth of the network is constant (*i.e.*, $z_d = 1$ km). We generate 50 random topologies such that sensor nodes are uniformly distributed and the sinkhole node is randomly chosen for each topology. In the following figures, we provide the average results obtained for the 50 topologies. Moreover, α is defined as the percent of ordinary nodes that are lured by the sinkhole node. α is varied between 0% and 50% with an increment of 10%. Three performance metrics are investigated: (i) average network lifetime, (ii) average end-to-end latency, and (iii) average energy consumption per node per round.

In Figs. 1a, 1b, and 1c, we present the average network lifetimes (*i.e.*, optimal solutions of $L_R \times T_R$ which are averaged over 50 random topologies) as a function of α for N = 20, 30, and 40, respectively. In each subfigure, N is fixed and three lifetime curves are shown for the three d_{net} values. Average network lifetimes are highest in the case of no sinkhole attack (*i.e.*, α = 0%). As α increases, average network lifetimes decrease regardless of N and d_{net} values. For example, in Fig. 1a, when $N = 20$ and $d_{net} = 4$ km, the average network lifetime is observed as 5.66×10^6 s when there is no sinkhole attack. However, if 20% of the nodes are lured by the sinkhole node (*i.e.*, α = 20%), the average network lifetime decreases to 2.93×10^6 s. Average network lifetimes drop as d_{net} values rise since nodes consume a high amount of energy to transmit their data over long acoustic links. Similarly, if d_{net} is kept constant, the increment in N results in the decrement of average network lifetimes. The most interesting aspect of this figure is that if half of the nodes are lured by the sinkhole node, average network lifetimes are at least 71% lower than the average network lifetimes which are obtained in the case of no sinkhole attack. Nevertheless, our results also show that

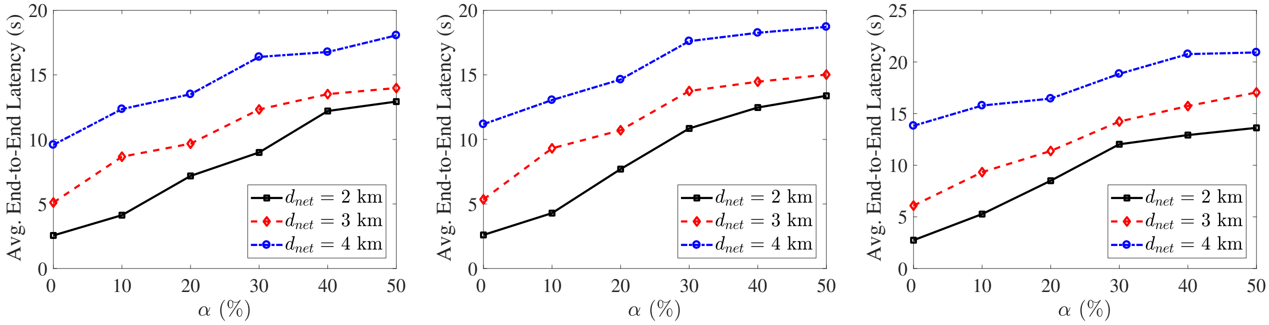


(a) $N = 20$

(b) $N = 30$

(c) $N = 40$

Figure 1: Avg. network lifetimes as a function of α for various network configuration options.

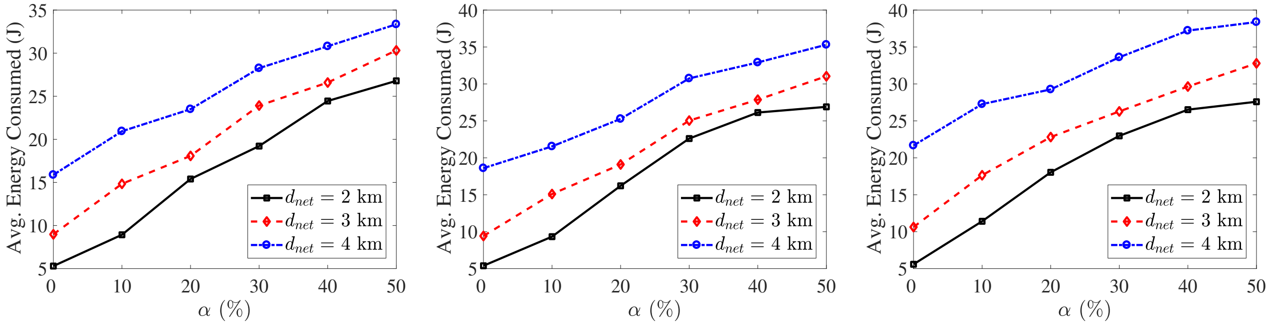


(a) $N = 20$

(b) $N = 30$

(c) $N = 40$

Figure 2: Avg. end-to-end latencies (s) as a function of α for various network configuration options.



(a) $N = 20$

(b) $N = 30$

(c) $N = 40$

Figure 3: Avg. energy consumed per node per round (J) as a function of α for various network configuration options.

the drop in average network lifetimes (when $\alpha = 0\%$) is at least by 48% if one-fifth of the nodes are lured by the sinkhole node.

In Figs. 2a, 2b, and 2c, average end-to-end latencies are provided. We use the optimal solutions of h_{ij}^k and g_{ij}^k values to calculate the average end-to-end latency as

$$\frac{\sum_{(i,j,k)}(h_{ij}^k + g_{ij}^k)\tau_{ij}^d}{\sum_{(i,j,k)}(h_{ij}^k + g_{ij}^k)}. \tag{11}$$

In the case of no sinkhole attack, average end-to-end latencies are lowest (between 2.56 s and 13.82 s). We have similar observations on average end-to-end latencies as in the lifetime analysis when the network density varies. Under the sinkhole attack, average end-to-end latencies are calculated in the interval of 4.13–20.92 s. When α increases, we observe a rise in average end-to-end latencies due to the increment in the hop count such that generated flows of lured nodes are first conveyed to the sinkhole node then the sinkhole node forwards all the captured flows to the intruder. Average end-to-end latencies in the case of no sinkhole attack increase at least by 41% if 20% of the sensor nodes are lured by the sinkhole node. Moreover, luring the half of the nodes in the network results in an increment of average end-to-end latencies (when $\alpha = 0\%$) at least by 89%.

In Figs. 3a, 3b, and 3c, we show average energy consumed per node per round as a function of α for the three aforementioned N values. This performance metric is calculated by using the optimal solutions of e_i values as

$$\frac{\sum_{i=2}^{N+2} e_i}{N \times L_R}. \tag{12}$$

Without a sinkhole attack, average energy consumptions are observed between 5.30 J and 21.67 J. In the case of a sinkhole attack, average energy consumptions increase 8.93–38.38 J. Since the sinkhole node is an ordinary sensor node with a limited battery energy, redirecting the traffic of lured nodes and forwarding this traffic to the intruder result sinkhole to consume high energy. If 20% and 50% of the nodes are lured by the sinkhole node, average energy consumptions are at least 35% and 77% higher than the average energy consumptions in the case of no sinkhole attack. Finally, it is apparent from this figure that average energy consumptions rise as d_{net} increases since nodes consume excessive energy for transmitting their flows over long links.

4 CONCLUSION

In this work, we studied the impact of sinkhole attacks on USNs lifetime, end-to-end latency, and energy-efficiency. The assessment is done by developing an IP framework that maximizes the lifetime of USNs. We gradually increase the percentage of nodes that are lured by the sinkhole node and investigate the changes in the aforementioned performance metrics. The results of our investigation show that network lifetimes drop at least by 71% as compared to the case when there are no sinkhole attacks if the sinkhole node lures half of the ordinary nodes. At the same time, end-to-end latencies and energy consumption of nodes increase at a minimum by 89% and 77% as compared to the case without a sinkhole attack.

REFERENCES

[1] Ian F Akyildiz, Dario Pompili, and Tommaso Melodia. 2005. Underwater acoustic sensor networks: research challenges. *Ad Hoc Networks* 3, 3 (2005), 257–279.

[2] Angelo Capossele, Gianluca De Cicco, and Chiara Petrioli. 2015. R-CARP: A reputation based channel aware routing protocol for underwater acoustic sensor networks. In *Proc. International Conference on Underwater Networks & Systems (WUWNET)*. Article 37, 6 pages.

[3] Yanping Cong, Guang Yang, Zhiqiang Wei, and Wei Zhou. 2010. Security in underwater sensor network. In *Proc. International Conference on Communications and Mobile Computing*, Vol. 1. 162–168.

[4] Anjana P Das and Sabu M Thampi. 2015. Secure communication in mobile underwater wireless sensor networks. In *Proc. International Conference on Advances in Computing, Communications and Informatics (ICACCI)*. 2164–2173.

[5] Mari Carmen Domingo. 2011. Securing underwater wireless communication networks. *IEEE Wireless Communications* 18, 1 (2011), 22–28.

[6] Lee Freitag, Matthew Grund, Sandipa Singh, James Partan, Peter Koski, and Keenan Ball. 2005. The WHOI micro-modem: an acoustic communications and navigation system for multiple platforms. In *Proc. MTS/IEEE OCEANS*, Vol. 2. 1086–1092.

[7] Guangjie Han, Jinfang Jiang, Lei Shu, and Mohsen Guizani. 2015. An attack-resistant trust model based on multidimensional trust metrics in underwater acoustic sensor network. *IEEE Transactions on Mobile Computing* 14, 12 (2015), 2447–2459.

[8] Guangjie Han, Jinfang Jiang, Ning Sun, and Lei Shu. 2015. Secure communication for underwater acoustic sensor networks. *IEEE Communications Magazine* 53, 8 (2015), 54–60.

[9] Jawaad Ullah Khan and Ho-Shin Cho. 2014. A data gathering protocol using AUV in underwater sensor networks. In *Proc. OCEANS - TAIPEI*. 1–6.

[10] Jiejun Kong, Zhengrong Ji, Weichao Wang, Mario Gerla, Rajive Bagrodia, and Bharat Bhargava. 2005. Low-cost attacks against packet delivery, localization and time synchronization services in under-water sensor networks. In *Proc. ACM Workshop on Wireless Security (WiSe)*. 87–96.

[11] Robert Martin and Sanguthevar Rajasekaran. 2016. Data centric approach to analyzing security threats in underwater sensor networks. In *Proc. MTS/IEEE OCEANS Monterey*. 1–6.

[12] Edith CH Ngai, Jiangchuan Liu, and Michael R Lyu. 2007. An efficient intruder detection algorithm against sinkhole attacks in wireless sensor networks. *Computer Communications* 30, 11 (2007), 2353–2364.

[13] Milica Stojanovic. 2006. On the relationship between capacity and distance in an underwater acoustic communication channel. In *Proc. ACM International Workshop on Underwater Networks (WUWNet)*. 41–47.

[14] Mohammad Wazid, Ashok Kumar Das, Saru Kumari, and Muhammad Khurram Khan. 2016. Design of sinkhole node detection mechanism for hierarchical wireless sensor networks. *Security and Communication Networks* 9, 17 (2016), 4596–4614.

[15] Michael Zuba, Zhijie Shi, Zheng Peng, and Jun-Hong Cui. 2011. Launching denial-of-service jamming attacks in underwater sensor networks. In *Proc. ACM International Workshop on Underwater Networks (WUWNet)*. Article 12, 5 pages.