Message Piece Dissemination Approach for Opportunistic Underwater Sensor Network Invaded by Underwater Spy-robots

Linfeng Liu, Houqian Zhang, Jiagao Wu, and Jia Xu

Abstract

Opportunistic Underwater Sensor Network (OUSN) is deployed for various underwater applications, such as underwater creatures tracking and tactical surveillance. Particularly, the OUSN in military applications may be invaded by some underwater spy-robots termed eavesdroppers. The eavesdroppers could move around some OUSN nodes and eavesdrop on their communication channels silently, and these eavesdropping actions are difficult to be perceived by OUSN nodes. To reduce the theft ratio of data messages and guarantee the required delivery ratio of data messages, we conceive the idea that each data message is encoded into several message pieces, and then the message pieces are disseminated to sink node individually. Besides, a lightweight encryption method is adopted to encrypt the message pieces before the dissemination. Such mechanism can protect the data messages from being stolen by eavesdroppers effectively. In this paper, we propose a Message Piece Dissemination Approach (MPDA) for the OUSN invaded by some underwater spy-robots. In MPDA, OUSN nodes disseminate the held message pieces to some selected neighboring nodes at each time slot, and a data message is considered to be delivered when all pieces of this data message have been delivered to the sink node. Extensive simulations and comparisons demonstrate the preferable performance of MPDA, i.e., MPDA can reduce the theft ratio of data messages and guarantee the required delivery ratio of data messages.

Index Terms

opportunistic underwater sensor networks; message pieces; underwater spy-robots; theft ratio; delivery ratio.

L. Liu, H. Zhang, J. Wu, and J. Xu are with the School of Computer Science and Technology, Nanjing University of Posts and Telecommunications, Nanjing 210023, China, and also with the Jiangsu Key Laboratory of Big Data Security and Intelligent Processing, Nanjing 210023, China.

Corresponding author: Jia Xu (email: xujia@njupt.edu.cn).

I. Introduction

Opportunistic Underwater Sensor Network (OUSN) [1], [2] technology enables various underwater applications, such as underwater creatures tracking [3] and tactical surveillance [4]. Due to the underwater mobility of nodes, the available contacts between nodes are scarce and short, and thus the data messages cannot be disseminated along stable communication routes. As shown in Fig. 1, environmental events are monitored by the OUSN nodes fastened on mobile underwater vehicles (such as whales) and are encapsulated into some data messages, and then the data messages are disseminated to the sink node through intermittent multi-hop links.

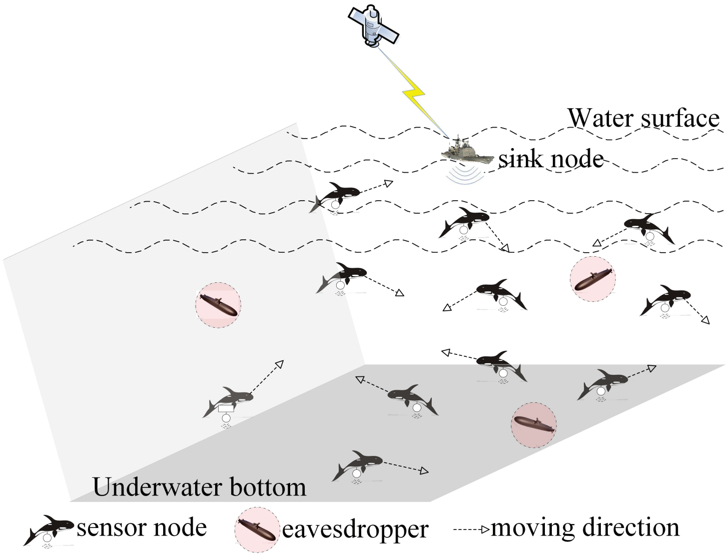


Fig. 1: An OUSN invaded by underwater spy-robots (silent eavesdroppers). The underwater spy-robots could move around some OUSN nodes and eavesdrop on their communication channels silently, and the data messages disseminated by these OUSN nodes could be captured by the underwater spy-robots.

Due to the intermittent links, the dissemination of data messages from source node to sink node could not be guaranteed even though the epidemic forwarding manner [5] is adopted, and thus the delivery ratio of data messages remains a vital issue in the message dissemination of OUSN. Especially, in many underwater military applications, the data messages containing confidential information are likely to be stolen by the enemy. For instance, some confidential data messages describing the underwater tactical environment are generated and disseminated through an OUSN, and some underwater spy-robots [6] (termed eavesdroppers) are dispatched by the enemy to invade the OUSN and steal the data messages.

The eavesdroppers could move around OUSN nodes and eavesdrop on their communication channels silently, making the eavesdroppers difficult to be perceived by OUSN nodes. The confidential data messages are probably captured by the adjacent eavesdroppers when they are being disseminated on the communication channels, and the captured data messages are considered to be stolen by eavesdroppers. Considering the fact that OUSN nodes are always unconscious of the adjacent eavesdroppers, which implies that the thefts of data messages cannot be reduced through intentionally avoiding the message dissemination in the insecure areas including eavesdroppers.

Some existing methodologies are helpful for the data message protection, e.g., the data messages could be carefully encrypted by a sophisticated encryption/decryption method, and an identity authentication mechanism could be utilized by nodes to identify the eavesdroppers. However, a sophisticated encryption/decryption method or identity authentication mechanism will give rise to a large computational cost, which is typically intolerable due to the limited computational power of nodes. Motivated by the above considerations, we encode each data message into several message pieces, and then the message pieces are individually disseminated to sink node. Besides, a lightweight encryption method is adopted to encrypt the message pieces before the dissemination, and thus the computational cost is not large. To the best of our knowledge, the encoding mechanism has not been applied to protect the data messages in the OUSN invaded by some eavesdroppers.

Such mechanism can protect the data messages from being stolen by eavesdroppers due to the following reasons: (a) It is difficult for the eavesdroppers to identify which data messages do the message pieces belong to, even though some message pieces have been captured by eavesdroppers. (b) The encoded message pieces conceal the semantic meanings of data messages, and hence the eavesdroppers cannot steal any confidential information from the message pieces. (c) The eavesdroppers do not learn about the lightweight encryption/decryption method and encryption keys, and thus they are hard to decipher the captured message pieces. Moreover, in our proposed approach the number of message pieces of each data message will be carefully investigated and set to guarantee the required delivery ratio 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 message dissemination problem. Section V presents a Message Piece Dissemination Approach (MPDA). Section VI analyzes the approach complexity, expected delivery ratio, and expected theft ratio. Section VII provides extensive simulation results to demonstrate the performance of MPDA. Finally, Section VIII gives some conclusions.

II. Related Work

A. Message Dissemination in Delay Tolerant Network

Extensive studies have been carried out on the message dissemination problem in a DTN (Delay Tolerant Network). The early representative work proposed in [5] is Epidemic Forwarding (EF), where the random pair-wise exchanges of data messages among mobile nodes ensure the maximum delivery ratio and the minimum delivery delay. However, numerous redundant message copies are produced in the transmissions. EF consumes an extremely large communication cost, which makes EF not suitable for most of practical OUSN applications. In [7], Zhao $et\ al.$ present two cooperative forwarding schemes by leveraging data fusion: epidemic routing with fusion and binary spray-and-wait with fusion, where the data packets are considered to be spatially-temporally correlated in the data forwarding process, and then the dissemination law of correlated data packets can be found out.

The security threats (such as the message thefts) are seldom considered in a DTN, and most of the message dissemination methods designed for a DTN focus on delivering the data messages to destination nodes as quickly as possible. Thus, the data messages cannot be protected from being stolen, when there are some adversaries in the DTN.

B. Message Dissemination in OUSN

Some relevant research has been conducted on the message dissemination of OUSN. Zhang $et\ al.$ develop a Beam width and Direction Concerned Routing protocol (BDCR) for the message dissemination problem [8], which can obtain a high delivery ratio by considering the beam width and three-dimensional direction. However, the measurement of beam width and three-dimensional direction is not always available, especially when the nodes move rapidly. An opportunistic routing framework considering the characteristics of underwater sensor networks, such as the network density, traffic load, underwater environment and acoustic channels is proposed in [9]. Reference [10] provides the GEographic and opportunistic routing with Depth Adjustment-based topology control Routing protocol (GEDAR). GEDAR is an anycast, geographic and opportunistic routing protocol that routes data packets from sensor nodes to multiple sonobuoys deployed at the sea's surface. When a node is located in a communication void region, GEDAR attempts to recover its connectivity through adjusting the depths of nearby nodes. In [11], an asymmetric link-based reverse routing is designed to ensure the bidirectional communications from source nodes to destination nodes. In this method, each node maintains a neighbor table in which the table items are utilized to analyze the link states, and the routing paths are established by prioritizing the utilization of symmetric links. In [12], a mobility assisted geo-opportunistic routing paradigm based on interference avoidance is designed for underwater sensor networks, and the network space is divided into some small cubes to reduce the interference and make proper routing decisions for efficient energy consumption.

In the message dissemination methods for an OUSN, a data message is typically disseminated from source node to destination node as a whole. Once the data message is captured by eavesdroppers, the confidential information contained in the data message is disclosed to the eavesdroppers. To overcome this drawback, our proposed approach will encode each data message into several message pieces and disseminate them individually.

C. Security Issues in Message Dissemination Problem

In [13], the effectiveness of erasure-code based DTN routing is evaluated, and the secret-sharing-based multi-path routing method is proposed to improve the delivery ratio of data messages. Wu $et\ al.$ present a resisting on/off attack data forwarding mechanism for mobile social networks to detect the on/off attacks [14]. Moreover, some contact-avoidance routing protocols have been put forward for the security threats in message dissemination, and most of these works seek to physically avoid the message dissemination happening in the insecure areas. Reference [15] proposes an avoidance routing framework named Multi-Path Avoidance Routing (MPAR). In MPAR, the source node first encodes a data message into k different message pieces, and these message pieces are disseminated along k different paths. However, MPAR utilizes the stable communication paths in wireless networks rather than the opportunistic paths in opportunistic networks.

In [17], a secure opportunistic path model integrating the delivery probability and the safety of opportunistic paths is constructed. Then, a Contact Avoidance Routing (CAR) protocol is given to securely disseminate a data message to the destination node against the contact-based compromise attacks. CAR assumes the adversaries can be identified by nodes, which is very difficult in the OUSN invaded by silent eavesdroppers. Reference [18] develops a certificateless authentication and road message dissemination protocol, where the certificateless signature and the relevant feedback mechanism are adopted for authentication and group key distribution. A geographic social trust routing approach is proposed in [19], where the users are distinguished by the trustworthiness and the social connectivity. This routing approach selects the shortest route comprised of trusted nodes for message dissemination. Reference [20] investigates the secure message dissemination in vehicular networks against insider attackers, and an optimal decision algorithm is proposed to make a decision on the message content by incorporating the underlying network topology information. In [21], a blockchain based message dissemination approach is provided to assess the authenticity of a data message and select the most suitable relay node in a completely decentralised manner.

The above works assume that the eavesdroppers (adversaries) can be identified through nodal action analysis or reputation assessments [22], whereas the silent eavesdroppers are difficult to be perceived by OUSN nodes. Hence, these message dissemination methods are not suitable for an OUSN. Furthermore, the large computational complexity of some sophisticated encryption methods is intolerable to the limited computational power of OUSN nodes, although these sophisticated encryption methods can strongly protect the disseminated data messages. To this end, a lightweight encryption method will be specially adopted in our proposed approach.

D. *Motivation of Our Work*

In an OUSN invaded by some eavesdroppers, the data messages are probably captured by the eavesdroppers. To reduce the theft ratio of data messages and guarantee the required delivery ratio of data messages, we allow each data message to be encoded into several message pieces, and then the message pieces are individually disseminated to the sink node. Besides, a lightweight encryption method is adopted to encrypt the message pieces before the dissemination. Such mechanism can protect the data messages from being stolen by eavesdroppers effectively.

III. System Model and Problem Formulation

A. *OUSN Model*

There are N OUSN nodes deployed in a convex space $\boldsymbol{D}$, where $\boldsymbol{D} \in \mathbb{R}^{+3}$ ($\mathbb{R}^{+3}$ denotes a 3D vector space). The time is divided into discrete time slots, as shown in Fig. 2, where t represents the absolute time slot, and τ denotes the relative time slot (from the generation of a data message). Each data message needs to be disseminated from source node to sink node within τ^* time slots. T denotes a observation period.

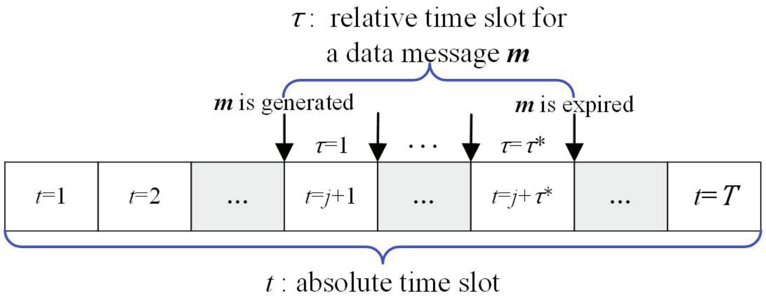


Fig. 2: Division of time slots. The time is divided into discrete time slots, t represents the absolute time slot, and τ denotes the relative time slot from the generation of a data message.

Suppose there are N_e eavesdroppers in the OUSN, and they can move around OUSN nodes and eavesdrop on the communication channels silently. As illustrated in Fig. 3, an eavesdropper moves close to a message holder (a node holding the copies of data messages) stealthily, and it could capture the data messages (or message pieces) being disseminated by the message holder.

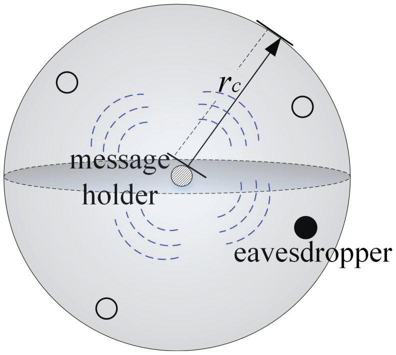


Fig. 3: An eavesdropper. The eavesdropper moves around a message holder and attempts to capture the data messages.

The communication range of each node is denoted by r_c. The coordinate of a node v_i at the t-th absolute time slot is denoted by $C(i)^{(t)}$. The distance between a node v_i and a node v_j at the t-th absolute time slot is denoted by $d(i,j)^{(t)}$. If $d(i,j)^{(t)} \leq r_c$, and then the potential communication link from v_i to v_j is denoted by $(i,j)^{(t)}$. Due to the signal irregularity phenomenon in underwater communications, the existence of a potential communication link $(i,j)^{(t)}$ is determined by a probability $P(i,j)^{(t)}$:

$$P(i,j)^{(t)} = \begin{cases} 0, & if\ d(i,j)^{(t)} > r_c, \\ c_1 \cdot \Omega(j)^{-\zeta} \cdot d(i,j)^{(t)^{-\eta}}, & otherwise, \end{cases} \tag{1}$$

where $\Omega(j)$ denotes the signal irregularity around v_j. The signal irregularity is caused by various factors, such as antenna directions, antenna gains, battery status, signal-noise-ratio threshold, and obstacles [23].

To simplify the problem analysis, we assume that the signal irregularity of each node obeys a uniform distribution $U(\Omega_{min}, \Omega_{max})$ [24]. In (1), c_1 is a constant, and $c_1 = \Omega_{min}^{\zeta} \cdot {r_0}^{\eta}$, where r_0 denotes the threshold of communication range between two neighboring nodes.

Besides, the underwater mobility pattern of OUSN nodes is comprised of autonomous movement and coordinate deviation, as introduced in our early work [25].

B. Message Pieces

At each time slot, each node generates a new data message with a probability ρ, and thus $N \cdot \rho$ new data messages are generated in the OUSN. Each data message is encoded into $\mathcal{K}$ message pieces, e.g., the data message $\boldsymbol{m}$ is encoded into $m_1, m_2, \cdots, m_{\mathcal{K}}$, and $\boldsymbol{m} = m_1 \oplus m_2 \oplus \cdots \oplus m_{\mathcal{K}}$. Here, $\oplus$ denotes the XOR operation [15].

Then, each message piece is encrypted by a lightweight encryption method (such as Data Encryption Standard (DES) [16]) and an encryption key which is randomly selected from $\mathcal{N}$ available encryption keys $e_1, e_2, \cdots, e_n, \cdots, e_{\mathcal{N}}$. The $\mathcal{N}$ encryption keys are reserved by OUSN nodes, and the eavesdroppers are assumed to decipher a captured message piece (encrypted by the n-th encryption key) with the probability p_n.

Each encrypted message piece is copied and disseminated during the future τ^* time slots, i.e., the piece holders (the nodes holding the copies of message pieces) produce and disseminate κ new copies of each held message piece at each time slot.

After receiving $\mathcal{K}$ different pieces of a data message, the sink node can recover the data message, i.e., the data message has been delivered to sink node. In contrast, a data message is considered to be stolen when $\mathcal{K}$ different pieces of the data message are captured and deciphered by an eavesdropper. The message dissemination process is described in Fig. 4.

C. Objective Function

To reduce the theft ratio of data messages and guarantee the required delivery ratio of data messages, the objectives of message dissemination problem are formally presented as follows:

$$\min \; Tr(\tau^*, T), \qquad s.t. \; \mathcal{R}(\tau^*) \geq \widetilde{\mathcal{R}}, \tag{2}$$

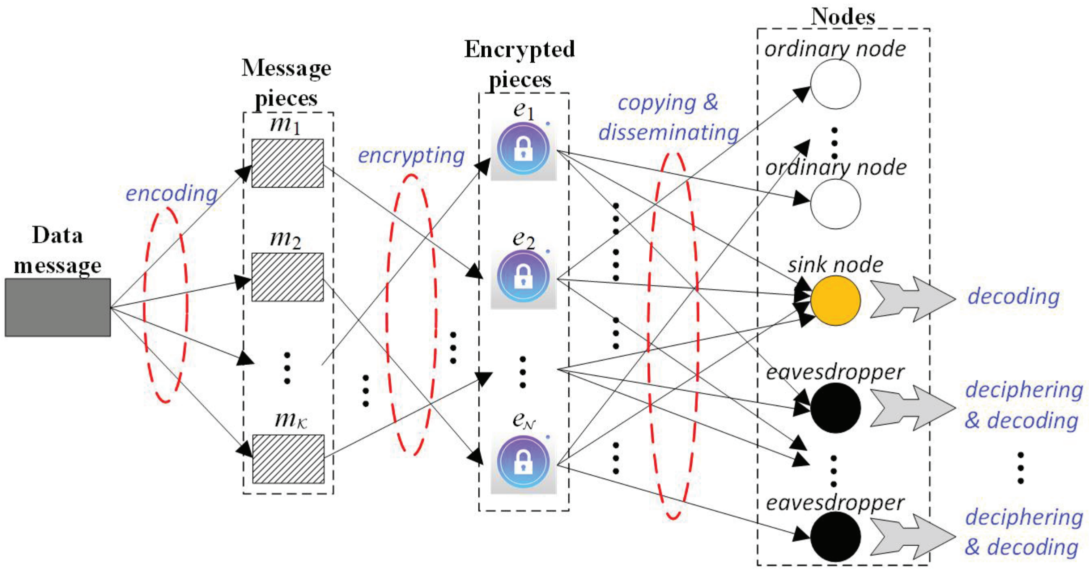


Fig. 4: Data message encoding, encrypting, disseminating, deciphering and decoding. A data message is first encoded in to $\mathcal{K}$ message pieces, and then the message pieces are encrypted. The encrypted message pieces are copied and disseminated to the sink node. The encrypted message pieces could be captured and deciphered by eavesdroppers as well.

where $Tr(\tau^*, T)$ denotes the theft ratio of data messages which is defined as the proportion of data messages (within τ^* time slots after the generation of each data message) stolen by eavesdroppers during a observation period T.

$\mathcal{R}(\tau^*)$ denotes the delivery ratio of data messages which is defined as the proportion of data messages (within τ^* time slots after the generation of each data message) delivered to sink node, and $\widetilde{\mathcal{R}}$ denotes the required delivery ratio.

IV. Analysis Framework

The explanations of main notations are presented in TABLE I.

A. Delivery Ratio

As depicted in Section III.B, the copy number of each message piece at the τ-th relative time slot is written as $(1+\kappa)^{\tau-1}$. When the nodes are evenly deployed into $\boldsymbol{D}$, the nodes can be approximatively considered to remain a uniform distribution after movements, as proven in [2]. Thus, the probability of a data message being delivered to sink node at the τ-th relative time slot is expressed as:

$$\mathcal{R}_a(\tau) = \left\{ \widetilde{P}_c \cdot \frac{4\pi \cdot {r_c}^3 \cdot (1+\kappa)^{\tau-1}}{3|\boldsymbol{D}|} \right\} \cdot \left\{ \widetilde{P}_c \cdot \frac{4\pi \cdot {r_c}^3 \cdot \sum_{j=1}^{\tau}(1+\kappa)^{j-1}}{3|\boldsymbol{D}|} \right\}^{\mathcal{K}-1}, \qquad (3)$$

TABLE I: Main Notations

Parameter	Description
$\mathcal{R}_a(\tau)$	Probability of a data message being delivered to sink node at the τ-th relative time slot
$\mathcal{R}(\tau)$	Probability of a data message being delivered to sink node within τ time slots
$\mathcal{E}_a(t,\tau)$	Probability of a data message (generated at the t-th absolute time slot) being stolen by eavesdroppers at the $(t+\tau-1)$-th absolute time slot
$\mathcal{E}(t,\tau)$	Probability of a data message (generated at the t-th absolute time slot) being stolen by eavesdroppers before or at the $(t+\tau-1)$-th absolute time slot
$P_b(t)^{(n)}$	Probability of a message piece (encrypted by the n-th key) being deciphered at the t-th absolute time slot
$P_{\mathcal{B}}(t,\tau)$	Probability of all encryption keys being deciphered before or at the $(t+\tau-1)$-th absolute time slot
$N(t)$	Number of data messages whose message pieces have been captured by an eavesdropper at the t-th absolute time slot
$Tr(\tau^*,T)$	Theft ratio of data messages

where $\mathcal{R}_a(\tau)$ is calculated as the probability that all message pieces are delivered to sink node within τ time slots and at least one message piece is delivered to sink node at the τ-th relative time slot. $\widetilde{P}_c \cdot \frac{4\pi \cdot {r_c}^3 \cdot (1+\kappa)^{\tau-1}}{3|\boldsymbol{D}|}$ denotes the probability that one of $\mathcal{K}$ message pieces has been delivered to sink node at the τ-th relative time slot, and $\left\{\widetilde{P}_c \cdot \frac{4\pi \cdot {r_c}^3 \cdot \sum_{j=1}^{\tau}(1+\kappa)^{j-1}}{3|\boldsymbol{D}|}\right\}^{\mathcal{K}-1}$ denotes the probability that $\mathcal{K}-1$ message pieces have been delivered to sink node within τ time slots.

In (3), $\widetilde{P}_c$ denotes the expected existence probability of a potential communication link, and $\widetilde{P}_c$ is calculated by:

$$\begin{aligned}\widetilde{P}_c &= \frac{c_1 \cdot \int_{\Omega_{min}}^{\Omega_{max}} \omega^{-\zeta} \mathbf{d}\omega}{\Omega_{max}-\Omega_{min}} \cdot \frac{\sum_{k=1}^{\frac{r_c}{r_0}} [k^3-(k-1)^3] \cdot (k \cdot r_0)^{-\eta}}{(\frac{r_c}{r_0})^3} \\ &= \frac{c_1 \cdot ({\Omega_{max}}^{1-\zeta} - {\Omega_{min}}^{1-\zeta})}{(1-\zeta)\cdot(\Omega_{max}-\Omega_{min})} \cdot \frac{\sum_{k=1}^{\frac{r_c}{r_0}} (3k^2-3k+1) \cdot (k \cdot r_0)^{-\eta}}{(\frac{r_c}{r_0})^3}.\end{aligned}$$

We have that $\mathcal{R}(\tau) = \mathcal{R}(\tau-1) + \mathcal{R}_a(\tau) \cdot \{1-\mathcal{R}(\tau-1)\}$, which yields that:

$$\mathcal{R}(\tau) \approx 1 - c_2 \cdot e^{-\int \mathcal{R}_a(\tau)\mathbf{d}\tau}, \tag{4}$$

and we obtain that $\mathcal{R}(1) = \left(\widetilde{P}_c \cdot \frac{4\pi \cdot {r_c}^3}{3|\boldsymbol{D}|}\right)^{\mathcal{K}}$, hence $c_2 = \{1-\mathcal{R}(1)\} \cdot e^{\frac{\mathcal{R}(1)}{\mathcal{K} \cdot \ln(1+\kappa)}}$.

B. Theft Ratio

When $\mathcal{K}$ different pieces of a data message have been captured by an eavesdropper, these message pieces will be deciphered by the eavesdropper.

The probability of an encryption key being selected to encrypt at least a message piece is written as $1-\left(\frac{\mathcal{N}-1}{\mathcal{N}}\right)^{\mathcal{K}}$. The probability of the n-th encryption key e_n being deciphered by an eavesdropper at the t-th absolute time slot is denoted by $P_b(t)^{(n)}$, and it is concerned with the number of data messages whose message pieces have been captured by the eavesdropper. Therefore, $P_b(t)^{(n)}$ is expressed as:

$$P_b(t)^{(n)} = \prod_{j=1}^{t-1} \left\{1 - P_b(j)^{(n)}\right\} \cdot \left\{1 - \left[1 - \left(1 - \left(\frac{\mathcal{N}-1}{\mathcal{N}}\right)^{\mathcal{K}}\right) \cdot p_n\right]^{N(t)}\right\}, \tag{5}$$

where $\prod_{j=1}^{t-1}\left\{1 - P_b(j)^{(n)}\right\}$ denotes the probability of e_n not being deciphered by the eavesdropper in the previous $(t-1)$ time slots, and $\left[1 - \left(1 - \left(\frac{\mathcal{N}-1}{\mathcal{N}}\right)^{\mathcal{K}}\right) \cdot p_n\right]^{N(t)}$ denotes the probability that e_n is not deciphered by the eavesdropper at the t-th absolute time slot. Note that once e_n is successfully deciphered by an eavesdropper, and then e_n becomes invalid to this eavesdropper in the future time slots.

As aforementioned above, the expired message pieces will be discarded by the piece holders. Thus, when $t \leq \tau^*$, there are $N \cdot \rho \cdot t$ data messages existing in the OUSN; otherwise, when $t > \tau^*$ there are $N \cdot \rho \cdot \tau^*$ data messages existing in the OUSN. The number of data messages whose message pieces have been captured by an eavesdropper at the t-th absolute time slot is denoted by $N(t)$ and is expressed as:

$$N(t) = \begin{cases} N \cdot \rho \cdot \mathcal{R}(1), & t = 1, \\ N \cdot \rho \cdot \sum_{j=1}^{t} \mathcal{R}_a(j), & 2 \leq t \leq \tau^*, \\ N \cdot \rho \cdot \sum_{j=1}^{\tau^*} \mathcal{R}_a(j), & \tau^* < t \leq T. \end{cases} \tag{6}$$

In (6), $\mathcal{R}_a(j)$ also denotes the probability of $\mathcal{K}$ different pieces of a data message being captured by an eavesdropper at the j-th relative time slot.

Therefore, with regard to a data message $\boldsymbol{m}$ generated at the t-th absolute time slot, the probability of $\boldsymbol{m}$ being stolen by eavesdroppers at the τ-th $(1 \leq \tau \leq \tau^*)$ relative time slot is given by:

$$\mathcal{E}_a(t,\tau) = N_e \cdot \mathcal{R}_a(\tau) \cdot P_{B}(t,\tau), \tag{7}$$

where $P_{B}(t,\tau)$ denotes the probability of all encryption keys being deciphered before or at the $(t+\tau-1)$-th absolute time slot, and $P_{B}(t,\tau)$ can be written as:

$$P_{B}(t,\tau) = \prod_{n=1}^{\mathcal{N}} \left\{ \begin{array}{c} \left[1 - \left(\frac{\mathcal{N}-1}{\mathcal{N}}\right)^{\mathcal{K}}\right] \cdot \prod_{j=1}^{t+\tau-2}\left(1 - P_b(j)^{(n)}\right) \cdot p_n \\ + \left(\frac{\mathcal{N}-1}{\mathcal{N}}\right)^{\mathcal{K}} \cdot \prod_{j=1}^{t+\tau-2}\left(1 - P_b(j)^{(n)}\right) + 1 - \prod_{j=1}^{t+\tau-2}\left(1 - P_b(j)^{(n)}\right) \end{array} \right\}. \tag{8}$$

Equation (8) indicates that $P_{B}(t,\tau)$ is calculated as the product of the probabilities of successfully deciphering the encryption keys. Specially, $\prod_{j=1}^{t+\tau-2}\left(1 - P_b(j)^{(n)}\right)$ denotes the probability of the key

e_n having not been deciphered in previous $(t+\tau-2)$ time slots; $\left(\frac{\mathcal{N}-1}{\mathcal{N}}\right)^{\mathcal{K}}$ denotes the probability of the key e_n not being selected to encrypt any message pieces of ***m***; $\left[1-\left(\frac{\mathcal{N}-1}{\mathcal{N}}\right)^{\mathcal{K}}\right]\cdot\prod_{j=1}^{t+\tau-2}\left(1-P_b(j)^{(n)}\right)\cdot p_n$ denotes the probability of the key e_n being successfully deciphered at the $(t+\tau-1)$-th absolute time slot.

Furthermore, there is $\mathcal{E}(t,\tau)=\mathcal{E}(t,\tau-1)+\mathcal{E}_a(t,\tau)\cdot[1-\mathcal{E}(t,\tau-1)]$, which can be approximated to a Bernoulli equation, and then we have that:

$$\mathcal{E}(t,\tau)\approx 1-c_3(t)\cdot e^{-\int\mathcal{E}_a(t,\tau)\mathbf{d}\tau}, \tag{9}$$

a special case of which is that $\mathcal{E}(t,1)=N_e\cdot\mathcal{R}(1)\cdot P_{_B}(t,1)$. We obtain that:

$$c_3(t)=\{1-N_e\cdot\mathcal{R}(1)\cdot P_{_B}(t,1)\}\cdot e^{\frac{N_e\cdot\mathcal{R}(1)\cdot P_{_B}(t,1)}{\mathcal{K}\cdot\ln(1+\kappa)}}, \tag{10}$$

and then the theft ratio of data messages can be expressed as:

$$Tr(\tau^*,T)=\frac{1}{T}\cdot\sum_{t=1}^{T}\mathcal{E}(t,\tau^*). \tag{11}$$

C. Optimal Setting of $\mathcal{K}$

The value of $\mathcal{K}$ has a significant impact on the delivery ratio and theft ratio. Theorem 1 proves that a smaller delivery ratio or a smaller theft ratio will be obtained if each data message is encoded into more message pieces.

Theorem 1: A larger $\mathcal{K}$ gives rise to a smaller delivery ratio or a smaller theft ratio.

Proof: The first-order derivative of $\mathcal{R}(\tau^*)$ with respect to $\mathcal{K}$ is written as:

$$\frac{\mathbf{d}\mathcal{R}(\tau^*)}{\mathbf{d}\mathcal{K}}=c_2\cdot\int\frac{\mathbf{d}\mathcal{R}_a(\tau)}{\mathbf{d}\mathcal{K}}\mathbf{d}\tau\cdot e^{-\int\mathcal{R}_a(\tau)\mathbf{d}\tau}\Bigg|_{\tau=\tau^*}, \tag{12}$$

where

$$\frac{\mathbf{d}\mathcal{R}_a(\tau)}{\mathbf{d}\mathcal{K}}=\left\{\begin{array}{c}\left[\widetilde{P}_c\cdot\frac{4\pi\cdot{r_c}^3\cdot(1+\kappa)^{\tau-1}}{3|\boldsymbol{D}|}\right]^{\mathcal{K}}\\ \cdot\ln\left[\widetilde{P}_c\cdot\frac{4\pi\cdot{r_c}^3\cdot(1+\kappa)^{\tau-1}}{3|\boldsymbol{D}|}\right]\end{array}\right\}<0, \tag{13}$$

which indicates that $\frac{\mathbf{d}\mathcal{R}(\tau^*)}{\mathbf{d}\mathcal{K}}<0$.

Likewise, the first-order derivative of $Tr(\tau^*,T)$ with respect to $\mathcal{K}$ is expressed as:

$$\frac{\mathbf{d}Tr(\tau^*,T)}{\mathbf{d}\mathcal{K}}=\frac{1}{T}\cdot\sum_{t=1}^{T}c_3(t)\cdot\frac{\mathbf{d}\mathcal{E}_a(t,\tau)}{\mathbf{d}\mathcal{K}}\cdot e^{-\int\mathcal{E}_a(t,\tau)\mathbf{d}\tau}\Bigg|_{\tau=\tau^*}, \tag{14}$$

where

$$\frac{\mathbf{d}\mathcal{E}_a(t,\tau)}{\mathbf{d}\mathcal{K}}=N_e\cdot\left[\frac{\mathbf{d}\mathcal{R}_a(\tau)}{\mathbf{d}\mathcal{K}}\cdot P_{_B}(t,\tau)+\frac{\mathbf{d}P_{_B}(t,\tau)}{\mathbf{d}\mathcal{K}}\cdot\mathcal{R}_a(\tau)\right]. \tag{15}$$

Moreover, we obtain that $\frac{\mathbf{d}P_B(t,\tau)}{\mathbf{d}\mathcal{K}} < 0$, and thus there is $\frac{\mathbf{d}Tr(\tau^*,T)}{\mathbf{d}\mathcal{K}} < 0$. □

The conclusion of Theorem 1 suggests the theft ratio can be minimized when the obtained delivery ratio is equal to the required delivery ratio $\widetilde{\mathcal{R}}$. Hence, the optimal setting of $\mathcal{K}$ should satisfy that $\mathcal{R}(\tau^*) = \widetilde{\mathcal{R}} + \delta$, where δ is a compensation for rectifying the delivery ratio deviation caused by some factors, such as the randomness in the position distributions of nodes, and the signal irregularity of underwater communications. $\mathcal{K}$ is set according to the following formula:

$$\mathcal{K} = \max\left\{\mathcal{K}' \middle| \ \mathcal{R}(\tau^*) \geq \widetilde{\mathcal{R}} + \delta, \ \mathcal{K}' \in \mathbb{N}^+\right\}. \tag{16}$$

(16) implies that $\mathcal{K}$ can be set larger when the required delivery ratio is given smaller.

V. Message Piece Dissemination Approach

Message Piece Dissemination Approach (MPDA) is specially designed for the OUSN invaded by some silent eavesdroppers. In MPDA, each data message is encoded into $\mathcal{K}$ message pieces, and then the message pieces are encrypted by DES method.

At each time slot, the message pieces held by each piece holder are copied and disseminated to κ neighboring nodes. Upon receiving (or capturing) $\mathcal{K}$ different pieces of a data message, the sink node will recover the message pieces into the original data message, and the data message is delivered; the eavesdroppers attempt to decipher and decode the message pieces, and the data message is considered to be stolen when $\mathcal{K}$ different pieces are successfully deciphered.

A. Detailed Description of MPDA

Suppose a data message $\boldsymbol{m}$ generated by the source node v_s at the t-th absolute time slot, and then $\boldsymbol{m}$ needs to be disseminated from v_s to the sink node v_d. Each node maintains a list regarding the held message pieces. TABLE II provides some symbols used in the description of MPDA.

The operation of MPDA is described in terms of six stages: message encoding, piece encrypting, inquiring, replying, piece disseminating and piece list updating, as illustrated in Fig. 5, where the symbol $(t+\tau-1)^+$ denotes some (small) time after the start of the $(t+\tau-1)$-th absolute time slot, and $(t+\tau)^-$ denotes some (small) time before the end of $(t+\tau-1)$-th absolute time slot, such that there is $(t+\tau-1) < (t+\tau-1)^+ < (t+\tau)^- < (t+\tau)$.

TABLE II: Symbols in MPDA Description

Symbol	Description
m_k	k-th message piece of data message $\boldsymbol{m}$
e_n	n-th encryption key
$pie\_list(i)$	List of message pieces held by v_i
$\mathcal{H}(i)^{(t+\tau-1)}$	Set of neighboring nodes of v_i at the $(t+\tau-1)$-th absolute time slot
$\mathcal{M}(j)^{(t+\tau-1)}$	Set of message pieces held by the neighboring nodes of v_j at the $(t+\tau-1)$-th absolute time slot
$S_p(i, m_k)$	Potential receiver set of the message piece m_k which is disseminated from v_i

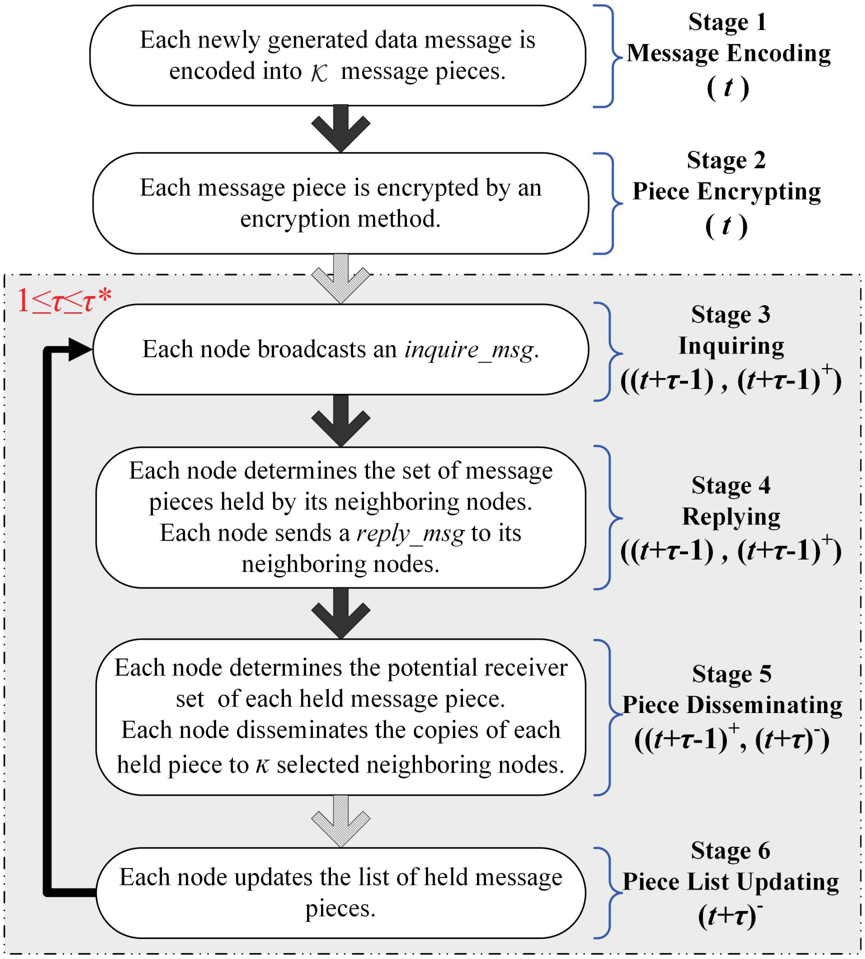

Each newly generated data message is encoded into $\mathcal{K}$ message pieces.
Stage 1
Message Encoding
(t)
Each message piece is encrypted by an encryption method.
Stage 2
Piece Encrypting
(t)
$1\le\tau\le\tau^*$
Each node broadcasts an *inquire_msg*.
Stage 3
Inquiring
$((t+\tau-1), (t+\tau-1)^+)$
Each node determines the set of message pieces held by its neighboring nodes. Each node sends a *reply_msg* to its neighboring nodes.
Stage 4
Replying
$((t+\tau-1), (t+\tau-1)^+)$
Each node determines the potential receiver set of each held message piece. Each node disseminates the copies of each held piece to κ selected neighboring nodes.
Stage 5
Piece Disseminating
$((t+\tau-1)^+, (t+\tau)^-)$
Each node updates the list of held message pieces.
Stage 6
Piece List Updating
$(t+\tau)^-$

Fig. 5: The stages of MPDA. There are six stages: message encoding, piece encrypting, inquiring, replying, piece disseminating, and piece list updating.

Stage 1. *Message Encoding*. At the t-th absolute time slot, the newly generated data message $\boldsymbol{m}$ is encoded into $\mathcal{K}$ message pieces $m_1, \cdots, m_k, \cdots, m_{\mathcal{K}}$ by the source node v_s.

Stage 2. *Piece Encrypting*. Each message piece of ***m*** is encrypted with an encryption key which is randomly selected from the encryption keys $e_1, \cdots, e_n, \cdots, e_{\mathcal{N}}$.

Stage 3. *Inquiring*. At the $(t+\tau-1)$-th absolute time slot (where $1 \le \tau \le \tau^*$), each node v_i broadcasts an $inquire\_msg$ including a quadruple $\big(v_i, t+\tau-1, C(i)^{(t+\tau-1)}, pie\_list(i)\big)$. Then, v_i determines the set of neighboring nodes on basis of the received $inquire_msg$s:

$$\mathcal{H}(i)^{(t+\tau-1)} = \left\{ v_j \middle| \, d(i,j)^{(t+\tau-1)} \le r_c \right\}. \tag{17}$$

Stage 4. *Replying*. On receiving the $inquire\_msg$ from v_i, each neighboring node v_j sends a $reply\_msg$ to v_i as a response, and the $reply\_msg$ includes a quadruple $\big(v_j, t+\tau-1, \mathcal{H}(j)^{(t+\tau-1)}, \mathcal{M}(j)^{(t+\tau-1)}\big)$, where $\mathcal{M}(j)^{(t+\tau-1)}$ is expressed as:

$$\mathcal{M}(j)^{(t+\tau-1)} = \bigcup \left\{ pie\_list(q) \middle| \, \forall v_q \in \mathcal{H}(j)^{(t+\tau-1)} \right\}. \tag{18}$$

Stage 5. *Piece Disseminating*. Suppose v_i holds a copy of the message piece m_k, and the potential receiver set of m_k is determined by:

$$S_p(i, m_k) = \left\{ v_j \middle| \, \forall v_j \in \mathcal{H}(i)^{(t+\tau-1)} \ \& \ m_k \notin pie\_list(j) \right\}. \tag{19}$$

With regard to a node $v_j \in S_p(i, m_k)$, the copy number of m_k in $\mathcal{M}(j)^{(t+\tau-1)}$ will be counted and sorted. Finally, the message piece m_k will be disseminated to κ neighboring nodes which are with the least copy numbers of m_k in their neighborhoods, and such mechanism can improve the delivery ratio of data messages because the copies of message pieces are disseminated evenly in the OUSN [26].

Stage 6. *Piece List Updating*. Suppose v_j has received the copy of m_k disseminated from v_i, and then the piece list of v_j will be updated by:

$$pie\_list(j) \leftarrow pie\_list(j) \bigcup m_k. \tag{20}$$

Above stages will be repeated until v_d receives $\mathcal{K}$ different pieces of ***m***, or the deadline of ***m*** (τ^* time slots) has been expired. If $\mathcal{K}$ different pieces have been delivered to v_d before the expiration of ***m***, an announcement originated from v_d will be broadcasted to all piece holders of ***m*** to stop the further dissemination. Note that the size of announcement message is very small and can be piggybacked with other messages. The pseudo-code of MPDA is given in Algorithm 1.

Algorithm 1 Pseudo-code of MPDA

```
Input: : $N$ mobile nodes, $\boldsymbol{D}$, $\tau^*$.
  A data message $\boldsymbol{m}$ is generated at the $t$-th absolute time slot.
  $\boldsymbol{m}$ is decoded into $\mathcal{K}$ different pieces.
  Each message piece of $\boldsymbol{m}$ is encrypted.
  $\tau \leftarrow 0$.
  while $\tau < \tau^*$ and $\boldsymbol{m}$ has not been delivered to $v_d$ do
    Each node interacts with neighboring nodes.
    for each message piece $m_k$ of $\boldsymbol{m}$ do
      for each node $v_i$ holds the message piece $m_k$ do
        Potential receiver set of $m_k$ is determined.
        $m_k$ is disseminated from $v_i$ to neighboring nodes in potential receiver set.
        if $v_j$ receives $m_k$ from $v_i$ then
          Piece list of $v_j$ is updated.
        end if
      end for
    end for
    $\tau \leftarrow \tau + 1$.
  end while
  if $\tau \leq \tau^*$ and $\mathcal{K}$ different pieces of $\boldsymbol{m}$ have been received by $v_d$ then
    $\boldsymbol{m}$ is delivered to $v_d$.
  end if
  Each node stops disseminating the message pieces of $\boldsymbol{m}$.
```

The message pieces are probably captured by eavesdroppers while the message pieces are being disseminated by the piece holders in Stage 5. As illustrated in Fig. 6, a piece holder sends a copy of m_k to a neighboring node, and an adjacent eavesdropper can capture the copy of m_k. When $\mathcal{K}$ different pieces of a data message have been captured by an eavesdropper, the eavesdropper will attempt to decipher the captured message pieces.

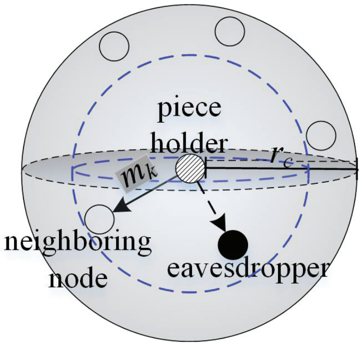


Fig. 6: A message piece captured by an eavesdropper. When a message piece is disseminated by a piece holder, the adjacent eavesdropper probably captures the message piece.

VI. Approach Analysis

A. Complexity of MPDA

TABLE III shows the message complexity and computational complexity of each stage in MPDA.

The messages of MPDA are mainly generated in Stage 3, Stage 4, and Stage 5. In Stage 3, each node broadcasts an $inquire\_msg$, and the message complexity is $\mathrm{O}(N)$; in Stage 4, each node sends a $reply\_msg$ to at most $\frac{\frac{4}{3}\pi\cdot{r_c}^3}{|\boldsymbol{D}|}\cdot N-1$ neighboring nodes, and therefore the number of $reply_msg$s reaches $\mathrm{O}(N^2)$ in the worst case; in Stage 5, each node disseminates the held message pieces to κ neighboring nodes. As a result, the message complexity of MPDA is written as $\mathrm{O}(N^2)$.

With regard to the computational complexity, in Stage 1 and Stage 2, the newly generated data messages are encoded and encrypted by source nodes, which results in $\mathrm{O}(N)$ computations; in Stage 3, each node determines the set of neighboring nodes according to the received $inquire_msg$s, and there is a total of $\mathrm{O}(N)$ computations; in Stage 4, each node merges the sets of held message pieces of neighboring nodes, and there are $\mathrm{O}(N^2)$ computations; in Stage 5, each node determines the potential receiver set for each held message piece, and the neighboring nodes are sorted according to the number of message pieces held by two-hop neighboring nodes, which gives rise to the computational complexity of $\mathrm{O}(N^2)$; in Stage 6, each node updates the list of held message pieces, and thus there are $\mathrm{O}(N)$ updates for all nodes. Therefore, the computational complexity of MPDA is $\mathrm{O}(N^2)$.

B. Expected Delivery Ratio

With regard to a message piece of a data message, there are $(1+\kappa)^{\tau^*}$ piece holders at the τ^*-th relative time slot, and thus the probability of the sink node receiving a copy of the message piece

TABLE III: Complexity of MPDA

Stage	Message Complexity	Computational Complexity
1	0	O(N)
2	0	O(N)
3	O(N)	O(N)
4	O(N^2)	O(N^2)
5	O(N^2)	O(N^2)
6	0	O(N)
Total	O(N^2)	O(N^2)

is written as $\frac{1}{N} \cdot (1+\kappa)^{\tau^*}$. Then, the probability of the sink node receiving $\mathcal{K}$ different pieces of the data message is written as $\left\{\frac{1}{N} \cdot (1+\kappa)^{\tau^*}\right\}^{\mathcal{K}}$, i.e., the expected delivery ratio of data messages is expressed as:

$$\widehat{\mathcal{R}}(\tau^*) = \left\{\frac{1}{N} \cdot (1+\kappa)^{\tau^*}\right\}^{\mathcal{K}}, \tag{21}$$

which implies that a larger κ or a smaller $\mathcal{K}$ will lead to a larger delivery ratio of data messages.

C. *Expected Theft Ratio*

In MPDA, each message piece is encrypted with a symmetrical encryption method and a randomly selected encryption key. Hence, the expected probability of a message piece being deciphered by an eavesdropper is written as $\frac{\sum_{n=1}^{\mathcal{N}} p_n}{\mathcal{N}}$.

Therefore, the expected theft ratio of data messages is approximatively expressed as:

$$\widehat{Tr}(\tau^*, T) = \left\{\frac{N_e}{N} \cdot (1+\kappa)^{\tau^*} \cdot \frac{\sum_{n=1}^{\mathcal{N}} p_n}{\mathcal{N}}\right\}^{\mathcal{K}}. \tag{22}$$

In (22), $(1+\kappa)^{\tau^*}$ denotes the copy number of each message piece after τ^* relative time slots. (22) suggests that a larger N_e or a smaller $\mathcal{K}$ leads to a larger theft ratio of data messages. Note that the value of $\mathcal{K}$ is also related to the required delivery ratio $\widetilde{\mathcal{R}}$, as depicted in (16).

VII. Simulations

In this section, MPDA is evaluated by observing the performance variations with respect to different parameters and by comparing with other algorithms (EF, BDCR, and CAR). We develop a simulator using ONE (Opportunistic Networks Environment) [27] to assess the performance of MPDA. ONE can generate the node mobility using different movement models and disseminate the data messages with various routing algorithms. The nodes are first evenly deployed into the underwater space, and then the nodes move according to the underwater mobility which is introduced in [25]. The inputs of our simulations include that: required delivery ratio, number of deadline time slots, number of nodes, number of copies of each message piece disseminated at each time slot, number of encryption keys, number of eavesdroppers. These inputs are integrated into the standard classes which are provided by the simulator ONE. Besides, the outputs of our simulations include that: number of message pieces, delivery ratio, theft ratio, and average energy consumption. The main parameter settings are shown in TABLE IV.

Note that there are various applications (or scenarios) of OUSNs, and some parameter settings may be much different in different applications, with different QoS requirements and with different capabilities of nodes. In our simulations, some vital parameter settings are cited from references, such as the communication range of nodes [28], the size of each data message [29], and the maximum autonomous speed of nodes [30].

A. Impacts of $\mathcal{K}$

The number of message pieces $\mathcal{K}$ is calculated by (16), and some numerical results are given in Fig. 7.

Fig. 7(a) indicates that a larger $\mathcal{K}$ will be output by (16) when a smaller $\widetilde{\mathcal{R}}$ or a larger τ^* is given. This is because the delivery ratio of data messages is enhanced when the message pieces are allowed to be disseminated within more time slots, and thus $\mathcal{K}$ can be set larger (each data message is encoded into more message pieces) to guarantee the same required delivery ratio $\widetilde{\mathcal{R}}$. On the contrary, a smaller $\widetilde{\mathcal{R}}$ is guaranteed more easily, which yields a larger $\mathcal{K}$ as well.

In Fig. 7(b), $\mathcal{K}$ increases with the increase of r_c, which is attributed to the fact that the sink node is more likely to receive the message pieces when each node is with a larger communication range, and each data message can be encoded into more message pieces under the constraint of $\widetilde{\mathcal{R}}$.

B. Delivery Ratio

The delivery ratio results are given in Fig. 8, and some observations are provided as follows:

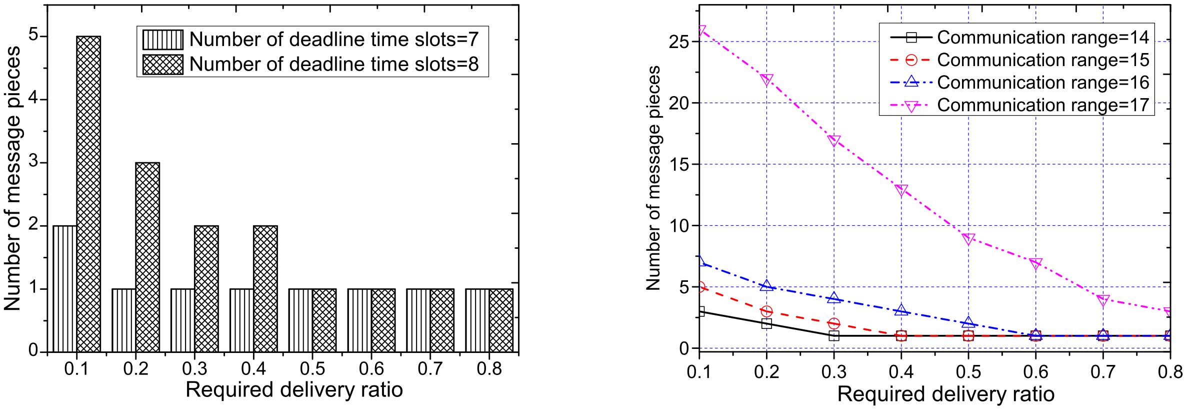
(*i*) In Fig. 8(a), the delivery ratio of data messages is increased with the continuous increase of $\widetilde{\mathcal{R}}$. The reason is that a smaller $\mathcal{K}$ is obtained due to a larger $\widetilde{\mathcal{R}}$, and the data messages could be

TABLE IV: Simulation Parameters

Parameter	Description	Value
N	Number of nodes	1,600
N_e	Number of eavesdroppers	3
$\|\boldsymbol{D}\|$	Size of deployment space	400×150×100 m^3
τ^*	Number of deadline time slots	8
T	Number of time slots in a observation period	200
r_c	Communication range of nodes	15 m [28]
r_0	Threshold of communication range between nodes	2 m
L_m	Size of each data message	500 B [29]
ρ	Probability of generating a data message at each time slot	0.05
c_1	Coefficient in signal irregularity formula	0.679
ζ	Exponent in signal irregularity formula	0.77
η	Exponent in signal irregularity formula	2
Ω_{min}	Minimum signal irregularity	0.1
Ω_{max}	Maximum signal irregularity	0.9
κ	Number of copies of each message piece disseminated at each time slot	2
$\mathcal{N}$	Number of encryption keys	6
p_n	Probability of deciphering the message piece encrypted with the n-th encryption key	0.25
$\widetilde{\mathcal{R}}$	Required delivery ratio	0.65
δ	Compensation for delivery ratio deviation	0.03
$\mathcal{V}_m$	Maximum autonomous speed	1.5 m/s [30]
τ_s	Duration of a time slot	6.02 s
$(v_x^{(0)}, v_y^{(0)}, v_z^{(0)})$	Initial velocity of water current	$(0.15, 0.2, 0.1)$ m/s
(K_x, K_y, K_z)	Coefficient of turbulent viscosity	$(0.5, 0.5, 1.0)$ m^2/s

delivered to sink node more easily when each data message is encoded into fewer message pieces. Besides, the bar with a larger τ^* is not always higher than that with a smaller τ^*, since a lager $\mathcal{K}$ will be obtained and applied in MPDA when the message pieces are allowed to be disseminated within more time slots, and thus the delivery ratio of data messages is accordingly cut down.

(*ii*) The delivery ratio of data messages grows rapidly with the increase of κ or N, as illustrated in Fig. 8(b). This is because a larger κ makes the message pieces be propagated much more quickly in the OUSN. Moreover, better relay nodes can be selected to improve the delivery ratio of data messages when the nodes are deployed more densely, and this phenomenon also indicates that MPDA exhibits a favorable scalability to the number of nodes. Especially, the delivery ratio of data messages reaches



(a) $\mathcal{K}$ vs. $\widetilde{\mathcal{R}}$ and τ^*

(b) $\mathcal{K}$ vs. $\widetilde{\mathcal{R}}$ and r_c

Fig. 7: Impacts of $\mathcal{K}$. A data message can be encoded into more message pieces when a smaller $\widetilde{\mathcal{R}}$, a larger τ^*, or a larger r_c is given.

0.985 when $N = 3,600$ and $\kappa = 3$.

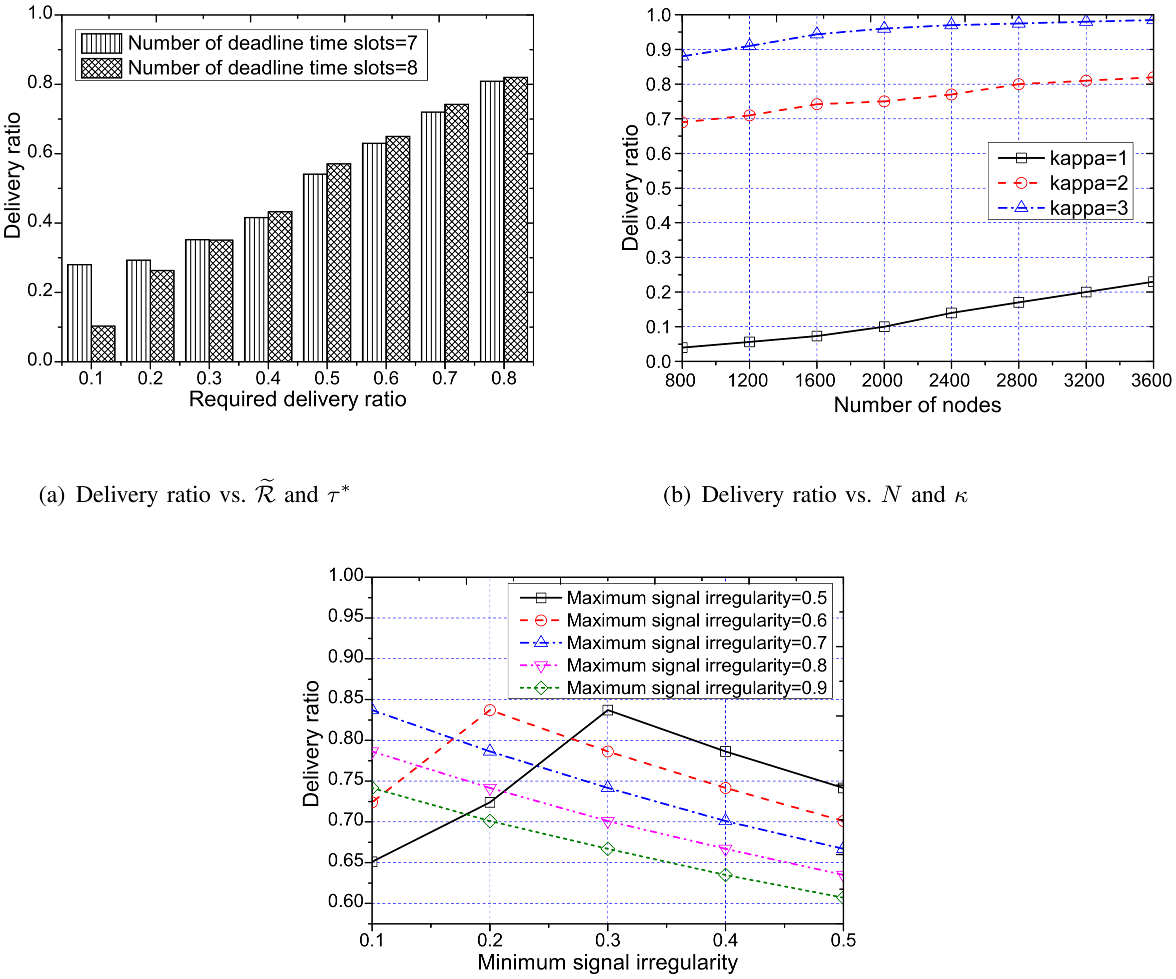
(iii) In Fig. 8(c), the obtained delivery ratio fluctuates with the variations of Ω_{min} and Ω_{max}, which is attributed to fact that the value of $\mathcal{K}$ is concerned with Ω_{min} and Ω_{max}, i.e., $\mathcal{K}$ becomes larger when the signal irregularity is smaller, although a smaller signal irregularity makes more potential communication links exist in the OUSN and enhances the delivery ratio of data messages. Note that MPDA can guarantee the obtained delivery ratio larger than the required delivery ratio as much as possible.

C. Theft Ratio and Average Energy Consumption

Similar to the phenomena in Fig. 8, in Fig. 9 the theft ratio of data messages increases with the increase of $\widetilde{\mathcal{R}}$ or N, and the theft ratio fluctuates with the variations of Ω_{min} and Ω_{max}.

Also, we find that the theft ratio of data messages will be reduced by providing more encryption keys for MPDA, as depicted in Fig. 9(a). However, in practical OUSN applications the nodes typically cannot deal with too many encryption keys, and the number of encryption keys is restricted by the computational power of nodes. Besides, the theft ratio of data messages is evidently raised when more eavesdroppers are dispatched by the enemy, as shown in Fig. 9(b).

Typically, the energy consumed on communications (message dissemination) is much larger than that on computations (message encoding and encrypting). The energy consumption is mainly deter-



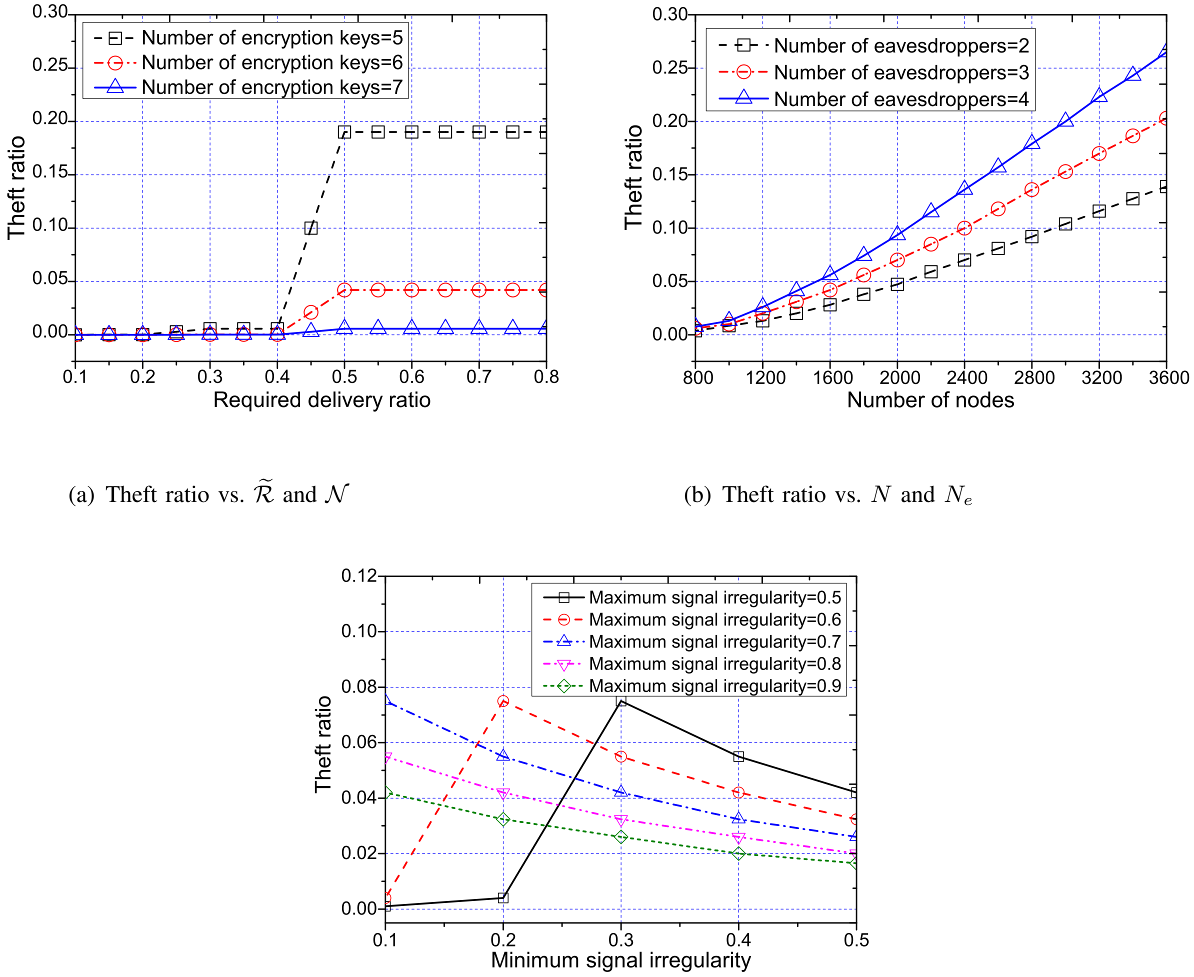
(a) Delivery ratio vs. $\widetilde{\mathcal{R}}$ and τ^*

(b) Delivery ratio vs. N and κ

(c) Delivery ratio vs. Ω_{max} and Ω_{min}

Fig. 8: Delivery ratio of data messages. The delivery ratio of data messages is increased with the increase of $\widetilde{\mathcal{R}}$, the increase of κ, or the increase of N.

mined by the message dissemination, which indicates that the energy consumption is closely related to the number of disseminated message pieces. In MPDA, the copy number of disseminated message pieces is restricted by the value of κ. The average energy consumption of each node is illustrated in Fig. 10, and two observations are obtained: (i) It is obvious that a larger average energy consumption is obtained with a larger κ, and this is because more copies of message pieces are disseminated with a larger κ. (ii) With the increase of N, the average energy consumption is gradually decreased, due the fact that the delivery ratio is increased with the increase of N (as shown in Fig. 8(b)), which implies that more data messages can be delivered during a shorter period and fewer copies of message



(a) Theft ratio vs. $\widetilde{\mathcal{R}}$ and $\mathcal{N}$

(b) Theft ratio vs. N and N_e

(c) Theft ratio vs. Ω_{max} and Ω_{min}

Fig. 9: Theft ratio of data messages. The theft ratio of data messages is increased with the increase of $\widetilde{\mathcal{R}}$ or the increase of N. Besides, the theft ratio of data messages can be reduced by providing more encryption keys.

pieces are disseminated. This phenomenon also exhibits a preferable scalability of MPDA in terms of energy consumption.

D. Algorithm Comparisons

To further analyze the merits of MPDA, we compare MPDA with other algorithms (EF, BDCR, and CAR) under the underwater mobility model introduced in [25]. EF adopts the epidemic dissemination manner, and the data messages held by each node will be disseminated to all the encountered nodes, which indicates that EF achieves the best delivery ratio and consumes the largest communication

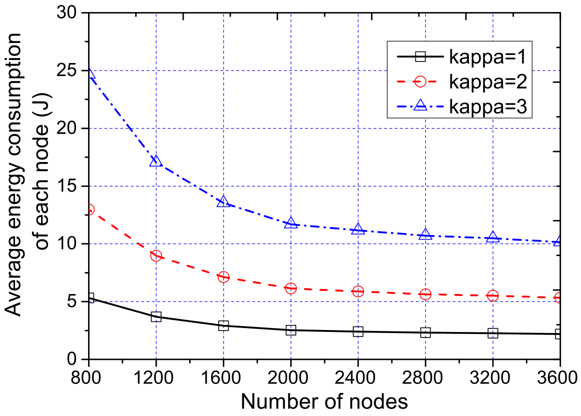


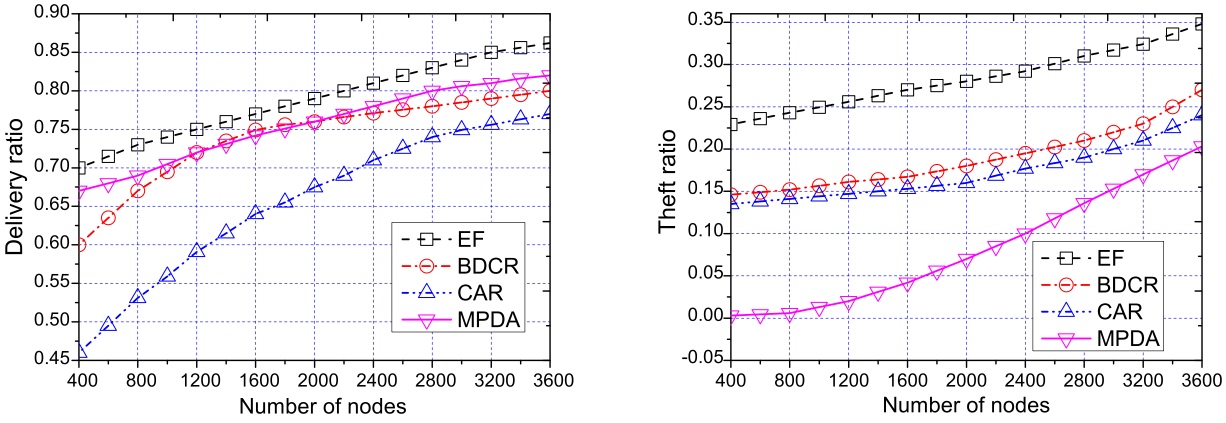
Fig. 10: Average energy consumption of each node. The average energy consumption is decreased with a smaller κ or a larger N.

cost. BDCR disseminates the data messages by exploiting the beam width and three-dimensional direction, and it can obtain a preferable delivery ratio. In CAR, each node holding a data message tries to avoid having a contact with adversaries, and the secure opportunistic paths are determined by integrating the delivery probability and the safety measurement.

These algorithms are compared in terms of delivery ratio and theft ratio, and the simulation results are provided in Fig. 11. Especially, we assume two-thirds of eavesdroppers can be identified and labeled in the simulations of CAR, while the eavesdroppers cannot be identified in the simulations of MPDA. However, the simulation results indicate that the performance of CAR is still seriously affected by the unidentified eavesdroppers (one-thirds of eavesdroppers).

We can observe that MPDA achieves a preferable delivery ratio of data messages compared with BDCR and CAR, although EF achieves the best delivery ratio through adopting the epidemic dissemination manner. However, EF is not suitable for most of OUSN applications due to the extremely large number of message copies, which could make the OUSN resource rapidly exhausted.

In particular, note that the theft ratio curve of MPDA is much lower than those of other algorithms, as shown in Fig. 11(b), and this is because in MPDA each data message is encoded into several message pieces, and the message pieces have been encrypted before the dissemination. Such mechanism makes the eavesdroppers difficult to capture and decipher all pieces of a data message, and thereby the theft ratio of MPDA is remarkably reduced.



(a) Delivery ratio

(b) Theft ratio

Fig. 11: Algorithm comparisons. The delivery ratio of MPDA is larger than those of BDCR and CAR, and MPDA always achieves the smallest theft ratio among these algorithms.

VIII. Conclusions

This study explores the message dissemination problem for OUSN invaded by some silent eavesdroppers. To reduce the theft ratio of data messages and guarantee the required delivery ratio of data messages, each data message is encoded into several message pieces, and the message pieces are encrypted before the dissemination. Besides, the optimal number of message pieces is analyzed mathematically and applied in our proposed MPDA. Simulation results demonstrate that MPDA can reduce the theft ratio of data messages as much as possible while it can guarantee the required delivery ratio of data messages, and MPDA is especially suitable for the OUSN confronted with the security threat of silent eavesdroppers. From the view point of industrial practices, our proposed MPDA can be taken as the routing logics and integrated into the network protocol software which is executed on nodes, and thus the data messages can be effectively protected in their dissemination processes.

The computational cost of encryption/decryption should be taken into account to make a preferable tradeoff between the theft ratio of data messages and the computational complexity. Furthermore, some threats have not been considered in this work: (i) The movement of eavesdroppers may be more intelligent than that of OUSN nodes, and the data messages could be purposefully stolen by eavesdroppers, e.g., some eavesdroppers can measure the dissemination importance of nodes, and then move around some vital nodes to capture more message pieces. Under such case, the nodes with large dissemination importance should be specially protected, and the message pieces held by these nodes could be relayed by some AUVs (Autonomous Underwater Vehicles). (ii) The environmental noises are ubiquitous especially in the shallow water, and the eavesdroppers could disguise them as underwater creatures by intentionally releasing some noises. The noises will alter the acoustic waves containing data messages or message pieces. However, the noises could be identified and exploited to protect the data messages or message pieces from being stolen by eavesdroppers. Our future research will focus on investigating these issues.

Data Availability Statement

The data used to support the findings of this study is available from the first author upon request.

Acknowledgments

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

References

[1] R. W. L. Coutinho, A. Boukerche, L. F. M. Vieira, and A. A. F. Loureiro, "EnOR: Energy Balancing Routing Protocol for Underwater Sensor Networks," *IEEE International Conference on Communications (ICC)*, pp. 574–582, Paris, France, 2017.

[2] L. Liu, R. Wang, G. Xiao, and D. Guo, "On the Throughput Optimization for Message Dissemination in Opportunistic Underwater Sensor Networks," *Computer Networks (Elsevier)*, vol. 169, pp. 1–16, 2020.

[3] R. Davis, M. Baumgartner, A. Comeau, and et al, "Tracking Whales on the Scotian Shelf using Passive Acoustic Monitoring on Ocean Gliders," *IEEE OCEANS'16*, Monterey, USA, 2016.

[4] B. G. Ferguson, and K. W. Lo, "Acoustic Detection, Localization, and Tracking of Tactical Autonomous Aerial and Underwater Vehicles," *Journal of the Acoustical Society of America*, vol. 140, no. 4, 2016.

[5] F. Li, and J. Wu, "LocalCom: A Community-based Epidemic Disseminating Scheme in Disruption-tolerant Networks," *IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks (IEEE SECON)*, pp. 574–582, Rome, Italy, 2009.

[6] J. Khurshid, and B. Hong, "Military Robots– A Glimpse from Today and Tomorrow," *8th Control, Automation, Robotics and Vision Conference*, pp. 771–777, Kunming, China, 2004.

[7] D. Zhao, H. Ma, S. Tang, and X. Li, "COUPON: A Cooperative Framework for Building Sensing Maps in Mobile Opportunistic Networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 26, no. 2, pp. 392–402, 2015.

[8] S. Zhang, and D. Li, "A Beam width and Direction Concerned Routing for Underwater Acoustic Sensor Networks," *2013 IEEE 9th International Conference on Mobile Ad-hoc and Sensor Networks*, pp. 17–24, Las Vegas, USA, 2013.

[9] R. W. L. Coutinho, A. Boukerche, L. F. M. Vieira, and A. A. F. Loureiro, "Performance Modeling and Analysis of Void-handling Methodologies in Underwater Wireless Sensor Networks," *Computer Networks (Elsevier)*, vol. 126, pp. 1–14, 2017.

[10] R. W. L. Coutinho, A. Boukerche, L. F. M. Vieira, and A. A. F. Loureiro, "Geographic and Opportunistic Routing for Underwater Sensor Networks," *IEEE Transactions on Computers*, vol. 65, no. 2, pp. 548–561, 2016.

[11] G. Han, L. Liu, N. Bao, J. Jiang, W. Zhang, and J. Rodriguesc, "AREP: An Asymmetric Link-based Reverse Routing Protocol for Underwater Acoustic Sensor Networks," *Journal of Network and Computer Applications (Elsevier)*, vol. 92, pp. 51–58, 2017.

[12] F. Ahmed, Z. Wadud, N. Javaid, N. Alrajeh, M. S. Alabed, and U. Qasim, "Mobile Sinks Assisted Geographic and Opportunistic Routing Based Interference Avoidance for Underwater Wireless Sensor Network," *Sensors*, vol. 18, no. 4, 2018.

[13] H. Arai, and M. Arai, "Erasure-Code-Based DTN Multi-Path Routing for Contact Avoidance," *IEEE 22nd Pacific Rim International Symposium on Dependable Computing (PRDC)*, Christchurch, New Zealand, 2017.

[14] D. Wu, F. Zhang, H. Wang, and R Wang, "Security-oriented opportunistic data forwarding in Mobile Social Networks," *Future Generation Computer Systems (Elsevier)*, vol. 87, pp. 803–815, 2018.

[15] K. Sakai, M. T. Sun, W. S. Ku, J. Wu, and T. H. Lai, "Multi-path Based Avoidance Routing in Wireless Networks," *IEEE 35th International Conference on Distributed Computing Systems (ICDCS)*, pp. 706–715, Columbus, USA, 2015.

[16] D. Coppersmith, "The Data Encryption Standard (DES) and Its Strength Against Attacks," *IBM Journal of Research and Development* , vol. 38, no. 3, pp. 243–250, 1994.

[17] T. Osuki, K. Sakai, and S. Fukumoto, "Contact Avoidance Routing in Delay Tolerant Networks," *IEEE Conference on Computer Communications (INFOCOM)*, Atlanta, USA, 2017.

[18] H. Tan, D. Choi, P. Kim, S. Pan, and I. Chung, "Secure Certificateless Authentication and Road Message Dissemination Protocol in VANETs," *Wireless Communications and Mobile Computing*, Article ID 7978027, 2018.

[19] A. Paranjothi, M. S. Khan, S. Zeadally, A. Pawar, and D. Hicks. "GSTR: Secure Multi-hop Message Dissemination in Connected Vehicles using Social Trust Model," *Internet of Things*, vol. 7, 2019.

[20] J. Chen, G. Mao, C. Li, and D. Zhang, "A Topological Approach to Secure Message Dissemination in Vehicular Networks," *IEEE Transactions on Intelligent Transportation Systems*, vol. 21, no. 1, pp. 135–148, 2020.

[21] F. Ayaz, Z. Sheng, D. Tian, G. Y. Liang, and V. Leung, "A Voting Blockchain based Message Dissemination in Vehicular Ad-Hoc Networks (VANETs)," *IEEE International Conference on Communications (ICC)*, Dublin, Ireland, 2020.

[22] Y. Qin, Y. Cao, W. Zhang, and S. Sun, "Research of Wireless Sensor Network Data Fusion Technology Based on RMSMTV," *4th International Conference on Information Science and Control Engineering (ICISCE)*, pp. 1622–1626, Changsha, China, 2017.

[23] G. Zhou, T. He, S. Krishnamurthy, and J. A. Stankovic, "Models and Solutions for Radio Irregularity in Wireless Senosr Networks," *ACM Transactions on Sensor Networks*, vol. 2, no. 2, pp. 221–262, 2006.

[24] M. Hussain, and N. Trigoni, "Distributed Localization in Cluttered Underwater Environments," *the Fifth ACM International Workshop on UnderWater Networks (WUWNet'10)*, Article no. 8, Massachusetts, USA, 2010.

[25] L. Liu, P. Wang, and R. Wang, "Propagation Control of Data Forwarding in Opportunistic Underwater Sensor Networks," *Computer Networks (Elsevier)*, vol. 114, pp. 80–94, 2017.

[26] L. Liu, R. Wang, and J. Wu, "On the Adaptive Data Forwarding in Opportunistic Underwater Sensor Networks Using GPS-Free Mobile Nodes," *Journal of Parallel and Distributed Computing (Elsevier)*, vol. 122, pp. 131–144, 2018.

[27] J. Dede, A. Förster, E. Hernández-Orallo, J. Herrera-Tapia, and et al, "Simulating Opportunistic Networks: Survey and Future Directions," *IEEE Communications Surveys & Tutorials* , vol. 20, no. 2, pp. 1547–1573, 2018.

[28] P. Goulet, C. Guinet, R. Swift, P. T. Madsen, and M. Johnson, "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.

[29] S. Zhang, L. Qian, M. Liu, Z. Fan, and Q. Zhang, "A Slotted-FAMA based MAC Protocol for Underwater Wireless Sensor Networks with Data Train," *Journal of Signal Processing Systems*, vol. 89, pp. 3–12, 2017.

[30] B. Reed, J. Leighton, M. Stojanovic, and F. Hover, "Multi-vehicle Dynamic Pursuit Using Underwater Acoustics," *Robotics Research*, vol. 114, pp. 79–94, 2016.

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, ACM TAAS, IEEE TSC, IEEE TVT, IEEE IoTJ, ACM TOIT, Computer Networks, Elsevier JPDC.

Houqian Zhang received the B. S. degree in computer science from the Wuhan University of Science and Technology in 2020. At present, he is a master student of Nanjing University of Posts and Telecommunications. His current research interest includes the areas of mobile opportunistic networks and electric vehicular networks.

Jiagao Wu received the Ph. D. degrees 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 interest includes the areas of mobile social networks and P2P networks.

Jia Xu received the M.S. degree in School of Information and Engineering from Yangzhou University, Jiangsu, China, in 2006 and the PhD. 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. He currently serves as the Publicity Co-Chair of SciSec 2021.