Journal Pre-proof

Defense Against Underwater Spy-robots: A Distributed Anti-Theft Topology Control Mechanism for Insecure UASN

Linfeng Liu, Yaoze Zhou, Zhiyuan Xi, Jiagao Wu, Jia Xu

PII: S0167-4048(23)00124-4
DOI: https://doi.org/10.1016/j.cose.2023.103214
Reference: COSE 103214

To appear in: *Computers & Security*

Received date: 15 June 2021
Revised date: 18 January 2023
Accepted date: 27 March 2023

Please cite this article as: Linfeng Liu, Yaoze Zhou, Zhiyuan Xi, Jiagao Wu, Jia Xu, Defense Against Underwater Spy-robots: A Distributed Anti-Theft Topology Control Mechanism for Insecure UASN, *Computers & Security* (2023), doi: https://doi.org/10.1016/j.cose.2023.103214

Defense Against Underwater Spy-robots: A Distributed Anti-Theft Topology Control Mechanism for Insecure UASN

Linfeng Liu [†,‡], Yaoze Zhou[†,‡], Zhiyuan Xi[†,‡], Jiagao Wu[†,‡], and Jia Xu[†,‡]
[†] School of Computer Science and Technology, Nanjing University of Posts and Telecommunications, Nanjing 210023, China
[‡] Jiangsu Key Laboratory of Big Data Security and Intelligent Processing, Nanjing University of Posts and Telecommunications, Nanjing 210023, China

***Abstract*—Underwater Acoustic Sensor Network (UASN) is deployed for various underwater applications, such as underwater creature tracking and underwater tactical surveillance. Particularly, UASN in military applications could be invaded by some underwater spy-robots termed eavesdroppers. The eavesdroppers navigate around some anchored nodes of UASN and eavesdrop on their communication channels silently. The anchored nodes are difficult to perceive the adjacent eavesdroppers, because the eavesdroppers never actively communicate with others. Thus, the anchored nodes could disseminate the data messages while they are blithely unaware of the adjacent eavesdroppers capturing the data messages. To reduce the theft ratio of data messages and guarantee the topology connectivity of UASN, an analysis framework regarding the theft ratio of data messages is first formulated, and then a geometric distribution is constructed for the in-degrees of anchored nodes. Furthermore, a binomial distribution for the communication ranges of anchored nodes is derived from this analysis framework. In our proposed Anti-Theft Topology Control Mechanism (ATTCM), the anchored nodes set the initial communication ranges according to the obtained binomial distribution, and then the communication ranges of anchored nodes are checked and adjusted to guarantee the topology connectivity. Simulation results demonstrate the superior performance of ATTCM, i.e., ATTCM can reduce the theft ratio of data messages effectively, and it can guarantee that there is at least one available communication path from each anchored node to the surface sink.**

***Index Terms*—underwater acoustic sensor network; topology control; eavesdropper; theft ratio; topology connectivity.**

I. Introduction

Underwater Acoustic Sensor Network (UASN) [1], [2] is the enabling technology for various underwater applications, such as under ocean monitoring, deep sea surveillance [3], distributed tactical surveillance, and mine reconnaissance [4]. The sensor nodes equipped with floating buoys are anchored to underwater bottom by ropes, as illustrated in Fig. 1, the measurements of environmental events are monitored by the anchored nodes and are encapsulated into some data messages which will be transferred to the surface sink through multi-hops.

In underwater military applications, the data messages contain some confidential information and are likely to be stolen by the enemy. For instance, some data messages describing the underwater tactical environment are generated and disseminated in UASN, and several underwater spy-robots [5] (termed *eavesdroppers*) dispatched by the enemy have invaded UASN. The data messages are possible to be stolen (captured and broken) by these eavesdroppers. Typically, the eavesdroppers navigate around some anchored nodes and eavesdrop on their communication channels silently. Each eavesdropper never actively communicates with anchored nodes or other eavesdroppers, making the eavesdroppers very difficult to be perceived by the anchored nodes. Thus, the anchored nodes could disseminate the data messages while some eavesdroppers navigate into their neighborhoods and capture the data messages.

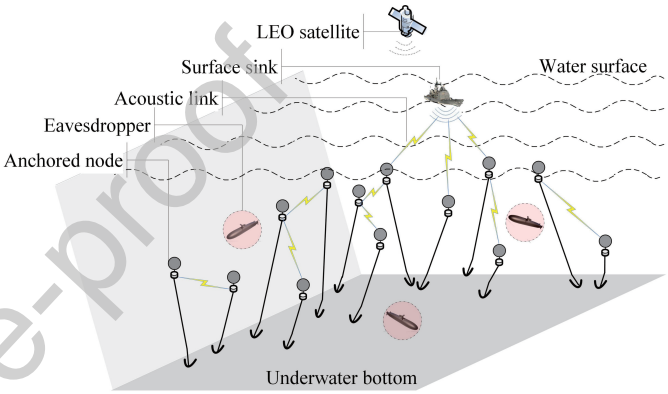


Fig. 1: UASN architecture.

The network topology is vital for the network performance, and in this paper the topology control technique of UASN is defined as the art of coordinating the communication ranges of anchored nodes to generate a desirable network topology, on which the proportion of data messages stolen by eavesdroppers (theft ratio of data messages) is reduced and the topology connectivity [6] is guaranteed. This paper conducts a study on an anti-theft topology control mechanism. We first construct a geometric distribution for the in-degrees of anchored nodes, and the probability distribution of communication ranges of anchored nodes is derived as a binomial distribution.

Then, the communication ranges of anchored nodes are coordinated according to the binomial distribution in a distributed manner to generate the network topology.

Note that although some methodologies (such as the encryption/decryption methods and identity authentication mechanisms) can help to resist the data message theft, our approach is investigated from the view of network topology, and it can be easily integrated with other methodologies jointly for a more reliable protection of data messages.

The remainder of this paper is organized as follows: Section II briefly surveys some existing related studies. Section III proposes a system model and a problem formulation. Section IV gives an analysis framework for the topology control problem. Section V presents Anti-Theft Topology Control Mechanism (ATTCM) for insecure UASN. Simulation results for performance evaluation of ATTCM are reported in Section VI. Finally, Section VII concludes this paper.

II. Related Work

A. Topology Control in WSN

The topology control problem in Wireless Sensor Network (WSN) has been extensively studied. A clustering-tree topology control algorithm based on the energy forecast is proposed for saving energy and balancing the network loads, while the link quality and packet loss rate are considered as well [7]. Tan $et\ al.$ present a topology control approach for energy harvesting WSN, and this approach allows each node to adaptively adjust its transmission power for utilizing the harvested energy effectively [8]. [9] investigates a Topology Control algorithm with Lifetime Extension (TCLE) which can construct dynamic network topologies. The topologies obtained by TCLE can improve the network lifetime significantly. In [10], a lightweight Adaptive Transmission Power Control (ATPC) is presented. In ATPC, each node builds a model to measure the correlation between transmission power and link quality. Roy $et\ al.$ focuses on the misbehaviors due to the presence of dumb nodes which can sense the surroundings but cannot communicate with neighbors [11], and an algorithm named Connectivity Re-establishment in the presence of Dumb nodes (CoRD) is designed to maintain the network self-adaptivity. [12] attempts to benchmark the efficacy of topology control protocols through two meta-heuristic algorithms, and the proposed solutions penalize the topology that impairs the topology coverage.

B. Topology Control in UASN

Several topology control methods that consider the characteristics of acoustic communications and underwater environments have been proposed for UASN. In [13], a Topology Control Strategy based on Complex Network theory (TCSCN) is put forward to construct a double clustering structure, where there are two kinds of clusterheads to ensure the connectivity and coverage, respectively. [14] proposes a physically inspired mobility model, and studies the time evolution of network coverage and connectivity, which indicates that the network mobility effect on coverage and connectivity is more significant in intermediately dense UASN. In [15], a single-leader-multi-follower Stackelberg game is utilized to formulate the topology control problem by exploiting the available communication opportunities. The ordinary nodes act as leaders, and the anchored nodes act as multiple followers. Zhang $et\ al.$ propose a vulnerability repair algorithm [16], where the coverage matrix and the vulnerability edge nodes are applied to determine whether the overlay vulnerability needs to be repaired.

C. Secure Topology Control

The secure issue has been considered in some topology control methods, such as [17], where a distributed fault-tolerant topology control algorithm is given for heterogeneous WSN. In this work, the ordinary nodes are supposed to be connected with the resource-rich nodes, and thus a k-vertex supernode-connected network topology can be constructed against the node failures caused by malicious attacks. In [18], an efficient Topology Control algorithm for node Mobility (TCM) is proposed, and the digital signature authentication based on error correction code is adopted in TCM. Lal $et\ al.$ [19] provide a hybrid architecture including physical layer security, software defined networking, node cooperation, cross-layering, context-awareness, and cognition. Specially, the network topology can be adjusted to counteract any on-going attacks. [20] develops a construction algorithm to generate a k-connected communication topology. Furthermore, a distributed event-triggered controller is designed to guarantee the consensus under Mode-Switching DoS (MSDoS) attacks.

D. Motivation of Our Work

In UASN invaded by some eavesdroppers, the data messages may be stolen by the eavesdroppers. Considering the aforementioned fact that the anchored nodes could be unconscious of the adjacent eavesdroppers, and thus the theft ratio of data messages cannot be reduced through intentionally avoiding the data message dissemination happening in the insecure areas around eavesdroppers. An intuitive idea for protecting the data messages is the employment of some encryption/decryption methods, i.e., the data messages are encrypted by the source nodes and are decrypted by the surface sink, and hence the confidential information encapsuled in the data messages will not be revealed, even if the data messages are captured by eavesdroppers. However, a sophisticated encryption/decryption method will give rise to a large computation cost, which is intolerable due to the limited computation power of anchored nodes in UASN.

Note that the theft ratio of data messages is affected seriously by the network topology (the network topology is formed by the communication ranges of anchored nodes), e.g., the data messages are easier to be stolen when the communication ranges of anchored nodes cover more eavesdroppers. In this paper, we attempt to protect the data messages from the view of topology control, and

we investigate a topology control mechanism to reduce the proportion of data messages stolen by eavesdroppers through generating a desirable network topology. Specifically, an appropriate probability distribution of in-degrees of anchored nodes is designed, and then the probability distribution of communication ranges of anchored nodes is derived to coordinate the communication ranges for anchored nodes.

III. System Model and Problem Formulation

A. Nodes

There are N anchored nodes and a surface sink, the set of which is expressed as $\boldsymbol{V} = \{v_1, v_2, \cdots, v_N, v_s\}$. The anchored nodes $v_1, v_2, \cdots, v_N$ are assumed to be uniformly deployed in a convex underwater space $\boldsymbol{D}$ ($\boldsymbol{D} \in \mathbb{R}^{+3}$), and the surface sink v_s berths at water surface. The topology of UASN is represented by a graph $\boldsymbol{G}(\boldsymbol{V}, \boldsymbol{E})$, where the set of links $\boldsymbol{E} \subseteq \boldsymbol{V} \times \boldsymbol{V}$.

There are N_e eavesdroppers which can navigate freely in the underwater space $\boldsymbol{D}$. The eavesdroppers typically navigate around some anchored nodes and intend to steal (capture and break) the data messages disseminated by these anchored nodes, as shown in Fig. 2.

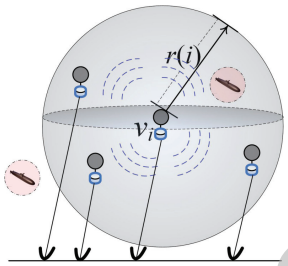


Fig. 2: An eavesdropper is eavesdropping on an anchored node v_i.

B. Communication Ranges and Links

The communication range of an anchored node v_i is denoted by $r(i)$, and $r(i)$ can be set to one of the following communication range levels: $r_0, 2r_0, 3r_0, \cdots, r_{max}$, where r_0 and r_{max} denote the minimum communication range and the maximum communication range, respectively.

The distance between two anchored nodes v_i and v_j is denoted by $d(i,j)$. If $d(i,j) \leq r(i)$, and then (i,j) is taken as a potential link. According to [21], [13], the Rayleigh fading is appropriate for describing the underwater acoustic channels, and the existence of a potential link (i,j) is determined by the probability $P_c(r(i), d(i,j))$:

$$P_c(r(i), d(i,j)) = \begin{cases} 0, & if\ d(i,j) > r(i), \\ \exp\left\{-\left[\frac{d(i,j)}{r(i)}\right]^{\frac{4\pi \cdot {r_{max}}^3 \cdot N}{3vol(\boldsymbol{D})}} \cdot \sigma^{-2}\right\}, & otherwise, \end{cases} \quad (1)$$

where σ is a Rayleigh fading parameter, and $vol(\boldsymbol{D})$ denotes the volume of the underwater space. (1) implies that a potential link could be unidirectional.

C. Objective Function

In order to reduce the theft ratio of data messages and guarantee the topology connectivity, the objective function is formally presented as follows:

$$\min\ R_t(G(\boldsymbol{V}, \boldsymbol{E})), \qquad s.t.\ Conn(G(\boldsymbol{V}, \boldsymbol{E})) > 0, \quad (2)$$

where $R_t(G(\boldsymbol{V}, \boldsymbol{E}))$ denotes the theft ratio of data messages, and the expression of $R_t(G(\boldsymbol{V}, \boldsymbol{E}))$ is given in the next section. $Conn(G(\boldsymbol{V}, \boldsymbol{E}))$ denotes the topology connectivity, and $Conn(G(\boldsymbol{V}, \boldsymbol{E})) > 0$ indicates that there is at least one available communication path from each anchored node to the surface sink, i.e.,

$$Conn(i) > 0, \qquad \forall v_i \in \boldsymbol{V} \setminus v_s, \quad (3)$$

where $Conn(i)$ denotes the path connectivity of v_i, and $Conn(i)$ is calculated as the maximum connectivity probability of all the communication paths from v_i to v_s.

IV. Analysis Framework

Because the anchored nodes are uniformly deployed, the theft ratio of data messages is related to the in-degrees of anchored nodes. The probability density function of the in-degrees of anchored nodes is denoted by $p(k)$ $(0 \leq k \leq K)$, where K is the number of neighboring anchored nodes, and evidently $K = \frac{4\pi \cdot {r_{max}}^3 \cdot N}{3vol(\boldsymbol{D})} - 1$.

Besides, the eavesdroppers navigate freely in the underwater space $\boldsymbol{D}$, and thus each eavesdropper is considered to locate in the communication range of each anchored node with an equivalent probability. Then, the expression of $R_t(G(\boldsymbol{V}, \boldsymbol{E}))$ is written as:

$$R_t(G(\boldsymbol{V}, \boldsymbol{E})) = \frac{N_e \cdot K}{N} \cdot \sum_{k=0}^{K} \left\{ p(k) \cdot \left[1 - (1-\alpha)^{k+1}\right] \right\}, \quad (4)$$

where α denotes the probability of an eavesdropper successfully breaking (deciphering) a captured data message. As illustrated in Fig. 3, if an eavesdropper is adjacent to an anchored node (with the in-degree equal to k), and then the eavesdropper locates in the communication ranges of $(k+1)$ anchored nodes.

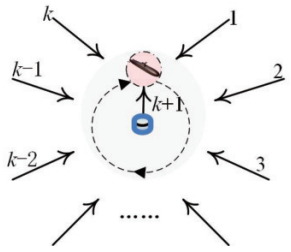


Fig. 3: An eavesdropper navigates around an anchored node (with the in-degree equal to k), and the eavesdropper could capture the data messages disseminated by a total of $(k+1)$ anchored nodes.

To simplify the analysis, the communication range of each anchored node is divided into several layers with the radius r_0, as depicted in Fig. 4. The distance between two

anchored nodes is denoted by $x \cdot r_0$, and thus the probability of the distance equal to $x \cdot r_0$ is expressed as:

$$g(x \cdot r_0) = \frac{(x \cdot r_0)^3 - [(x-1) \cdot r_0]^3}{{r_{max}}^3}, \tag{5}$$

where $x = 1, 2, \cdots, \frac{r_{max}}{r_0}$.

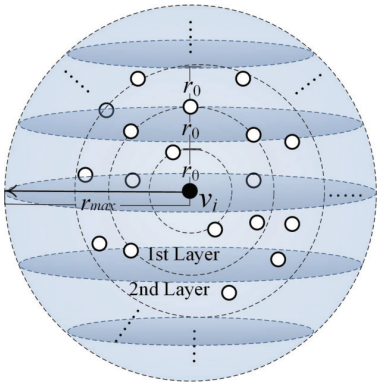


Fig. 4: Layers of the communication range of an anchored node.

A. Probability Distribution of In-degrees of Anchored Nodes

The probability density function of the in-degrees of anchored nodes $p(k)$ is given by:

$$p(k) = \left\{ \sum_{x=1}^{\frac{r_{max}}{r_0}} Q(x \cdot r_0) \cdot g(x \cdot r_0) \right\}^k \cdot \left\{ \sum_{x=1}^{\frac{r_{max}}{r_0}} \overline{Q}(x \cdot r_0) \cdot g(x \cdot r_0) \right\}^{K-k}, \tag{6}$$

where $Q(x \cdot r_0)$ denotes the probability of a link (the link length is equal to $x \cdot r_0$) existing in the network topology, and $\overline{Q}(x \cdot r_0)$ denotes the probability of a link (the link length is equal to $x \cdot r_0$) not existing in the network topology. $Q(x \cdot r_0)$ and $\overline{Q}(x \cdot r_0)$ are written as:

$$Q(x \cdot r_0) = \sum_{\kappa=x}^{\frac{r_{max}}{r_0}} P_c(\kappa \cdot r_0, x \cdot r_0) \cdot q(\kappa \cdot r_0), \tag{7}$$

$$\begin{aligned} \overline{Q}(x \cdot r_0) &= 1 - Q(x \cdot r_0) \\ &= \sum_{\kappa=1}^{x-1} q(\kappa \cdot r_0) + \sum_{\kappa=x}^{\frac{r_{max}}{r_0}} [1 - P_c(\kappa \cdot r_0, x \cdot r_0)] \cdot q(\kappa \cdot r_0), \end{aligned} \tag{8}$$

where $q(\cdot)$ denotes the probability density function of the communication ranges of anchored nodes.

The form of (6) motivates us to construct the expression of $p(k)$ as a geometric distribution:

$$p(k) = \beta \cdot b^{-k}, \quad b > 1, \tag{9}$$

and there is $\sum_{k=0}^{K} p(k) = 1$, which yields that $\beta \cdot \sum_{k=0}^{K} b^{-k} = \beta \cdot \frac{1-\left(\frac{1}{b}\right)^{K+1}}{1-\frac{1}{b}} = 1$. Hence, we obtain that:

$$\beta = \frac{1 - \frac{1}{b}}{1 - \left(\frac{1}{b}\right)^{K+1}}. \tag{10}$$

Thus, $R_t(G(\boldsymbol{V}, \boldsymbol{E}))$ can be rewritten as:

$$\begin{aligned} R_t(G(\boldsymbol{V}, \boldsymbol{E})) &= \frac{N_e \cdot K}{N} \cdot \left\{ 1 - \sum_{k=0}^{K} p(k) \cdot (1-\alpha)^{k+1} \right\} \\ &= \frac{N_e \cdot K}{N} \cdot \left\{ 1 - \frac{(1-\alpha) \cdot \left(1 - \frac{1}{b}\right)}{1 - \left(\frac{1}{b}\right)^{K+1}} \cdot \frac{1 - \left(\frac{1-\alpha}{b}\right)^{K+1}}{1 - \frac{1-\alpha}{b}} \right\}. \end{aligned} \tag{11}$$

When K is large enough (the anchored nodes are not sparsely deployed), there is obviously $\frac{\partial R_t(G(\boldsymbol{V}, \boldsymbol{E}))}{\partial b} < 0$, which indicates that the increase of b leads to the decrease of $R_t(G(\boldsymbol{V}, \boldsymbol{E}))$.

Besides, in order to guarantee the topology connectivity, the total number of in-degrees of anchored nodes should satisfy the following inequality:

$$(N-1) \cdot N \geq N \cdot \sum_{k=0}^{K} k \cdot p(k) \geq N - 1, \tag{12}$$

where $\sum_{k=0}^{K} k \cdot p(k)$ can be further approximated as:

$$\begin{aligned} \sum_{k=0}^{K} k \cdot p(k) &\approx \beta \cdot \int_0^K k \cdot b^{-k} \mathbf{d}k \\ &= \frac{1 - \frac{1}{b}}{1 - \left(\frac{1}{b}\right)^{K+1}} \cdot \left\{ \frac{1}{(\ln b)^2} - \frac{b^{-K}}{(\ln b)^2} - \frac{K \cdot b^{-K}}{\ln b} \right\}, \end{aligned} \tag{13}$$

which is approximately equal to $\frac{b-1}{b \cdot (\ln b)^2}$, and (13) implies that the maximum value of b can be achieved when $\sum_{k=0}^{K} k \cdot p(k) = \frac{N-1}{N}$.

Some numerical results of b are provided in Fig. 5. Fig. 5 indicates that the numerical value of b is related to N: b is gradually decreased with the increase of N when $N < 700$, and b almost remains a constant 2.05 when $N \geq 700$.

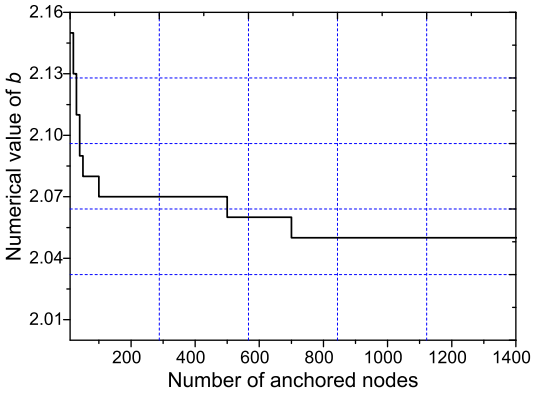


Fig. 5: Numerical value of b (the probability in the geometric distribution of in-degrees of anchored nodes).

B. Probability Distribution of Communication Ranges of Anchored Nodes

To guarantee that the communication range of each anchored node falls into the value interval $[r_0, r_{max}]$, we enable the communication ranges of anchored nodes to

obey a binomial distribution $B\left(\frac{r_{max}}{r_0}, \lambda\right)$, and the probability density function $q(x \cdot r_0)$ $(1 \leq x \leq \frac{r_{max}}{r_0})$ is defined as:

$$q(x \cdot r_0) = \begin{pmatrix} \frac{r_{max}}{r_0} - 1 \\ x - 1 \end{pmatrix} \cdot \lambda^{x-1} \cdot (1-\lambda)^{\frac{r_{max}}{r_0} - x}, \quad (14)$$

where $0 \leq \lambda \leq 1$.

According to (6), (9) and (14), we can obtain the numerical value of λ by the following equations:

$$\begin{cases} \frac{\sum_{x=1}^{\frac{r_{max}}{r_0}} \overline{Q}(x \cdot r_0) \cdot g(x \cdot r_0)}{\sum_{x=1}^{\frac{r_{max}}{r_0}} Q(x \cdot r_0) \cdot g(x \cdot r_0)} = b, \\ \left\{ \sum_{x=1}^{\frac{r_{max}}{r_0}} \overline{Q}(x \cdot r_0) \cdot g(x \cdot r_0) \right\}^K = \beta, \end{cases} \quad (15)$$

and (15) can be further simplified as:

$$\begin{cases} \sum_{x=1}^{\frac{r_{max}}{r_0}} \overline{Q}(x \cdot r_0) \cdot g(x \cdot r_0) = \sqrt[K]{\beta}, \\ \sum_{x=1}^{\frac{r_{max}}{r_0}} Q(x \cdot r_0) \cdot g(x \cdot r_0) = \frac{\sqrt[K]{\beta}}{b}. \end{cases} \quad (16)$$

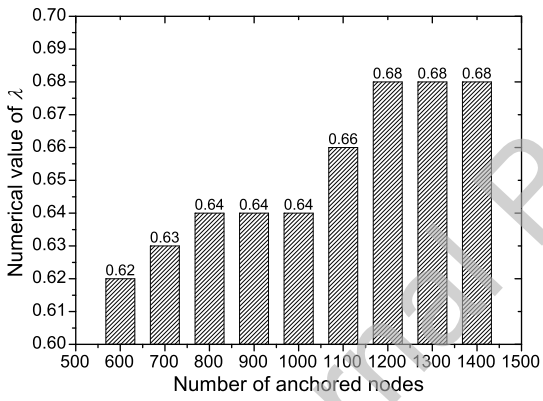


Fig. 6: Numerical value of λ (the probability in the binomial distribution of communication ranges of anchored nodes).

As shown in Fig. 6, λ is increased with the increase of N. Specially, $\lambda = 0.64$ when $N = 1,000$.

V. Anti-Theft Topology Control Mechanism

Anti-Theft Topology Control Mechanism (ATTCM) is designed for the topology construction in insecure UASN. In ATTCM, each anchored node set its initial communication range according to the obtained binomial distribution, as described in Section IV.B. Then, the communication ranges of anchored nodes are checked and adjusted to guarantee the topology connectivity (there is at least an available communication path from each anchored node to the surface sink). Note that ATTCM is a completely distributed mechanism, and thereby the communication cost and computation cost of ATTCM are very low.

TABLE I provides the main symbols used in the description of ATTCM.

TABLE I: Symbols in ATTCM description

Symbol	Definition
$\boldsymbol{S}_c$	Set of anchored nodes whose communication ranges having been checked
$\boldsymbol{S}_u$	Set of anchored nodes whose communication ranges having not been checked
$C(i)$	Coordinate of an anchored node v_i
$random(0, t_b)$	Random backoff time
t_w	Waiting time
msg_type	Type of message
$inquire\_msg$	Message from a newly checked node to inquire the neighboring unchecked nodes
$reply\_msg$	Message from an unchecked node to reply the received $inquire\_msg$
$check\_msg$	Message from a newly checked node to confirm the link of an unchecked node

A. Detailed Description of ATTCM

The detailed description of ATTCM is given as follows:

Step 1. The binomial distribution of communication ranges $B\left(\frac{r_{max}}{r_0}, \lambda\right)$ is determined by (16), and then each anchored node v_i sets its communication range $r(i)$ according to the binomial distribution independently. $\boldsymbol{S}_c$ and $\boldsymbol{S}_u$ are initialized by:

$$\boldsymbol{S}_c \leftarrow v_s, \quad \boldsymbol{S}_u \leftarrow \boldsymbol{V} \setminus v_s. \quad (17)$$

Step 2. The communication ranges of anchored nodes are checked and adjusted. This process is started from v_s and will be executed for several rounds. In each round, each newly checked node (the anchored node is added to $\boldsymbol{S}_c$ in the last round) broadcasts an $inquire\_msg$ in the maximum communication range r_{max}.

Suppose v_j has been checked in the $(t-1)$-th round, and in the t-th round v_j broadcasts an $inquire\_msg$ which contains a quintuple $(msg\_type, v_j, t, C(j), r(j))$. Besides, the $inquire\_msg$ is broadcasted by each newly checked node after a random backoff time $random(0, t_b)$, and thus the communication collisions can be avoided.

Step 3. Suppose v_i receives the $inquire\_msg$ from v_j, and the following two cases are discussed:

- (i) if $v_i \in \boldsymbol{S}_c$, and then the received $inquire\_msg$ is ignored;
- (ii) if $v_i \notin \boldsymbol{S}_c$, and then v_i sends a $reply\_msg$ containing the initial communication range $r(i)$ to v_j. A $reply\_msg$ is expressed as a sextuple form $(msg\_type, v_i, v_j, t, C(i), r(i))$.

Step 4. When v_j receives the $reply\_msg$ from v_i, and then v_j sends a $check\_msg$ to v_i in the maximum communication range r_{max}. Note that the $check\_msg$ is to confirm the existence of the link (i, j), and the existence of the link (i, j) also indicates that there is at least one available communication path from v_i to v_s.

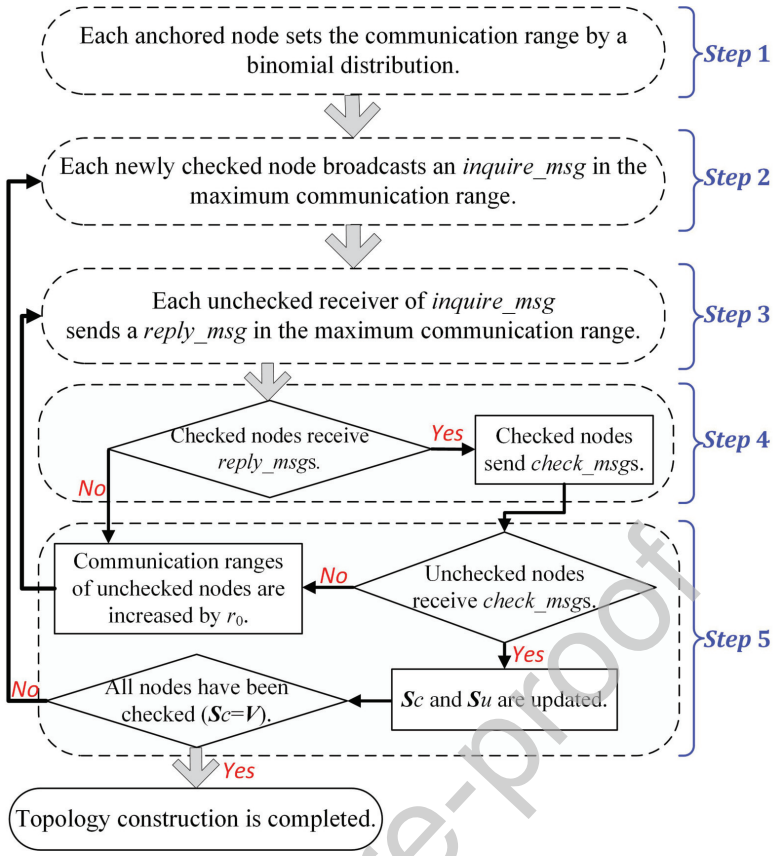


Fig. 7: Flowchart of ATTCM.

Step 5. After receiving the $check\_msg$ from v_j during a waiting time t_w, $\boldsymbol{S}_c$ and $\boldsymbol{S}_u$ are updated by:

$$\boldsymbol{S}_c \leftarrow \boldsymbol{S}_c \bigcup v_i, \quad \boldsymbol{S}_u \leftarrow \boldsymbol{S}_u \setminus v_i. \tag{18}$$

If v_i does not receive the $check\_msg$ from any checked nodes, and then $r(i)$ is increased by: $r(i) \leftarrow r(i) + r_0$. The stage from Step 3 to Step 5 will be repeated until $r(i)$ has been increased to r_{max}.

ATTCM should be re-executed at a constant interval, and thus the communication ranges of anchored nodes are periodically varied to balance the energy consumption of anchored nodes. Moreover, there are some vital anchored nodes, such as the anchored nodes with larger communication ranges or carrying more confidential information, and the re-execution mechanism can prevent the eavesdroppers from finding these vital anchored nodes.

The flowchart of ATTCM is depicted in Fig. 7, and the message interactions in ATTCM are illustrated in Fig. 8, where there are two unchecked nodes v_i and v_k adjacent to a newly checked node v_j, and v_k increases the communication range $r(k)$ when it does not receive the $check\_msg$ during a waiting time. v_i receives the $check\_msg$ and becomes a newly checked node, and then v_i broadcasts an $inquire\_msg$ to inquire the neighboring unchecked nodes.

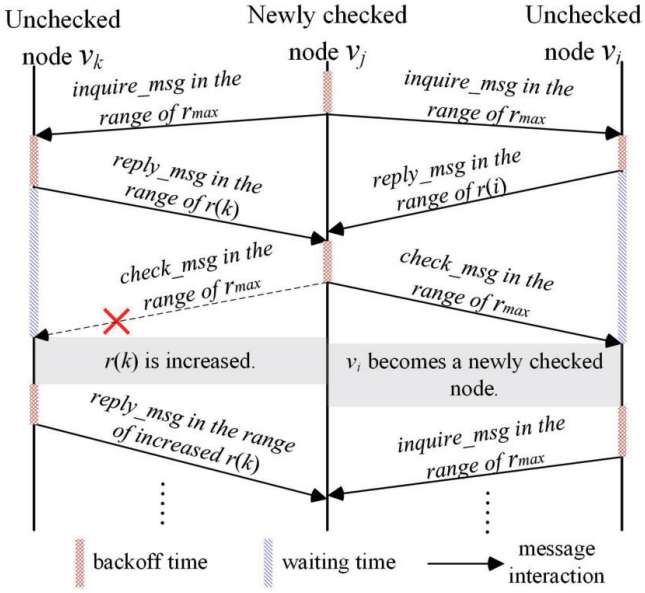


Fig. 8: Message interactions in ATTCM.

B. Complexity of ATTCM

TABLE II shows the communication complexity and computational complexity of each step in ATTCM.

The messages of ATTCM are mainly generated in Step 2,

Step 3, and Step 4. In Step 2, at most $(N-1)$ checked nodes broadcast the $inquire_msg$s. In Step 3, each unchecked node sends the $reply\_msg$ to at most K neighboring checked nodes. In the worst case, $K \cdot (N-1) \cdot \frac{r_{max}}{r_0}$ $reply_msg$s are produced. In Step 4, each checked node sends at most K $check_msg$s, which gives rise to a total number of $K \cdot (N-1)$ $check_msg$s. When r_{max} is large enough, the value of K is related to that of N, and thus the communication complexity of ATTCM is of $\mathrm{O}(N^2)$.

With regard to the computational complexity: in Step 1, $\mathrm{O}(1)$ computations are required for obtaining the numerical value of λ. In Step 2, each checked node should generate an $inquire\_msg$ and determine a random backoff time, and thus there is a total of $\mathrm{O}(N)$ computations. Likewise, the number of computations in Step 3 and Step 4 reaches $\mathrm{O}(N)$ as well. In Step 5, the sets $\boldsymbol{S}_c$ and $\boldsymbol{S}_u$ are updated for the newly checked nodes, and there are $\mathrm{O}(N)$ updates. Therefore, the computational complexity of ATTCM is of $\mathrm{O}(N)$.

TABLE II: Complexity of ATTCM

Step	Communication Complexity	Computational Complexity
1	0	O(1)
2	O(N)	O(N)
3	O(N^2)	O(N)
4	O(N^2)	O(N)
5	0	O(N)
Total	O(N^2)	O(N)

C. Theft Ratio of ATTCM

As described in Step 5 of ATTCM, some unchecked nodes could not receive the $check_msg$s from neighboring checked nodes and have to increase their communication ranges in the following cases: (i) the initial communication ranges of the unchecked nodes are shorter than the distances to the neighboring checked nodes; (ii) $reply_msg$s or $check_msg$s are not received due to the underwater probabilistic links.

Suppose the communication range of an unchecked node is r ($r_0 \le r \le r_{max}$), and the probability of the unchecked node increasing its communication range is written as:

$$\begin{aligned} P_a(r) =& P(r \ge d) \cdot [1 - P_c(r,d)] + P(r < d) \\ =& \sum_{x=0}^{\frac{r-r_0}{r_0}} g(r - x \cdot r_0) \cdot [1 - P_c(r, r - x \cdot r_0)] \\ &+ \sum_{x=1}^{\frac{r_{max}-r}{r_0}} g(r + x \cdot r_0). \end{aligned} \tag{19}$$

Then, the expectation of increase in the communication range is expressed as:

$$\mathbb{E}(\triangle r) = r_0 \cdot \sum_{x=1}^{\frac{r_{max}}{r_0}-1} \left\{ q(x \cdot r_0) \cdot \sum_{y=1}^{\frac{r_{max}}{r_0}-x} [y \cdot P_i(y)] \right\}, \tag{20}$$

where $P_i(y)$ denotes the probability of the communication range being increased by $y \cdot r_0$:

$$P_i(y) = \prod_{k=0}^{y-1} P_a(x \cdot r_0 + k \cdot r_0) \cdot [1 - P_a(x \cdot r_0 + y \cdot r_0)]. \tag{21}$$

Thus, the expectation of communication range is denoted by $\mathbb{E}(r)$ and is expressed as:

$$\mathbb{E}(r) = (r_{max} - r_0) \cdot \lambda + \mathbb{E}(\triangle r). \tag{22}$$

Therefore, the expectation of theft ratio of data messages is given by:

$$\begin{aligned} &\mathbb{E}(R_t(G(\boldsymbol{V},\boldsymbol{E}))) = \frac{N_e \cdot K}{N} \cdot \\ &\left\{ 1 - \sum_{x=1}^{\frac{\mathbb{E}(r)}{r_0}-1} \left\{ \begin{array}{l} \left\{ \frac{[(x+1)\cdot r_0]^3 - (x \cdot r_0)^3}{\mathbb{E}(r)^3} \right\} \\ \cdot \left\{ \begin{array}{l} 1 - P_c(\mathbb{E}(r), x \cdot r_0) + \\ P_c(\mathbb{E}(r), x \cdot r_0) \cdot (1-\alpha) \end{array} \right\} \end{array} \right\} \right\}, \end{aligned} \tag{23}$$

where $\frac{[(x+1)\cdot r_0]^3 - (x \cdot r_0)^3}{\mathbb{E}(r)^3}$ denotes the probability that the distance between an anchored node and an eavesdropper falls into the numerical interval $[x \cdot r_0, (x+1) \cdot r_0)$, and $[1 - P_c(\mathbb{E}(r), x \cdot r_0)] + P_c(\mathbb{E}(r), x \cdot r_0) \cdot (1-\alpha)$ denotes the probability that an eavesdropper fails to capture or break the data messages disseminated by neighboring anchored nodes.

VI. Simulations

In this section, ATTCM is evaluated by observing the performance variations with respect to different parameters and by comparing with other algorithms (TCLE, TCSCN, and TCM). We develop a simulator using Python language to assess the performance of ATTCM. Each anchored node generates a new data message every second, and the settings of main parameters are given in TABLE III.

TABLE III: Simulation parameters

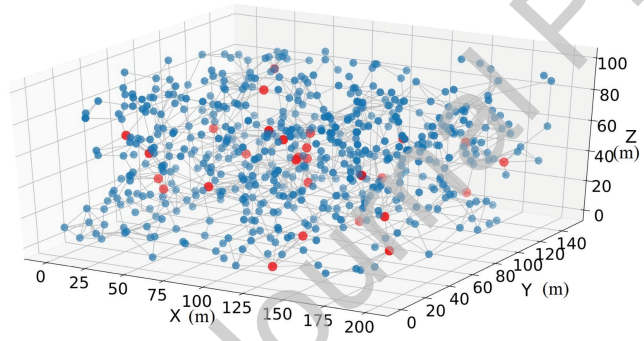
Parameter	Description	Value
N	Number of anchored nodes	1,000
N_e	Number of eavesdroppers	3
$vol(\boldsymbol{D})$	Volume of underwater space	200×150 ×100 m^3
r_{max}	Maximum communication range	20 m
r_0	Minimum communication range	2 m
σ	Rayleigh fading parameter	1.0
b	Probability in geometric distribution	2.05
λ	Probability in binomial distribution	0.64
t_b	Maximum backoff time	0.5 s
t_w	Waiting time	1.5 s
S_{uw}	Propagation speed of underwater acoustic sound	1,500 m/s
L_m	Size of each data message	500 B
B	Channel capacity	8 kbps
ρ	Probability of generating a data message each second	0.05
α	Probability of an eavesdropper breaking a captured data message	0.3

Note that the anchored nodes typically equip a kind of miniature acoustic modems [22], [23] which are with small size, low cost, and low energy consumption. Hence, the communication ranges of anchored nodes are small.

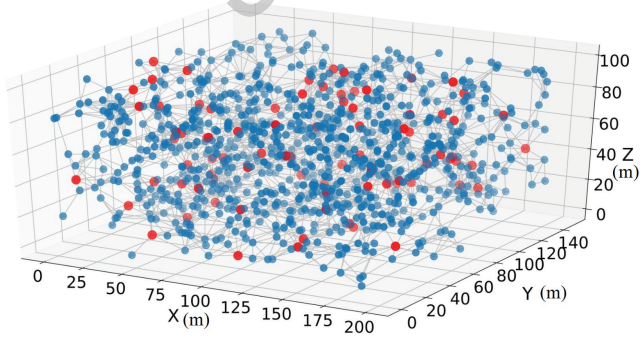
A. Topology Connectivity

Some example topologies obtained by ATTCM are provided in Fig. 9, where the nodes with in-degrees larger than 6 are marked in red. Fig. 9 indicates that the number of anchored nodes with the in-degrees larger than 6 is much smaller than N, i.e., most of the anchored nodes adopt small communication ranges to maintain the topology connectivity, and thus the theft ratio of data messages can be reduced.

ATTCM endows each anchored node with at least one available communication path to the surface sink. However, some communication paths could be invalid due to the underwater probabilistic links. To measure the quality of topology connectivity, we observe the average path connectivity which is calculated as $\frac{\sum_{i=1}^{N} Conn(i)}{N}$, and the simulation results are presented in Fig. 10, which shows that the average path connectivity grows with the increase of N or r_{max}, and this is attributed to the following two facts: (i) when the anchored nodes are deployed more densely (N becomes larger), more available communication paths from each anchored node to the surface sink can be found, and hence the average path connectivity is improved; (ii) because the communication ranges of anchored nodes obey a binomial distribution given in (14), and a larger r_{max} always gives rise to the larger communication ranges of anchored nodes, which makes more potential links exist in the topology of UASN.



(a) 600 anchored nodes



(b) 1,000 anchored nodes

Fig. 9: Example topologies obtained by ATTCM ($N = 600$, and $N = 1,000$).

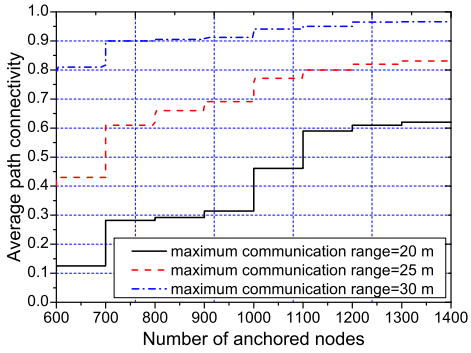


Fig. 10: Average path connectivity under different settings of N and r_{max}.

B. Theft Ratio

In Fig. 11(a), we observe that more data messages are stolen by eavesdroppers with the increase of N or r_{max}, and this is because the increase of N or r_{max} leads to the enlargements of the communication ranges of anchored nodes, implying that each eavesdropper could eavesdrop on more anchored nodes. Besides, the probability of an eavesdropper capturing the data messages disseminated by neighboring anchored nodes is raised, when the communication ranges of anchored nodes are enlarged.

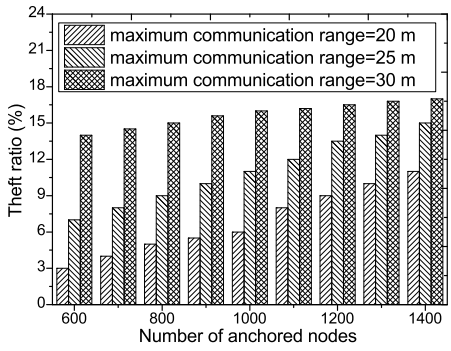
Moreover, as depicted in Fig. 11(b), a larger α indicates that the eavesdroppers are easier to break the captured data messages (e.g., each eavesdropper has a stronger computational power, or the data messages are encrypted by a simpler encryption method). A larger N_e indicates that more eavesdroppers have navigated into the underwater space, and hence more data messages are probably captured and broken by eavesdroppers. Specially, the theft ratio of data messages reaches 18.7% when $\alpha = 0.9$ and $N_e = 5$.

C. Average Energy Consumption

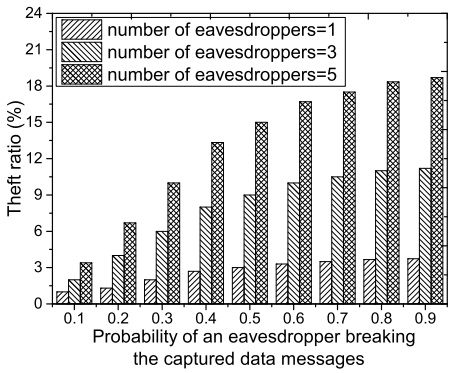
The average energy consumption is obtained as the average of all anchored nodes in unit time (every second), and thus the regularity in the variations of energy consumption can be observed. The energy consumption is calculated as [24], and the calculation details of energy consumption are provided in the section of Appendix.

Fig. 12 illustrates the average energy consumption with the variations of N and r_{max}. Two observations are obtained as follows: (i) the curved surface gradually rises up with the increase of N, and this is because the average energy consumption is linearly related to the number of anchored nodes; (ii) the average energy consumption rapidly grows as r_{max} increases, and the reason for this phenomenon is that a larger r_{max} makes the anchored nodes adopt larger communication ranges, and the anchored nodes consume more energy with larger communication ranges.

The impact of r_{max} on the average energy consumption is much larger than that of N, because the number of



(a) Theft ratio under different settings of N and r_{max}



(b) Theft ratio under different settings of α and N_e

Fig. 11: Theft ratio.

neighboring anchored nodes is the third-power of the communication range of an anchored node, while the average energy consumption is linearly related to the number of anchored nodes.

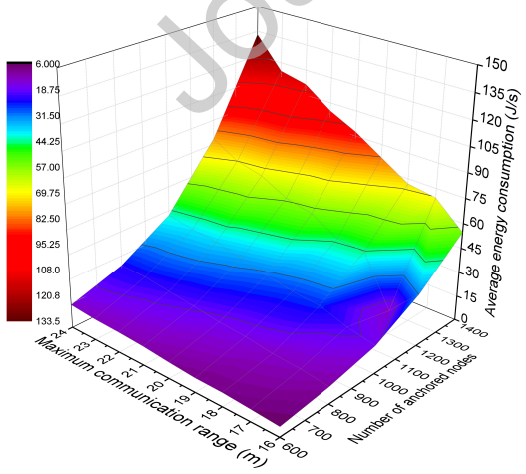


Fig. 12: Average energy consumption under different settings of N and r_{max}.

D. Algorithm Comparisons

To further analyze the merits of ATTCM, we compare ATTCM with other algorithms (TCLE, TCSCN, and TCM). These algorithms are compared in terms of the average path connectivity, theft ratio, average energy consumption, and propagation delay. The simulation results are given in Fig. 13 and Fig. 14.

To make the fair comparisons among these algorithms, these algorithms adopt the same calculations of energy consumption and transmission delay, as described in Section VIII. Besides, the simulation parameters describing the network environment are set the same, such as the number of nodes, number of eavesdroppers, size of deployment space, size of each data message, maximum/minimum communication range, and the parameters in signal irregularity formula.

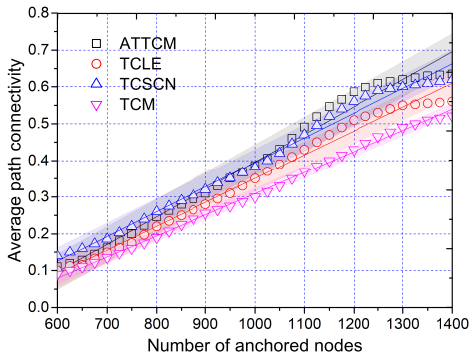
Fig. 13 and Fig. 14 indicate that ATTCM outperforms other algorithms in terms of theft ratio and average energy consumption significantly. The reason for the phenomena in Fig. 13(b) and Fig. 14(a) is that ATTCM set the communication ranges of anchored nodes according to a binomial distribution to reduce the theft ratio of data messages, i.e., the communication ranges of anchored nodes are set smaller when there has been one available communication path from each anchored node to the surface sink, and such mechanism can protect the data messages from being captured by the eavesdroppers as much as possible. Thus, the theft ratio of data messages is reduced, while the average energy consumption of anchored nodes is cut down as well. Besides, the theft ratio curve of TCM is lower than those of TCLE and TCSCN, and this is because a digital signature authentication is applied in TCM.

As shown in Fig. 13(a), the curves regarding the average path connectivity gradually ascend with the increase of N. When $N > 1,000$, ATTCM obtains the best results among these algorithms. The results of TCSCN are larger than those of ATTCM when $N < 950$, and this is due to the fact that TCSCN allows some anchored nodes to adopt large communication ranges when the number of anchored nodes is small, and more available communication paths can be found. When the number of anchored nodes becomes larger, the topology connectivity of ATTCM is remarkably improved through increasing the value of λ.

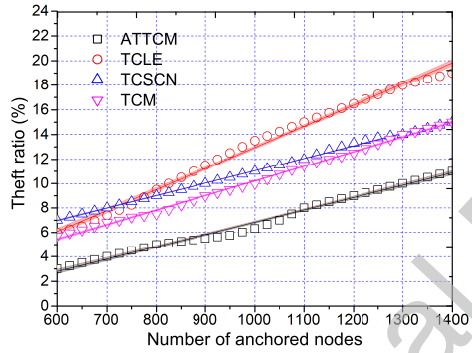
In Fig. 14(b), the propagation delay is computed as the average delay of data messages disseminated from the source nodes to the surface sink, and the transmission delay on each link is calculated as [25]. Likewise, when N is large enough, the propagation delay of ATTCM is very preferable. With the increase of the number of anchored nodes, the propagation delay of all these algorithms is reduced, because better relay nodes can be selected for the data message dissemination when the anchored nodes are deployed more densely. The propagation delay of ATTCM is shorter than those of other algorithms when the number of anchored nodes is large enough, due to the desirable network topology generated by ATTCM.

The above simulation results demonstrate that ATTCM

can reduce the theft ratio of data messages effectively through making a tradeoff between the theft ratio and the topology connectivity, and it is especially suitable for the topology construction of UASN invaded by some eavesdroppers.



(a) Average path connectivity

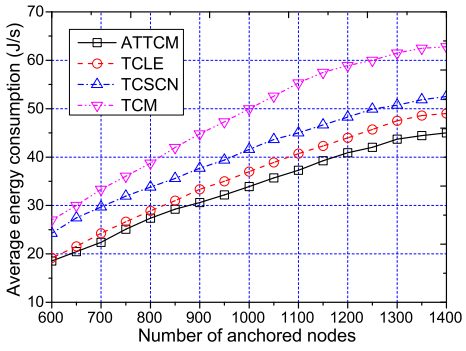


(b) Theft ratio

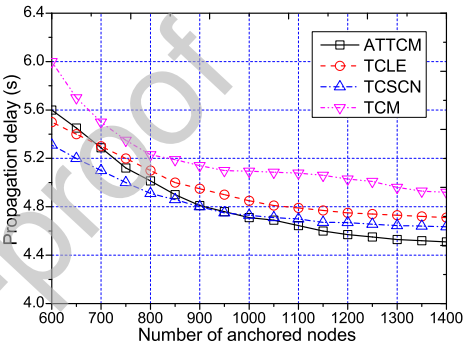
Fig. 13: Comparisons of average path connectivity and theft ratio (confidence interval=0.95).

VII. Conclusions

This study explores the topology control problem in UASN invaded by some eavesdroppers. To reduce the theft ratio of data messages and guarantee the topology connectivity, the probability distribution of in-degrees of anchored nodes is first investigated, and then a binomial distribution of communication ranges of anchored nodes is derived to generate the network topology. In our proposed Anti-Theft Topology Control Mechanism (ATTCM), each anchored node sets the initial communication range according to the binomial distribution, and then the communication range of each anchored node is checked and adjusted to guarantee the topology connectivity. Simulation results demonstrate that ATTCM can reduce the theft ratio of data messages effectively, while ATTCM can guarantee that there is at least one available communication path from each anchored node to the surface sink.



(a) Average energy consumption



(b) Propagation delay

Fig. 14: Comparisons of average energy consumption and propagation delay.

In ATTCM, several parameters should be calculated according to the deployment environment of UASN, and the calculated parameters should be released to all anchored nodes for their use. This process could bring a large delay, which should be further considered in our work.

The movement of eavesdroppers may be much more intelligent, and more data messages could be purposefully stolen by eavesdroppers, e.g., the eavesdroppers move around some anchored nodes with high degrees. A lightweight encryption/decryption mechanism with low complexity could help to reduce the number of data messages stolen by eavesdroppers effectively. Besides, in real scenario of UASN applications, more characteristics regarding the acoustic channels, such as the variable speed of sound, reflection, refraction, and large propagation losses, should be considered in the acoustic channel model. Our future research will focus on investigating these issues.

VIII. Appendix

A. Energy Consumption

The energy consumption is mainly produced by the sonar of nodes due to the transmissions of acoustic waves. For example, the energy consumption of an anchored node v_i

for each data message dissemination (in Joule per byte) is calculated by:

$$E(r(i)) = \frac{P_0 \cdot r(i)^{\varepsilon+1} \cdot 10^{\frac{r(i)\cdot\alpha(f)}{10}}}{S_{uw}},$$

where P_0 denotes the minimum received power level to guarantee the required quality of reception [24]. The energy spreading factor and absorption coefficient are denoted by $\varepsilon(\varepsilon \in [1, 2])$ and $\alpha(f)$, respectively.

The absorption coefficient for the frequency range of interest is calculated according to Thorp's expression, as introduced in [24]:

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

where $\alpha(f)$ is in dB/km, and f is in kHz. The total energy consumption of all anchored nodes is calculated by:

$$E_{total} = \sum_{i=1}^{N} E(r(i)).$$

B. Transmission Delay

The transmission delay on a link (i, j) is expressed as [25]:

$$TD(i,j) = \frac{L_m}{B} + \frac{d(i,j)}{S_{uw}},$$

where L_m is the size of each data message, and B denotes the channel capacity (in bits per second). The transmission delay consists of the channel preparation delay and the propagation delay. $\frac{L_m}{B}$ denotes the channel preparation delay (the period of data messages being prepared on channels), and $\frac{d(i,j)}{S_{uw}}$ denotes the propagation delay which is caused by the propagation of acoustic waves.

In real underwater environment, the communication bandwidth is related to temperature, pressure, and water salinity, and thus the communication bandwidth could be different with different water depth. If the variation of the communication bandwidth is considered, the anchored nodes with larger communication bandwidth should be with larger in-degrees, i.e., these anchored nodes should undertake more relay tasks for the data message dissemination. This method can be easily evolved from our proposed ATTCM by assigning larger weights to the anchored nodes with larger communication bandwidth.

Acknowledgment

This research is supported by National Natural Science Foundation of China under Grant Nos. 62272237, 61872191, 61872193; Six Talents Peak Project of Jiangsu Province under Grant No. 2019-XYDXX-247.

References

[1] G. Han, J. Du, C. Lin, *et al*, "An Energy-Balanced Trust Cloud Migration Scheme for Underwater Acoustic Sensor Networks," *IEEE Transactions on Wireless Communications*, vol. 19, no. 3, pp. 1636–1649, 2020.

[2] L. Liu, Z. Zhang, J. Wu, *et al*, "Entropy Optimization of Degree Distributions against Security Threats in UASNs," *Computer Networks*, vol. 205, 2022.

[3] E. Felemban, F. K. Shaikh, U. M. Qureshi, *et al*, "Underwater Sensor Network Applications: A Comprehensive Survey," *International Journal of Distributed Sensor Networks*, vol. 2015, Article ID 896832, 2015.

[4] G. Tuna and V. C. Gungor, "A Survey on Deployment Techniques, Localization Algorithms, and Research Challenges for Underwater Acoustic Sensor Networks," *International Journal of Communication Systems*, vol. 30, no. 3, 2017.

[5] Q. Wang and H. N. Dai, "On Modeling of Eavesdropping Behavior in Underwater Acoustic Sensor Networks," *IEEE 18th International Symposium on A World of Wireless, Mobile and Multimedia Networks (WoWMoM)*, Macau, China, 2017.

[6] N. Saeed, A. Celik, M.-S. Alouini, *et al*, "Performance Analysis of Connectivity and Localization in Multi-Hop Underwater Optical Wireless Sensor Networks," *IEEE Transactions on Mobile Computing*, vol. 18, no. 11, pp. 2604–2615, 2019.

[7] Z. Hong, R. Wang, and X. Li, "A Clustering-tree Topology Control Based on the Energy Forecast for Heterogeneous Wireless Sensor Networks," *IEEE/CAA Journal of Automatica Sinica*, vol. 3, no. 1, pp. 68–77, 2016.

[8] Q. Tan, W. An, Y. Han, *et al*, "Energy Harvesting Aware Topology Control with Power Adaptation in Wireless Sensor Networks," *Ad Hoc Networks*, vol. 27, pp. 44–56, 2015.

[9] M. Xu, Q. Yang, and K. S. Kwak, "Distributed Topology Control With Lifetime Extension Based on Non-Cooperative Game for Wireless Sensor Networks," *IEEE Sensors Journal*, vol. 16, no. 9, pp. 3332–3342, 2016.

[10] S. Lin, F. Miao, J. Zhang, *et al*, "ATPC: Adaptive Transmission Power Control for Wireless Sensor Networks," *ACM Transactions on Sensor Networks*, vol. 12, no. 1, Article 6, 2016.

[11] A. Roy, S. Misra, P. Kar, *et al*, "Topology Control for Self-Adaptation in Wireless Sensor Networks with Temporary Connection Impairment," *ACM Transactions on Autonomous and Adaptive Systems*, vol. 11, no. 14, Article 21, 2017.

[12] M. M. Fouad, A. I. Hafez, and A. E. Hassanien, "Optimizing Topologies in Wireless Sensor Networks: A Comparative Analysis between the Grey Wolves and the Chicken Swarm Optimization Algorithms," *Computer Networks*, vol. 163, 2019.

[13] L. Liu, Y. Liu, and N. Zhang, "A Complex Network Approach to Topology Control Problem in Underwater Acoustic Sensor Networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 12, pp. 3046–3055, 2014.

[14] F. Bouabdallah, "Time Evolution of Underwater Sensor Networks Coverage and Connectivity Using Physically Based Mobility Model," *Wireless Communications and Mobile Computing*, Article ID 9818931, 2019.

[15] Y. Yuan, C. Liang, M. Kaneko, *et al*, "Topology Control for Energy-Efficient Localization in Mobile Underwater Sensor Networks Using Stackelberg Game," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 2, pp. 1487–1500, 2019.

[16] W. Zhang, G. Han, Y. Liu, and J. Wang "A Coverage Vulnerability Repair Algorithm Based on Clustering in Underwater Wireless Sensor Networks," *Mobile Networks and Applications*, DOI: 10.1007/s11036-020-01621-4, 2020.

[17] F. Deniz, H. Bagci, I. Korpeoglu, *et al*, "An Adaptive, Energy-aware and Distributed Fault-tolerant Topology-control Algorithm for Heterogeneous Wireless Sensor Networks," *Ad Hoc Networks*, vol. 44, pp. 104–117, 2016.

[18] Y. Zhang, W. Chen, J. Liang, *et al*, "A Network Topology Control and Identity Authentication Protocol with Support for Movable Sensor Nodes," *Sensors*, vol. 15, no. 12, pp. 29958–29969, 2015.

[19] C. Lal, R. Petroccia, K. Pelekanakis, *et al*, "Toward the Development of Secure Underwater Acoustic Networks," *IEEE Journal of Oceanic Engineering*, vol. 42, no. 4, pp. 1075–1087, 2017.

[20] T. Zhang and D. Ye, "Distributed Secure Control Against Denial-of-Service Attacks in Cyber-Physical Systems Based on K-Connected Communication Topology," *IEEE Transactions on Cybernetics*, vol. 50, no. 7, pp. 3094–3103, 2020.

[21] G. Zhou and T. Shim, "Simulation Analysis of High Speed Underwater Acoustic Communication Based on a Statistical Channel Model," *Proc. Congress on Image and Signal Processing 2008*, pp. 512–517, Sanya, China, 2008.

[22] D. Sarriá, O. Pallarés, J. del-RÍo-Fernández, *et al*, "Low Cost OFDM based Transmitter for Underwater Acoustic Communications," *2013 MTS/IEEE OCEANS*, Bergen, Norway, 2013.

[23] P. Goulet, C. Guinet, R. Swift, *et al*, "A Miniature Biomimetic Sonar and Movement Tag to Study the Biotic Environment and Predator-prey Interactions in Aquatic Animals," *Deep-Sea Research*, vol. 148, pp. 1–11, 2019.

[24] L. Liu, R. Wang, and J. Wu, "A Time-inhomogeneous Markov Chain and Its Distributed Solution for Message Dissemination in OUSNs," *Journal of Parallel and Distributed Computing (Elsevier)*, vol. 130, pp. 179–192, 2019.

[25] S. Ibrahim, J. H. Cui, and R. Ammar, "Surface-level Gateway Deployment for Underwater Sensor Networks," *IEEE Military Communications Conference 2007*, pp. 1–7, Sanfrancisco, CA, 2007.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

CREDIT AUTHOR STATMENT

Linfeng Liu: Conceptualization, Methodology, Writing - review & editing, Funding acquisition

Yaoze Zhou: Software, Validation, Writing - original draft

Zhiyuan Xi: Investigation, Formal analysis

Jiagao Wu: Formal analysis, Data curation

Jia Xu: Writing - review & editing, Project administration

AUTHOR BIOGRAPHY

Linfeng Liu received the B. S. and Ph. D. degrees in computer science from the Southeast University, Nanjing, China, in 2003 and 2008, respectively. At present, he is a Professor in the School of Computer Science and Technology, Nanjing University of Posts and Telecommunications, China. His main research interests include the areas of vehicular ad hoc networks, wireless sensor networks and multi-hop mobile wireless networks. He has published more than 80 peer-reviewed papers in some technical journals or conference proceedings, such as IEEE TMC, IEEE TPDS, IEEE TIFS, IEEE TITS, IEEE TVT, IEEE TSC, ACM TAAS, ACM TOIT, Computer Networks, Elsevier JPDC. He has served as the TPC member of Globecom, ICONIP, VTC, WCSP.

Yaoze Zhou received the B. S. degree in computer science from the Nanjing University of Posts and Telecommunications in 2020. At present, he is a master student of Nanjing University of Posts and Telecommunications. His current research interests include the areas of underwater wireless sensor networks and vehicular ad-hoc networks.

Zhiyuan Xi received the B. S. degree in communication engineering from the Nanjing University of Posts and Telecommunications in 2018. At present, he is a master student of Nanjing University of Posts and Telecommunications. His current research interests include the areas of mobile opportunistic networks and electric vehicular networks.

Jiagao Wu received the Ph. D. degree in computer science from the Southeast University, Nanjing, China, in 2006. At present, he is an associate professor of the School of Computer Science and Technology, Nanjing University of Posts and Telecommunications. His current research interests include the areas of mobile social networks and P2P networks.

Jia Xu received the Ph. D. Degree in School of Computer Science and Engineering from Nanjing University of Science and Technology, Jiangsu, China, in 2010. He is currently a professor in Jiangsu Key Laboratory of Big Data Security and Intelligent Processing at Nanjing University of Posts and Telecommunications. His main research interests include crowdsourcing, edge computing and wireless sensor networks. Prof. Xu has served as the PC Co-Chair of SciSec 2019, Organizing Chair of ISKE 2017, TPC member of Globecom, ICC, MASS, ICNC, EDGE, and has served as the Publicity Co-Chair of SciSec 2021.