Hindawi
Security and Communication Networks
Volume 2018, Article ID 3729046, 13 pages
https://doi.org/10.1155/2018/3729046

Research Article

Secure Data Delivery with Linear Network Coding for Multiple Multicasts with Multiple Streams in Internet of Things

Lianmin Shi, Yihuai Wang, Zhengqing Wen, and Tao Peng

School of Computer Science and Technology, Soochow University, China

Correspondence should be addressed to Yihuai Wang; yihuaiw@suda.edu.cn

Received 15 January 2018; Accepted 2 May 2018; Published 13 June 2018

Academic Editor: Pedro Peris-Lopez

With the rapid developments of *Internet of Things* (IoT), tremendous number of sensors are deployed in the environment to monitor and collect different types of information. When a group of sensors located with the same location (or area) should deliver their data to a set of users and they have connected with the same network device, e.g., base station or access point, the data delivery between them and their users can be treated as a single source multicast in the core network from the network device connected with them to the network devices connected with their users. Generally, in such a case, multiple multicast sessions exist in the network simultaneously. In this paper, we study two major considerations, *i.e.*, transmission throughput and information security, for multiple multicasts with multiple streams in IoT by using *linear network coding* (LNC). Specifically, we jointly consider the transmission rate allocation, transmission topology selection, and secure LNC design for multiple multicasts to maximize the total *secure weighted throughput* (SWT), which is referred to as the *secure delivery for multiple multicasts with multiple streams* (SMMS) problem. To this end, we firstly consider the SMMS problem in the case that each sensor is connected with a fixed network device. We then study the SMMS problem when the source of each multicast can be selected from a set of nodes. For the first case, we formulate it to be a *linear programming* (LP), based on which we give the MORT algorithm to optimally solve it. On the other hand, for the second case, we first formulate it to be an *integer linear programming* (ILP) and then propose an efficient MBLP algorithm based on linear programming relaxation to obtain a suboptimal solution. Finally, we conduct extensive simulations to show the effectiveness and efficiency of the proposed algorithms.

1. Introduction

Internet of Things (IoT) has been widely studied and applied in the past ten years [1, 2]. In IoT shown in Figure 1, multiple sensor nodes are allocated in different areas and they can access the core network by connecting the base station located within their communication range. To analyze and further utilize the data information collected by these sensors, the data should be transmitted from these sensors to the different users. Transmission throughput and information security are two major considerations in IoT.

Network coding (NC) is a promising technology to be used in the next-generation network because it can maximize the throughput capacity of a network [3, 4]. By using NC, nodes in the network can encode and decode the received data packets instead of only store and forward. When the encoding and decoding are linear operations on a finite field, it is called *linear network coding* (LNC) [4]. For multiple multicast, LNC has been applied to improve the transmission throughput [5, 6].

Related studies have proved that LNC not only can make the multicast transmission reach the theoretical upper bound of throughput [7, 8] but also can provide information confidentiality due to its inherent characteristics [9]. Specifically, when applying LNC to multicast communication, the data information transmitted in the network is no longer the original data chunk, but the linear combination of original data chunks, which is called the *encoded packet*. If the attacker cannot receive enough encoded packets, it cannot obtain information about the original data chunk. In this condition, LNC becomes an effective way to resist passive attacks and provide secure data transmission without the key distribution protocols, which reduces the system complexity [10–18].

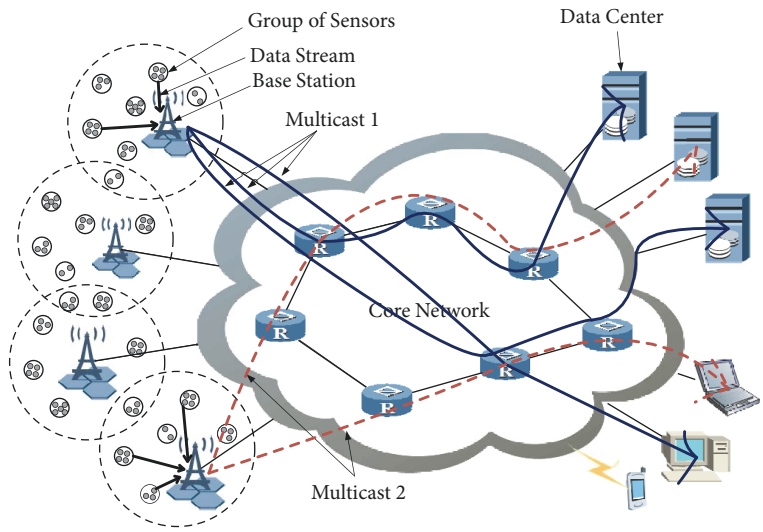


Figure 1: An example of IoT.

In order to provide data confidentiality, existing researches mainly focus on two different security requirements: *Information Theoretical Security* (ITS) [14, 15, 17, 18] and Weak Security (WS) [10–13]. ITS requires that any nonzero linear combination of original data chunks cannot be obtained by attackers. In order to achieve ITS, random information must be added to encode together with original data chunks during data transmission. On the other hand, WS does not allow any *meaningful information*, *e.g.*, the coded packets that can be generated by the original data packets of the same data stream be leaked to the attacker. We note that the data stream means a data flow in which all the data are collected by the same sensor.

In practice, a group of sensors with different types may be deployed at the same place to monitor the same area from different aspects [1, 2]. For example, a group of sensors, including temperature sensor, humidity sensor, PM2.5 sensor, and camera, may be placed at each place to monitor the same area and deliver their data information to a group of users, *e.g.*, meteorological department, military department, companies, and personal devices. Since the group of sensors is located at the same place, they connect to the same network device, *e.g.*, base station or access point. The data information sent from them must pass through the network device that they connected with; *i.e.,* the network device can be seen as the source of data information. Similarly, the network devices can be seen as the destinations of data information requested by the users connected with it. Therefore, the data delivery from each group of sensors located in the same place to a group of users can be seen as a single source multicast which is from the network device connected with them to the group of network devices connected with their users. Moreover, multiple data streams generated by the different sensors exist in the single source multicast. With the consideration of the limitation of the bandwidth capacity of the core network, when multiple single source multicasts exist, the transmission rate should be allocated for each data stream in each multicast to maximize the total throughput. We also give each data stream a weight to reflect the different requirements or importance.

In our previous study [19], we have considered the optimal transmission rate allocation and weakly secure LNC for single multicast scenario. In this paper, we will further study the multiple multicasts scenario and the source selection problem when the source of each multicast can be selected from a set of nodes. Next, we will give an example to show the differences between these two scenarios, *i.e.*, the achieved *secure weighted throughput* (SWT) in the cases of considering multiple multicasts individually and considering multiple multicasts together. In the following, we do not show the sensors and the users. Next, we give the examples to show the motivation and the importance of our research.

The core network G is given in Figure 2, in which nodes represent network devices, *e.g.*, base stations, access points, and routers, and they are connected by a wired core network. Specifically, there are two multicasts in this network; *i.e.*, source node s_1 sends data to the destination node set $T_1 = \{t_1, t_3\}$ and source node s_2 sends data to the destination node set $T_2 = \{t_2, t_4\}$. In addition, nodes v_1 and v_2 are assumed to be attackers in the network. The bandwidth capacity of each link is set to 1. In Figures 3(a)–3(d), we assume that there are two data streams sent by source s_1 which are denoted as x and y, and two data streams sent by source s_2 which are denoted as a and b, respectively. In particular, encoding operations are only done between the data with the same source [10, 11, 13, 15, 16]. We also assign a unit weight to each data stream. We should allocate the transmission rate of each data stream and design secure LNC scheme under the transmission rate allocation to maximize the total SWT. For example, in the network, if the transmission rate of data stream x is 2, it means the source node s_1 can send two packets of data stream x in one transmission round: x_1 and x_2. In addition, the coding coefficients of the LNC are chosen from the finite fields $\mathbb{F}_2$.

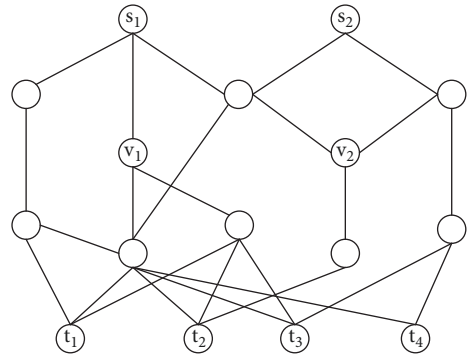


Figure 2: The network topology G (without showing the sensors and the users).

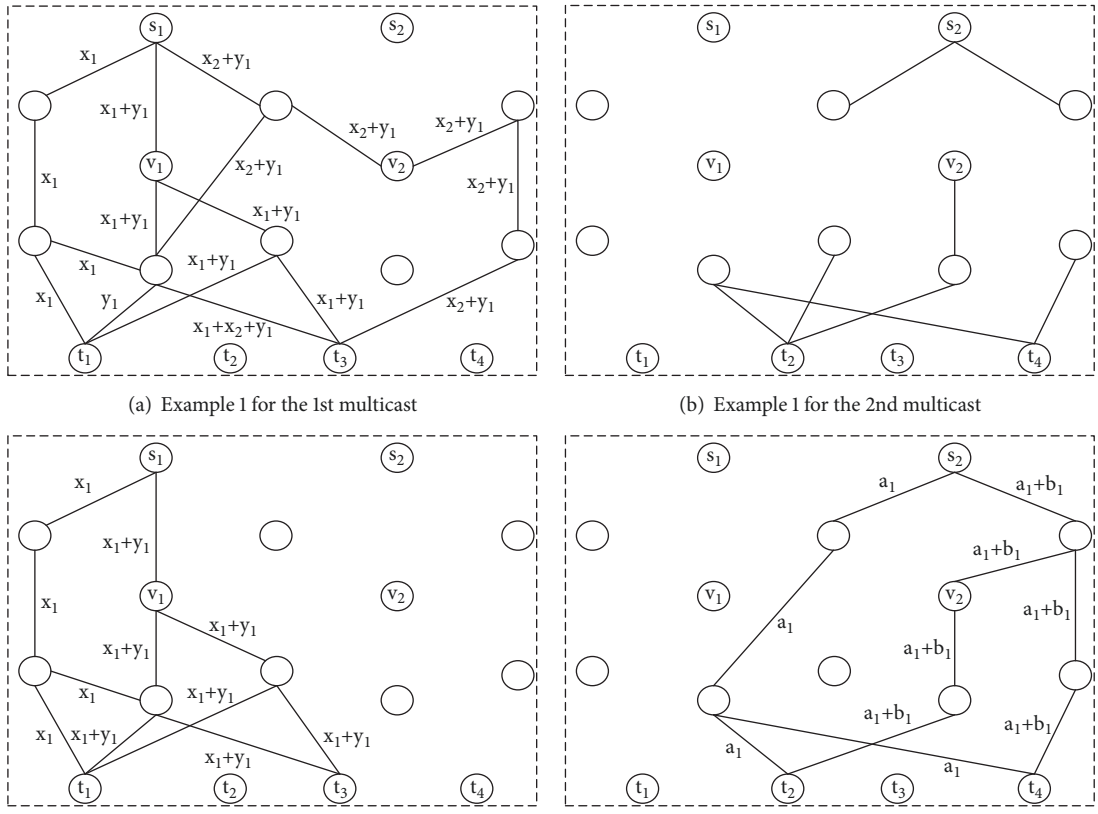


Figure 3: An example of secure multicast for multiple data streams.

Firstly, in the network G, when we consider each multicast individually, the maximum flow from source node s_1 to any destination node in T_1 is 3. Therefore, we can allocate the transmission rate 2 to data stream 1 and transmission rate 1 to data stream 2. The transmission topology and secure LNC of the first multicast are shown in Figure 3(a). Specifically, the destination t_1 can decode and recover x_1, $x_2 = (x_1+x_2+y_1)+(x_1+y_1)$ and $y_1 = x_1+(x_1+y_1)$. The destination t_3 can decode and recover $x_1 = (x_1+x_2+y_1)+(x_2+y_1)$, $x_2 = (x_1+x_2+y_1)+(x_1+y_1)$, and $y_1 = (x_1+x_2+y_1)+(x_1+y_1)+(x_2+y_1)$. Moreover, the attacker v_1 cannot obtain any nonzero coded data packet generated only by the data from the same stream, because it only receives one coded data packet $x_1 + y_1$. Although the maximum flow from source node s_2 to any destination node of T_2 in G is 2, since each link has unit bandwidth capacity, after the first multicast occupying the set of links shown in Figure 3(a), the maximum flow from source node s_2 to any destination node of T_2 is 0 in the remaining network topology which is shown in Figure 3(b). In this case, the total SWT of the two multicasts is $\mathbf{1} \times \mathbf{3} + \mathbf{1} \times \mathbf{0} = \mathbf{3}$.

Secondly, when we consider the two multicasts together to optimize the total SWT, the transmission topologies and secure LNCs of the two multicasts are shown in Figures 3(c) and 3(d), respectively. Specifically, for the first multicast, we

can allocate the transmission rate 1 to data stream 1 and transmission rate 1 to data stream 2. Both the destinations t_1 and t_3 can decode and recover x_1 and $y_1 = x_1 + (x_1 + y_1)$. For the second multicast, we can allocate the transmission rate 1 to data stream 1 and transmission rate 1 to data stream 2. Both the destinations t_2 and t_4 can decode and recover a_1 and $b_1 = a_1 + (a_1 + b_1)$. Moreover, the attackers v_1 and v_2 cannot obtain any nonzero coded data packet generated only by the data from the same stream. Therefore, in this case, the total SWT of the two multicasts is $\mathbf{1} \times \mathbf{2} + \mathbf{1} \times \mathbf{2} = \mathbf{4}$. Compared to the schemes shown in Figures 3(a) and 3(b), the SWT is improved by 33%.

From the above examples, we can conclude that, to maximize the total SWT, multiple multicasts should be considered together. Therefore, in this paper, we will consider the transmission rate allocation, transmission topology selection, and the secure LNC schemes for multiple multicasts to maximize the total SWT, which is referred to as the *secure delivery for multiple multicast with multiple streams* (SMMS) problem. To this end, we will firstly consider the SMMS problem in the case that each sensor is connected with a fixed network device; *i.e.*, each multicast has a fixed source. We then study the SMMS problem when the source of each multicast can be selected from a set of nodes; *i.e.*, multiple network devices can be selected for each sensor.

The rest of the paper is organized as follows. We first introduce the network model in Section 2. We then formulate the SMMS problem and design algorithms based on linear programming and its relaxations in Section 3. We then conduct extensive simulations to illustrate the performance of the proposed algorithms in Section 4. Finally, we conclude the paper in Section 5.

2. SMMS Problem Modeling

2.1. The Network Model. In this section, we first introduce the network model, important parameters, the multiple multicast network coding scheme, and the security model to be used in this paper. Secondly, we give the formal definition of the weakly secure linear multicast code. Finally, we formally define the *secure delivery for multiple multicasts with multiple streams* (SMMS) problem.

In this paper, we consider an IoT network consisting of sensors, network device, *e.g.*, base station, access point and routers, and end users, *e.g.*, departments, companies, and personal devices [1, 2]. We consider multiple groups of sensors which are deployed in different areas to monitor the environment. Each group is located at the same place and they connect to the same network device, *e.g.*, base station or access point. The data information sent from them must pass through the network device that they connected with; *i.e.,* the network device can be seen as the source of data information. Similarly, the network devices can be seen as the destinations of data information requested by the users connected with it. Consequently, the data delivery from each group of sensors located in the same place to a group of users can be seen as a single source multicast which is from the network device connected with them to the group of network devices connected with their users. Therefore, in the following, we only consider multicasts within the wired core network. Moreover, multiple data streams generated by the different sensors exist in the single source multicast. With the consideration of the limitation of the bandwidth capacity of the core network, when multiple single source multicasts exist, the transmission rate should be allocated for each data stream in each multicast to maximize the total throughput.

We use a directed graph $G = (V, E)$ to present the wired core network, where V is the set of nodes and E is the set of links. Firstly, we assume that there are H multicasts in G and the source node of the h^{th} multicast is denoted as $s_h \in V, h \in \{1, \dots H\}$. Let $S = \{s_1, \cdots, s_H\}$. The set of destinations of h^{th} multicast is denoted as T_h. Let $T = \bigcup_{h=1}^{H} T_h = \{t_1, \cdots, t_N\}, T \subset V$. The h^{th} multicast session can be expressed as (s_h, T_h). Specifically, the source s_h actually represents the group of sensors which connect to s_h and has the set of destinations T_h. If the number of sensors in the group is L_h, then there are a total of L_h data streams in multicast (s_h, T_h), each of which is generated (or sent) by a sensor node. The total transmission rates of the first l^{th} data streams are denoted as D_l^h and the transmission rate of the l^{th} stream is $D_l^h - D_{l-1}^h$ and $D_0^h = 0$. Specifically, these L_h data streams can be sent from s_h to T_h at different transmission rates in each transmission round.

In particular, for the l^{th} data stream of the h^{th} multicast, we define its weight as $\omega_l^h > 0, \forall h \in \{1, \cdots, H\}, \forall l \in \{1, \cdots, L_h\}$. The weights reflect different requirements or importance. In addition, for $\forall e_{u,v} \in E$, it has a certain bandwidth capacity $c_{u,v}$. For convenience, the important symbols are defined as shown in Table 1.

2.2. Linear Network Coding for Multiple Multicast. In this paper, the encoding operations are performed only between different data packets of streams of the same multicast [10, 11, 13, 15], which means data streams from different multicasts will not be encoded together. We define the set of original data packets sent by the source node s_h as $\mathbf{M}_h = [m_{1,1}^h, m_{1,2}^h, \dots, m_{1,D_1^h}^h, m_{2,1}^h, \dots, m_{L_h,1}^h, \dots, m_{L_h,D_{L_h}^h - D_{L_h-1}^h}^h]^T, \forall h \in \mathcal{H}$. Therefore, in a transmission round, the set of original data packets for the l^{th} data stream sent from the source node s_h can be defined as $\mathbf{M}_{h,l} = [m_{l,1}^h, m_{l,2}^h, \dots, m_{l,D_l^h - D_{l-1}^h}^h]^T$.

Although multiple multicasts share the capacity of each link, only the data packets belonging to the same multicast will be encoded together. Therefore, when the transmission rate allocation and the transmission topology have been obtained, the LNC scheme for each multicast session can be designed individually. $\forall e_{u,v} \in E$, if there is a coded packet m_h from the multicast (s_h, T_h) passing through it, we can use a $D_{L_h}^h$-dimensional row vector $\mathbf{f}(e_{u,v}, h)$ to represent the *global encoding vector* (GEV) of the coded packet as long as $m_h = \mathbf{f}(e_{u,v}, h)\mathbf{M}_h$. In addition, the LNC design is implemented in a finite field $\mathbb{F}_q$ with size q, which means all elements of the GEVs are taken from the finite field $\mathbb{F}_q$. In particular, for an original data packet from multicast (s_h, T_h), its GEV is a row of the $D_{L_h}^h \times D_{L_h}^h$-dimensional identity matrix. We denote the

Table 1: Symbol definition.

Symbol	Definition
Bold Font	Linear spaces, matrixes and vectors
Symbol^T	Transpose of a matrix or vector
$Rank(\mathbf{B})$	The rank of a matrix or a vector set $\mathbf{B}$
$\mathbb{F}_q$	The finite field with size q
$e_{u,v}$	Directed link from node u to node v
$c_{u,v}$	Bandwidth capacity of link $e_{u,v}$
$\mathbf{A}_i$	The set of global encoding vectors received by intermediate node v_i
$\mathscr{H}$	$\mathscr{H} = \{1, \cdots, H\}$
$\mathscr{L}_h$	$\mathscr{L}_h = \{1, \cdots, L_h\}, \forall h \in \mathscr{H}$
D_l^h	The sum of the transmission rates of the first l^{th} data streams in the h^{th} multicast

set of links entering node v as $In(v)$ and the set of links leaving node v as $Out(v)$. For the source node $s_h \in S, \forall h \in \mathscr{H}$, it is assumed that $In(s_h)$ constitutes $D_{L_h}^h$ virtual links, and each virtual link represents an original data packet of the multicast.

Therefore, for multicast $(s_h, T_h), \forall h \in \mathscr{H}$, the $D_{L_h}^h$-dimensional linear multicast code $\phi(G, \mathbb{F}_q, s_h, T_h, L_h, H)$ can be defined as follows.

Definition 1. $\forall h \in \mathscr{H}$, the $D_{L_h}^h$-dimensional linear multicast code $\Phi(G, \mathbb{F}_q, s_h, T_h, L_h, H)$ exists if the following three conditions are satisfied:

(1) For the source $s_h \in S$ in multicast (s_h, T_h), $\bigcup_{e \in In(s_h)} \{\mathbf{f}(e, h)\}$ consists of the basis of the vector space $\mathbb{F}_q^{D_{L_h}^h}$.

(2) $\forall e_{v,w} \in Out(v)$, $\mathbf{f}(e_{v,w}, h)$ is a linear combination of $\bigcup_{e_{u,v} \in In(v)} \{\mathbf{f}(e_{u,v}, h)\}, \forall v \in V$.

(3) For each destination $t, \forall t \in T_h$ in multicast (s_h, T_h), $\bigcup_{e_{u,t} \in In(t)} \{\mathbf{f}(e_{u,t}, h)\}$ consists of the basis of the vector space $\mathbb{F}_q^{D_{L_h}^h}$.

The above definition shows that (1) for $s_h \in S, \forall h \in \mathscr{H}$, all the coded data packets transmitted in the network which related to multicast (s_h, T_h) can be generated by it; (2) $\forall v \in V$, all the coded data packets sent out from it can be generated by linearly combining the coded data packets received from its incoming links; (3) for $t \in T_h, \forall h \in \mathscr{H}$, it can decode the received coded packets for the original data of all the L_h streams. In addition, $\forall h \in \mathscr{H}$, if the destination node in the multicast (s_h, T_h) receives $D_{L_h}^h$ linearly independent coded packets, it can decode and obtain $D_{L_h}^h$ original data packets. For example, suppose that the matrix $\mathbf{M}_h'$ is composed of coded data packets as its rows and the matrix $\mathbf{A}_h$ is composed of the corresponding GEVs as its rows, then we have $\mathbf{A}_h \mathbf{M}_h = \mathbf{M}_h'$. Therefore, the destination node can decode and obtain the original data packets by $\mathbf{M}_h = \mathbf{A}_h^{-1} \mathbf{M}_h'$. Additionally, $\forall v_i \in V$, let $\mathbf{A}_{h,i} = \{\mathbf{f}(e, h) \mid e \in In(v_i), h \in \mathscr{H}\}$.

2.3. Security Model. We assume that, in G, there exists a set of inside passive attackers $\overline{I}, \overline{I} = V - S - T \subseteq I$, each of which tries to acquire *meaningful* information of original data by collecting the data packets passing through them individually [10] (similar to the attack model considered in [11, 13–15, 19]).

For the secure requirement, we consider the *Weak Security* (WS) [10] in this paper, which has been widely studied in the literature [11–13, 19]. Since only the data packets belonging to the same multicast can be encoded together, the WS requirements should be satisfied for each multicast. Let $\mathbf{B}_{h,i}$ be the matrix consisting of nonzero vectors in $\mathbf{A}_{h,i}$ as its row vectors. For the above-mentioned attack model and multiple multicast models with multiple data streams, the weakly secure linear multicast code can be defined as follows.

Definition 2. $\forall h \in \mathscr{H}$, the $D_{L_h}^h$-dimensional linear multicast code $\Phi(G, \mathbb{F}_q, s_h, T_h, L_h, H)$ constructed on the finite field $\mathbb{F}_q$ with size q is weakly secure, if it satisfies that for any malicious node $v_i \in \overline{I}$:

$$H\left(\mathbf{M}_{h,l} \mid \mathbf{B}_{h,i} \mathbf{M}_h\right) = H\left(\mathbf{M}_{h,l}\right), \quad \forall l \in \mathscr{L}_h \tag{1}$$

Equation (1) shows that $\forall h \in \mathscr{H}, \forall l \in \mathscr{L}_h$ and $\forall i$, $\mathbf{M}_{h,l}$ and $\mathbf{B}_{h,i} \mathbf{M}_h$ are independent with each other. Any malicious node cannot obtain a nonzero linear combination of original data packets from the same data stream of the same multicast.

Definition 3. $\forall h \in H$, if the $D_{L_h}^h$-dimensional linear multicast code $\omega(G, \mathbb{F}_q, s_h, T_h, L_h, H)$ constructed on the finite field $\mathbb{F}_q$ with size q satisfies weakly secure requirements, then it is weakly secure for the multicast (s_h, T_h).

For the multicast (s_h, T_h), the LNC can achieve the requirements of WS when $L_h > 1$. This is because the original data packets from one data stream of the multicast can be encoded with the original data packets from the other data streams of the multicast to hide the information of the original data packet of the same stream.

Table 2: Parameters and decision variables.

Symbol	Definition
$\mathbf{J}(v)$	the set of all the links entering node v, $\mathbf{J}(v) = \{u \mid e_{u,v} \in In(v)\}$
$\bar{\mathbf{J}}(v)$	the set of all the links leaving node v, $\bar{\mathbf{J}}(v) = \{w \mid e_{v,w} \in Out(v)\}$
$x_{u,v}^{h,t}$	the data flow of multicast (s_h, T_h) transmitted on link $e_{u,v}$ heading for destination node t, $\forall h \in \mathcal{H}, \forall t \in T_h, \forall e_{u,v} \in E$
$y_{u,v}^{h}$	the actual data flow of multicast (s_h, T_h) transmitted on link $e_{u,v}$, $\forall h \in \mathcal{H}$
$b_v^{h,t}$	The difference of data flow of multicast (s_h, T_h) between the data flow entering and leaving node v, which heading for destination node t, $\forall h \in \mathcal{H}$

2.4. SMMS Problem Description. In this paper, we will study the problem of secure delivery *for multiple multicasts with multiple streams* (SMMS).

Definition 4. For a given network G, a malicious node set $\bar{I}$ and H multicasts, each of which has a source node s_h, a set of destination node T_h, and L_h data streams, secure delivery for multiple multicast with multiple streams (SMMS) problem is to consider the transmission rate allocation, transmission topology selection, and the secure LNC schemes for multiple multicasts to maximize the total SWT.

3. Problem Formulation and Algorithm Design

In this section, we will firstly study the SMMS problem for multiple multicasts scenario when each multicast has a fixed source node. We then further consider the SMMS problem for multiple multicasts when the source of each multicast can be selected from a set of nodes in G.

3.1. The SMMS Problem with Fixed Source. For single multicast, in our previous work [19], we have shown that the sufficient and necessary condition. Specifically, in the SMMS problem, the condition that a secure linear multicast code exists for multicast (s_h, T_h) is that (1) there exists a network flow F_h with capacity $D_{L_h}^h$ between s_h and each destination in T_h, and (2) for each malicious node $v_i \in \bar{I}$, the actual data flow of F_h that enters v_i should not be more than $D_{L_h}^h - \max_{l \in \mathcal{L}_h}\{D_l^h - D_{l-1}^h\}$.

For H multicasts simultaneously transmitted in the network G, we next formulate the SMMS problem when each multicast has a fixed source node. Before building a mathematical programming for the SMMS problem, we firstly define new parameters and decision variables, as shown in Table 2.

We can formulate a mathematical programming for the SMMS problem as follows:

$$\mathbf{MP}: \mathbf{Maximize}: \quad \sum_{h \in \mathcal{H}} \sum_{l \in \mathcal{L}_h} \omega_l^h \left(D_l^h - D_{l-1}^h\right), \tag{2}$$

$$\text{s.t.} \quad D_l^h - D_{l-1}^h > 0, \quad \forall h \in \mathcal{H},\ \forall l \in \mathcal{L}_h \tag{3}$$

$$b_v^{h,t} = \sum_{u \in \mathbf{J}(v)} x_{u,v}^{h,t} - \sum_{w \in \bar{\mathbf{J}}(v)} x_{v,w}^{h,t}, \quad \forall h \in \mathcal{H},\ \forall t \in T_h,\ \forall v \in V \tag{4}$$

$$b_{S_h}^{h,t} = -D_{L_h}^h, \quad \forall h \in \mathcal{H},\ \forall t \in \mathcal{T}_h \tag{5}$$

$$b_t^{h,t} = D_{L_h}^h, \quad \forall h \in \mathcal{H},\ \forall t \in \mathcal{T}_h \tag{6}$$

$$b_v^{h,t} = 0, \quad \forall h \in \mathcal{H},\ \forall t \in \mathcal{T}_h,\ \forall v \in V - \{s_h, t\} \tag{7}$$

$$y_{v,w}^h \geq \max_{t \in T_h}\left\{x_{v,w}^{h,t}\right\}, \quad \forall h \in \mathcal{H},\ \forall v \in V,\ \forall w \in \bar{\mathbf{J}}(v) \tag{8}$$

$$\sum_{u \in \mathbf{J}(v)} y_{u,v}^h \leq D_{L_h}^h - \max_{l \in \mathcal{L}_h}\left\{D_l^h - D_{l-1}^h\right\}, \quad \forall h \in \mathcal{H},\ \forall v \in \bar{I} \tag{9}$$

$$\sum_{h \in \mathcal{H}} y_{v,w}^h \leq c_{v,w}, \quad \forall v \in V,\ \forall w \in \bar{\mathbf{J}}(v) \tag{10}$$

$$x_{v,w}^{h,t} \geq 0, \quad \forall h \in \mathcal{H},\ \forall t \in \mathcal{T}_h,\ \forall v \in V,\ \forall w \in \bar{\mathbf{J}}(v) \tag{11}$$

$$D_l^h \geq 0, \quad \forall h \in \mathcal{H},\ \forall l \in \mathcal{L}_h \tag{12}$$

$$D_0^h = 0, \quad \forall h \in \mathcal{H} \tag{13}$$

The meanings of the objective and the constraints in the above mathematical programming **MP** are shown in Table 3.

Because of the existence of the nonlinear constraints (8)-(9) in **MP**, it cannot be solved directly. Therefore, next, we will equally transform the mathematical programming problem into a *linear programming* (LP) problem. Specifically, the nonlinear constraints (8)-(9) in **MP** can be replaced by the following constraints:

Table 3: The meanings of objectives and constraints.

Constraint	Meaning
Objective(2)	Maximize the total SWT
Constraint(3)	The transmission rate of any data stream transmitted in the network must be greater than 0
Constraints(4)–(7)	In network topology, nodes need to follow the network flow constraints
Constraint(8)	For multicast (s_h, T_h), the actual flow rate passing through any link in the network is no less than the flow rate passing through the link to any destination node because the coded data packets can be useful for all the destinations in T_h with LNC
Constraint(9)	The data flow of multicast (s_h, T_h) passing through any malicious node in the network should meet the requirements of WS
Constraint(10)	The sum of all data flows passing through the link should be no greater than the bandwidth capacity of the link
Constraints(11)–(13)	Ranges of variables

$$y_{v,w}^h \geq x_{v,w}^{h,t}, \quad \forall h \in \mathscr{H},\ \forall t \in T_h,\ \forall v \in V,\ \forall w \in \bar{\mathbf{J}}(v) \tag{14}$$

$$p_v^h \geq D_l^h - D_{l-1}^h, \quad \forall h \in \mathscr{H},\ \forall l \in \mathscr{L}_h,\ \forall v \in \bar{I} \tag{15}$$

$$\sum_{u \in \mathbf{J}(v)} y_{u,v}^h \leq D_{L_h}^h - p_v^h, \quad \forall h \in \mathscr{H},\ \forall v \in \bar{I} \tag{16}$$

Firstly, the constraint (14) is used to replace the constraint (8). Specifically, the constraint (14) is equivalent to $y_{v,w}^h \geq \max_{t \in T}\{x_{v,w}^{h,t}\}$.

Secondly, the constraint (9) can be equally transformed into constraints (15)-(16). For $\forall h \in \mathscr{H}$, $\forall v_i \in \bar{I}$, if the constraints (15)-(16) are satisfied together, we can get $\sum_{u \in \mathbf{J}(v)} y_{u,v}^h \leq D_{L_h}^h - p_v^h \leq D_{L_h}^h - \max_{l \in \mathscr{L}_h}\{D_l^h - D_{l-1}^h\}$ which means that the solution also satisfies the constraint (9). On the other hand, $\forall h \in \mathscr{H}$, $\forall v_i \in \bar{I}$, if there is a solution of $y_{u,v}^h$ satisfying the constraint (9), then there must be a set of values of $p_v^h = \max_{l \in \mathscr{L}_h}\{D_l^h - D_{l-1}^h\} \geq D_l^h - D_{l-1}^h$ which makes the value of $y_{u,v}^h$ satisfy the constraint (16). Thus, with the linearization process, the optimal solution of **MP** will not be changed.

Therefore, the nonlinear programming **MP** can be transformed into the following *linear programming* (LP) $\mathbf{MP}_1$:

$$\mathbf{MP}_1 : \mathbf{Maximize} : \sum_{h \in \mathscr{H}} \sum_{l \in \mathscr{L}_h} \omega_l^h \left(D_l^h - D_{l-1}^h\right) \quad \text{s.t.} \quad \text{constraints (3)–(7), (10)–(16).} \tag{17}$$

The above LP $\mathbf{MP}_1$ can be solved efficiently. The obtained solution gives the transmission rate allocation, *i.e.*, $\{D_l^h \mid l \in \mathscr{L}_h\}$, and transmission topology, *i.e.*, $\{y_{u,v}^h \mid e_{u,v} \in E\}$, for each multicast h. Based on the transmission rate allocation and transmission topology for each multicast (s_h, T_h), H secure linear multicast codes can be designed individually [19] to achieve the maximum total SWT given by the objective (2). We refer to the algorithm based on LP $\mathbf{MP}_1$ to find the transmission rate allocation and transmission topology for H multicasts as the *optimal rate allocation and transmission topology selection for multiple multicasts* (MORT) algorithm.

3.2. The SMMS Problem with Source Selection. In the above subsection, we have considered the SMMS problem in the case that each group of sensors is connected with a fixed network device; *i.e.*, each multicast has a fixed source. In this subsection, we will further study the SMMS problem in the case that each group of sensors can decide to connect to a network device; *i.e.*, the source of each multicast can be selected from a set of nodes. Specifically, it means that the source of multicast in core network is different when each group of sensors selects different network devices. Obviously, such source selection will have impacts on the total SWT when multiple multicasts exist in the network. Based on the knowledge that the set of network devices can be selected for each group of sensors, for each multicast, we will select one node as the source node of the multicast in the core network. In the following, we firstly model the problem as a mathematical programming. Then, by linearizing the mathematical programming, we have *integer linear programming* (ILP) algorithm. Finally, we design an efficient *Multicast Based on LP-Relaxation* (MBLP) algorithm based on linear programming relaxation. We firstly define new parameters and decision variables as shown in Table 4.

We can formulate the SMMS problem with source selection as follows:

$$\mathbf{MP}' : \mathbf{Maximize} : \sum_{h \in \mathscr{H}} \sum_{l \in \mathscr{L}_h} \omega_l^h \left(D_l^h - D_{l-1}^h\right) \tag{18}$$

$$\text{s.t.} \quad D_l^h - D_{l-1}^h > 0, \quad \forall h \in \mathscr{H},\ \forall l \in \mathscr{L}_h \tag{19}$$

$$b_v^{h,k,t} = \sum_{u \in \mathbf{J}(v)} x_{u,v}^{h,k,t} - \sum_{w \in \bar{\mathbf{J}}(v)} x_{v,w}^{h,k,t}, \quad \forall h \in \mathscr{H},\ \forall k \in \mathscr{K}_h,\ \forall t \in T_h,\ \forall v \in V \tag{20}$$

$$-Z_k^h \pi \leq b_{s_k^h}^{h,k,t} \leq 0, \quad \forall h \in \mathscr{H},\ \forall k \in \mathscr{K}_h,\ \forall t \in T_h \tag{21}$$

Table 4: Parameters and decision variables.

Symbol	Definition
s_k^h	The k^{th} node can be selected as source of the h^{th} multicast, $s_k^h \in V$
$\mathcal{K}_h$	$\{1, \cdots, K_h\}$, in which K_h is the number of source nodes can be selected for the h^{th} multicast
$x_{u,v}^{h,k,t}$	The data flows passing through link $e_{u,v}$, sent from source node s_k^h to the destination node t
$y_{u,v}^{h,k}$	The actual data flows passing through link $e_{u,v}$, sent from source node s_k^h
$b_v^{h,k,t}$	The difference between the data flows entering and leaving node v, sent from source node s_k^h to destination node t
π	A sufficient large number
Z_k^h	A $0-1$ decision variable, which denotes whether the source node s_k^h is selected for the h^{th} multicast or not

$$\sum_{k \in \mathcal{K}_h} b_{s_k^h}^{h,k,t} = -D_{L_h}^h, \quad \forall h \in \mathcal{H},\ \forall t \in T_h \tag{22}$$

$$0 \le b_t^{h,k,t} \le Z_k^h \pi, \quad \forall h \in \mathcal{H},\ \forall k \in \mathcal{K}_h,\ \forall t \in T_h \tag{23}$$

$$\sum_{k \in \mathcal{K}_h} b_t^{h,k,t} = D_{L_h}^h, \quad \forall h \in \mathcal{H},\ \forall t \in T_h \tag{24}$$

$$b_v^{h,k,t} = 0, \quad \forall h \in \mathcal{H},\ \forall k \in \mathcal{K}_h,\ \forall t \in T_h,\ \forall v \in V - \left\{s_k^h, t\right\} \tag{25}$$

$$y_{v,w}^{h,k} \ge \max_{t \in T_h} \left\{x_{v,w}^{h,k,t}\right\}, \quad \forall h \in \mathcal{H},\ \forall k \in \mathcal{K}_h,\ \forall v \in V,\ \forall w \in \bar{\mathbf{J}}(v) \tag{26}$$

$$\sum_{u \in \mathbf{J}(v)} \sum_{k \in K_h} y_{u,v}^{h,k} \le D_{L_h}^h - \max_{l \in \mathcal{L}_h} \left\{D_l^h - D_{l-1}^h\right\}, \quad \forall h \in \mathcal{H},\ \forall v \in \bar{I} \tag{27}$$

$$\sum_{h \in \mathcal{H}} \sum_{k \in \mathcal{K}_h} y_{v,w}^{h,k} \le c_{v,w}, \quad \forall v \in V,\ \forall w \in \bar{\mathbf{J}}(v) \tag{28}$$

$$x_{v,w}^{h,k,t} \ge 0, \quad \forall h \in \mathcal{H},\ \forall k \in \mathcal{K}_h,\ \forall t \in T_h,\ \forall v \in V,\ \forall w \in \bar{\mathbf{J}}(v) \tag{29}$$

$$D_l^h \ge 0, \quad \forall h \in \mathcal{H},\ \forall l \in \mathcal{L}_h \tag{30}$$

$$D_0^h = 0, \quad \forall h \in \mathcal{H} \tag{31}$$

$$\mathcal{Z}_k^h \in \{0, 1\}, \quad \forall h \in \mathcal{H},\ \forall k \in \mathcal{K}_h \tag{32}$$

$$\sum_{k \in \mathcal{K}_h} \mathcal{Z}_k^h = 1, \quad \forall h \in \mathcal{H} \tag{33}$$

The meanings of the objective and the constraints in the above mathematical programming **MP′** are shown in Table 5.

Similar to the linearization of **MP**, the mathematical programming **MP′** can be equivalently transformed into a LP. The following linear constraints can be used to replace constrains (26)-(27) in **MP′**:

$$y_{v,w}^{h,k} \ge x_{v,w}^{h,k,t}, \quad \forall h \in \mathcal{H},\ \forall k \in \mathcal{K}_h,\ \forall t \in T_h,\ \forall v \in V,\ w \in \bar{\mathbf{J}}(v) \tag{34}$$

$$p_v^h \ge D_l^h - D_{l-1}^h, \quad \forall h \in \mathcal{H},\ \forall l \in \mathcal{L}_h,\ \forall v \in \bar{I} \tag{35}$$

$$\sum_{u \in \mathbf{J}(v)} \sum_{k \in K_h} y_{u,v}^{h,k} \le D_{L_h}^h - p_v^h, \quad \forall h \in \mathcal{H},\ \forall v \in \bar{I} \tag{36}$$

Specifically, the constraint (34) replaces constraint (26), and constraints (35) and (36) replace constraint (27). Therefore, according to the above linearization, the SMMS problem with source selection can be formulated into the following ILP $\mathbf{MP}_1'$;

$$\mathbf{MP}_1' : \mathbf{Maximize} : \sum_{h \in \mathcal{H}} \sum_{l \in \mathcal{L}_h} \omega_l^h \left(D_l^h - D_{l-1}^h\right) \quad \text{s.t.} \quad \text{constraints (19)–(25), (28)–(36).} \tag{37}$$

When the size of the SMMS problem with source selection is small, the above ILP $\mathbf{MP}_1'$ can be used to obtain the optimal source selection, rate allocation, and transmission topology for H multicasts. However, with the increase of the problem size, the computational complexity of the ILP will be extremely high. Therefore, we next propose an efficient *Multicast Based on LP-Relaxation* (MBLP) algorithm to get

Table 5: The meanings of objectives and constraints.

Constraint	Meaning
Objective (18)	Maximize the total SWT
Constraint(19)	The transmission rate of each data stream must be greater than 0
Constraint(20)–(25)	(1) Nodes in the network must follow the network flow constraints, and (2) for each multicast, only one source node can be select and send out data streams.
Constraint(26)	The actual data flow sent from the source node s_k^h and transmitted on each link in the network should be no less than the flow sent from the source node s_k^h transmitted on the link to each destination node
Constraint(27)	Each data flow passing through the malicious node in the network should meet the requirements of WS
Constraint(10)	The sum of data flows passing through each link should not be more than the bandwidth capacity of the link
Constraint(29)–(31)	The ranges of the variables
Constraint(32)	Whether the node s_k^h is selected as the source node of the h^{th} multicast
Constraint(33)	Only one node can be selected as the source node of each multicast

(1) Replace constraint (32) by constraint (38) in $\mathbf{MP}_1'$.
(2) Obtain the optimal solution $\{\mathbf{Z}^1, \mathbf{Z}^2, \cdots, \mathbf{Z}^H\}$ by solving the LP consisting of the objective (18), constraints (19)–(25), constraints (28)–(31) and constraints (33), (34), (35), (36), and (38).
(3) For the h^{th} multicast, select the k^{th} node who has the biggest value in set $\mathbf{Z}^h$ as its source node, and let the corresponding $\mathscr{Z}_k^h$ value be 1 and other values in $\mathbf{Z}^h$ be 0.
(4) After selecting the source node for each multicast, treat $\mathbf{Z}^h, \forall h \in \{1, \cdots, H\}$ as the know parameters in $\mathbf{MP}_1'$ and solve it to obtain the optimal transmission rate allocation and transmission topology.

Algorithm 1: The *Multicast Based onLP-Relaxation* (MBLP) algorithm.

the approximate optimal solution. Specifically, we will firstly relax the integer linear constraints of the ILP and obtain the solution of the linear programming. We then round these real number solutions to integer solution.

The MBLP algorithm mainly includes the following steps:

(1) Replace constraint (32) by constraint (38):

$$0 \le \mathscr{Z}_k^h \le 1, \quad \forall h \in \mathscr{H}, \ \forall k \in \mathscr{K}_h \tag{38}$$

(2) The objective (18), constraints (19)–(25), constraints (28)–(31), and constraints (33), (34), (35), (36), and (38) compose a new LP. We denote the optimal solution of the LP as $\{\mathbf{Z}^1, \mathbf{Z}^2, \cdots, \mathbf{Z}^H\}$, in which $\mathbf{Z}^h = \{\mathscr{Z}_1^h, \mathscr{Z}_2^h, \cdots, \mathscr{Z}_{K_h}^h\}$, $\forall h \in \{1, \cdots, H\}$. $\mathscr{Z}_k^h, \forall h \in \{1, \cdots, H\}$ and $\forall k \in \{1, \cdots, K_h\}$, is the optimal solution obtained by solving the LP relaxed by ILP $\mathbf{MP}_1'$. We note that the value of $\mathscr{Z}_k^h$ may not be an integer.

(3) For each multicast (s_h, T_h), $\forall h \in \mathscr{H}$, we will select one node from the available source node set as its source node. Specifically, as shown in Algorithm 1, for each multicast (s_h, T_h), we select the k^{th} node s_k^h in the available source node set who has the biggest value in set $\mathbf{Z}^h = \{\mathscr{Z}_1^h, \mathscr{Z}_2^h, \cdots, \mathscr{Z}_{K_h}^h\}$ as the source node of the h^{th} multicast, and let the corresponding $\mathscr{Z}_k^h$ value be 1 and other values in $\mathbf{Z}^h$ be 0.

(4) After obtaining the values of the $\mathscr{Z}_k^h, \forall h \in \{1, \cdots, H\}$ and $\forall k \in \{1, \cdots, K_h\}$, we treat them as known parameter in $\mathbf{MP}_1'$. Accordingly, $\mathbf{MP}_1'$ becomes LP and we can solve it to obtain the optimal transmission rate allocation and transmission topology. Furthermore, H secure linear multicast code can be further designed for H multicast individually [19] to achieve the throughput obtained by $\mathbf{MP}_1'$.

4. Simulation Results

In this section, we will conduct extensive simulations to evaluate the performance of the proposed MORT algorithm and the MBLP algorithm for the SMMS problem with fixed source and source selection, respectively.

4.1. Simulation Settings. We will use the Waxman model [20] to generate the random network topology $G = \langle V, E \rangle$ to represent the core network. Specifically, in the Waxman model, there are three parameters: λ, α, β and the size of the domain is 10×10.

We randomly select N nodes in V as the set of destination nodes T. For the h^{th} multicast, we first randomly select the value $|T_h|$ from $[1, N]$ and then randomly select $|T_h|$ nodes from the set of destination nodes T as the set T_h. For the SMMS problem with fixed source, we randomly select one node in $V - T_h$ for the h^{th} multicast as its source node. On the other hand, for the SMMS problem with source selection, we first randomly select the value $|\mathscr{K}_h|$ from $[1, sn]$ and then randomly select $|\mathscr{K}_h|$ nodes from $V - T_h$ for the h^{th} multicast

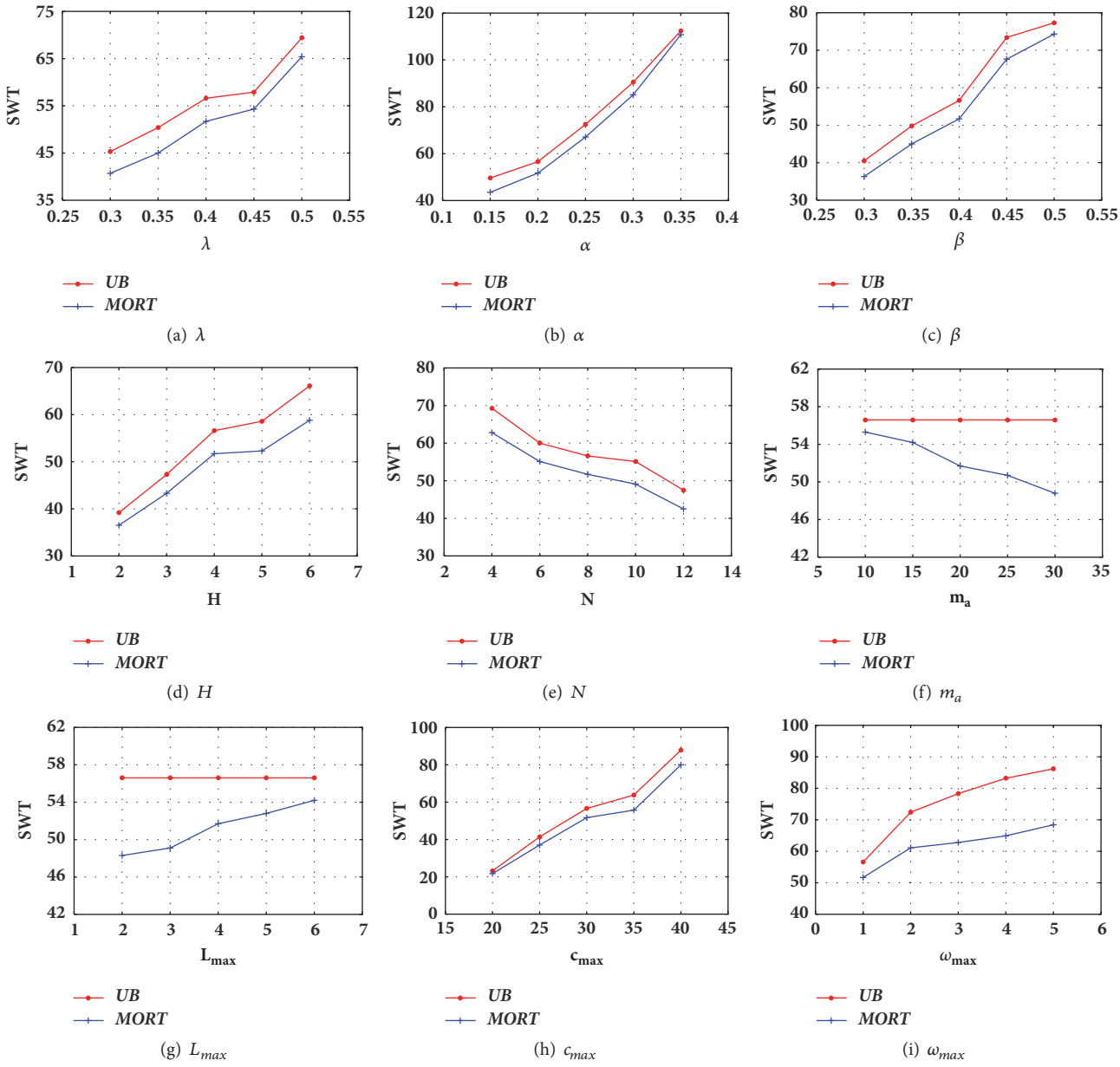


FIGURE 4: Simulation results for the MORT algorithm.

as the source set $\mathcal{K}_h$. In addition, m_a nodes are randomly selected from the remaining nodes as passive attackers. For each link $e_{u,v} \in E$, its bandwidth capacity $c_{u,v}$ is selected randomly from $[1, c_{max}]$.

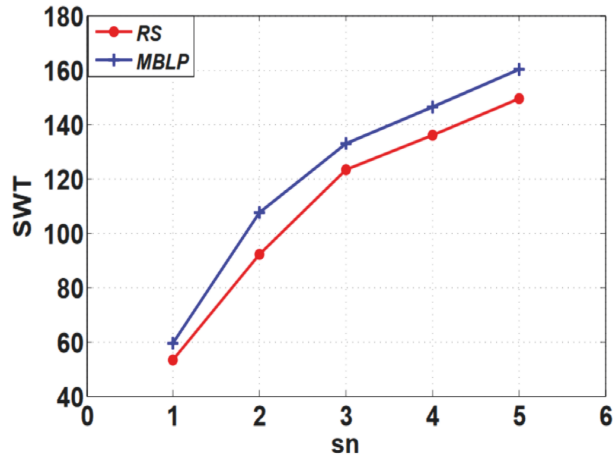
For the h^{th} multicast, the number of data streams l_h is randomly selected from $[1, L_{max}]$. Moreover, for the L^{th} data stream of the h^{th} multicast, the weight ω_l^h is given by the following steps. Firstly, we randomly select a number $\overline{\omega}_l^h$ from $[1, \omega_{max}]$. Then, the weight ω_l^h can be calculated by $(\overline{\omega}_l^h \times L_h)/\sum_{l=1}^{L_h} \overline{\omega}_l^h$, which makes sure that the total weights of a multicast with L_h streams are L_h.

In the following simulations, for each set of parameters, we conduct 50 different groups of network topologies and obtain the average value of them. Moreover, for each figure shown in Figures 4 and 5, the performance is evaluated when changing only one parameter. In detail, the parameters used in our simulations are shown in Table 6. The default values of related parameters are $\lambda = 0.4$, $\alpha = 0.2$, $\beta = 0.4$, $H = 4$, $c_{max} = 30$, $m_a = 20$, $N = 8$, $L_{max} = 4$, $\omega_{max} = 1$, and $sn = 2$.

4.2. Performance of the MORT Algorithm. In order to evaluate the performance of the MORT algorithm, we will compare the MORT algorithm with an *upper bound* (UB). Specifically, when the constraint (15) and the constraint (16) in the LP $\mathbf{MP}_1$ are removed, the objective value obtained by the LP is obviously an upper bound of the MORT algorithm.

Table 6: Simulation parameters.

Parameter	Definition
λ, α, β	Parameters of the Waxman model, $\lambda \in \{0.30, 0.35, 0.40, 0.45, 0.50\}$, $\alpha \in \{0.15, 0.20, 0.25, 0.30, 0.35\}$ and $\beta \in \{0.30, 0.35, 0.40, 0.45, 0.50\}$
H	The number of multicasts, $H \in \{2, 3, 4, 5, 6\}$
N	The total number of destination nodes, *i.e.*, $N = \|T\| \in \{4, 6, 8, 10, 12\}$
m_a	The number of malicious nodes, *i.e.*, $m_a = \|\bar{I}\| \in \{10, 15, 20, 25, 30\}$
L_{max}	The maximum number of data streams, $L_{max} \in \{2, 3, 4, 5, 6\}$
c_{max}	The maximum value of the link bandwidth capacity, $c_{max} \in \{20, 25, 30, 35, 40\}$
ω_{max}	The value to control the weight of the data stream, $\omega_{max} \in \{1, 2, 3, 4, 5\}$
sn	The maximum size of the source node set for the SMMS problem with source selection, $sn \in \{1, 2, 3, 4, 5\}$



Available source node set size: sn

Figure 5: Simulation results for the MBLP algorithm.

We will compare the performances of the MORT algorithm with UB when the following seven sets of parameters change.

4.2.1. Network Parameters: λ, α, and β. With the increase of λ, the number of nodes in the network topology increases. When the parameter β is a constant, more links can be selected to transmit data streams. Therefore, as shown in Figure 4(a), both the MORT algorithm and the UB can achieve higher weighted throughput. However, the MORT algorithm not only guarantees the WS requirements during the transmission, but also keeps the relative gap of the upper bound weighted throughput within 10%, even when the number of nodes and links are sufficiently large in the network. Moreover, with the increase of the node density, the SWT of the MORT algorithm is closer to that of UB.

As shown in Figures 4(b) and 4(c), with the increase of α and β, the weighted transmission throughput of the two algorithms also increases. Since α or β becomes larger, the probability of the existence of the link between two nodes also increases. Although the node density in the network does not change, the number of links in the network increase with the increase of α or β, which directly increases the transmission throughput of the network. On the other hand, when the network is sparse, the relative gap between the SWT obtained by the MORT algorithm and weighted throughput obtained by UB is about 10%. Moreover, when the network becomes denser, the MORT algorithm is closer to UB.

4.2.2. Number of Multicasts H. As shown in Figure 4(d), with the increase of H multicast, both the SWT of MORT and the weighted throughput of UB increase, because more multicast leads to larger total weighted throughput. However, since the SWT of MORT is limited by the WS requirements, the gap between the MORT and the UB increases with the increase of H.

4.2.3. Number of Destination Nodes N. In Figure 4(e), both the SWT of the MORT and the weighted throughput of UB decrease with the increase of the number of destinations. The reason is that, in each multicast, all the destinations should receive data streams with the same rate, *i.e.*, the throughput of the multicast. Therefore, the more destinations, the lower the SWT achieved by the MORT and the weighted throughput of UB.

4.2.4. Number of Malicious Nodes m_a. As we can see from Figure 4(f), the weighted throughput of the UB remains stable with the increase of m_a. The reason is that the UB does not consider the security of data transmission. On the other hand, with the increase of malicious nodes, the SWT of MORT algorithm decreases. This is because that the SWT of MORT is limited by the WS requirements on all malicious nodes. It is worth noting that, even when $m_a = 30$, *i.e.*, 90% of intermediate nodes are malicious, the MORT algorithm also can achieve SWT 49, which also can achieve 86% weighted throughput of the UB.

4.2.5. The Maximum Number of Data Streams L_{max}. As shown in Figure 4(g), the weighted throughput of the UB does not change with the increase of L_{max}. This is because when the network topology is fixed, the increase of the number of data streams in a multicast will not affect the weighted throughput of the multicasts. On the other hand, the SWT obtained by the MORT algorithm increases with the increase of L_{max}. When the number of data streams of a multicast increases, different data streams can be encoded together to satisfy the requirements of WS. It means that the constraints (15) and (16) related to the requirements of WS will be easily satisfied. Therefore, with the increase of L_{max}, the SWT obtained by the MORT algorithm will be closer to the weighted throughput obtained by the UB. We note that the gap between them tends to 0 when L_{max} is large enough.

4.2.6. The Maximum Link Bandwidth Capacity c_{max}. As shown in Figure 4(h), when the link bandwidth capacity becomes larger, both the SWT of the MORT and the weighted throughput of UB increase. The reason is obvious. In addition, the relative difference between the SWT obtained by the MORT algorithm and the weighted throughput obtained by the UB is no more than 10%.

4.2.7. ω_{max}. As mentioned in the example of Section 1, to maximize the total SWT, the weight of each data stream is an important parameter and it will directly affect the network weighted throughput. As shown in Figure 4(i), when the network topology is fixed, with the increase of the weight of each data stream, it will inevitably lead to a rapid increase of both the SWT of the MORT and the weighted throughput of UB. Moreover, the increase of the weight of each data stream also amplifies the gap between the SWT of the MORT and the weighted throughput of UB.

4.3. Performance of the MBLP Algorithm. In order to evaluate the performance of the MBLP algorithm, we will compare it with the *Random Selection* (RS) algorithm. Specifically, in the RS algorithm, we randomly select a node from the node set $\{s_1^h, s_2^h, \cdots, s_{K_h}^h\}$ as the source node of the h^{th} multicast, $\forall h \in \{1, \cdots, H\}$, and then obtain the maximum SWT by solving the MORT algorithm. Therefore, the SWT achieved by the RS algorithm composed a lower bound of the SMMS problem with source selection. We will compare the performances of the MBLP algorithm with the RS algorithm when the *sn*, *i.e.*, the maximum size of the source node set, changes.

As shown in Figure 5, when the *sn* becomes larger, the SWT achieved by both algorithms increases significantly. The reason is that, for each multicast, the more the nodes that can be selected as the source, the higher optimization space (probability) that higher SWT can be achieved by the MBLP (RS) algorithm. Since the optimization space becomes larger with the increase of *sn*, the gap between the SWTs achieved by the MBLP and the RS becomes larger.

5. Conclusion

In this paper, the *secure delivery for multiple multicast with multiple streams* (SMMS) problem has been considered to maximize the total *secure weighted throughput* (SWT). Specifically, we considered the problem in the following cases. (1) When the source is fixed in each multicast, we firstly formulated the problem as a *linear programming* (LP) based on the problem model and then proposed the MORT algorithm to optimally solve the LP. (2) When the source of each multicast can be selected from a set of nodes, we firstly formulated the problem as an *integer linear programming* (ILP) and then proposed a near-optimal MBLP algorithm based on LP relaxation to solve the ILP. After we proposed the MORT algorithm and the MBLP algorithm, we also designed an upper bound for the MORT algorithm and a lower bound for the MBLP algorithm, respectively. Finally, we conducted extensive simulations to evaluate the performance of the two proposed algorithms, which showed the efficiency of them. Specifically, the proposed MORT algorithm is close to the upper bound when the network size or the problem size is large, and the proposed MBLP algorithm is far away from the lower bound when the available source node set size is large.

Data Availability

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

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work is supported in part by the National Natural Science Foundation of China under Grant no. 61672370, Natural Science Research Foundation of Jiangsu Higher Education Institutions under Grants nos. 17KJB520037 and 17KJB520035, and CERNET Next-Generation Internet Technology Innovation Project under Grant no. NGII20170311.

References

[1] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of things: a survey on enabling technologies, protocols, and applications," *IEEE Communications Surveys & Tutorials*, vol. 17, no. 4, pp. 2347–2376, 2015.

[2] L. Atzori, A. Iera, and G. Morabito, "The internet of things: a survey," *Computer Networks*, vol. 54, no. 15, pp. 2787–2805, 2010.

[3] R. Bassoli, H. Marques, J. Rodriguez, K. W. Shum, and R. Tafazolli, "Network coding theory: A survey," *IEEE Communications Surveys & Tutorials*, vol. 15, no. 4, pp. 1950–1978, 2013.

[4] S. R. Li, R. W. Yeung, and N. Cai, "Linear network coding," *Institute of Electrical and Electronics Engineers Transactions on Information Theory*, vol. 49, no. 2, pp. 371–381, 2003.

[5] D. S. Lun, N. Ratnakar, R. Koetter, D. R. Karger, T. Ho, and E. Ahmed, "Minimum-cost multicast over coded packet networks," *IEEE/ACM Transactions on Networking*, vol. 52, no. 6, pp. 2608–2623, 2006.

[6] M. A. Raayatpanah, H. Salehi Fathabadi, B. H. Khalaj, and S. Khodayifar, "Minimum cost multiple multicast network coding with quantized rates," *Computer Networks*, vol. 57, no. 5, pp. 1113–1123, 2012.

[7] R. Ahlswede, N. Cai, S. R. Li, and R. W. Yeung, "Network information flow," *Institute of Electrical and Electronics Engineers Transactions on Information Theory*, vol. 46, no. 4, pp. 1204–1216, 2000.

[8] H. Ghasvari, M. A. Raayatpanah, B. H. Khalaj, and H. Bakhshi, "Optimal sub-graph selection over coded networks with delay and limited-size buffering," *IET Communications*, vol. 5, no. 11, pp. 1497–1505, 2011.

[9] Y. Wu and S.-Y. Kung, "Distributed utility maximization for network coding based multicasting: a shortest path approach," *IEEE Journal on Selected Areas in Communications*, vol. 24, no. 8, pp. 1475–1488, 2006.

[10] K. Bhattad and K. R. Narayanan, "Weakly secure network coding," in *Proceedings of the 1st Workshop on Network Coding, Theory, and Applications (NetCod)*, pp. 1–6, 2005.

[11] J. Wang, J. Wang, K. Lu, B. Xiao, and N. Gu, "Optimal linear network coding design for secure unicast with multiple streams," in *Proceedings of the 29th IEEE International Conference on Computer Communications (INFOCOM)*, pp. 2240–2248, San Diego, CA, USA, March 2010.

[12] X. Chang, J. Wang, J. Wang, V. Lee, K. Lu, and Y. Yang, "On achieving maximum secure throughput using network coding against wiretap attack," in *Proceedings of the 2010 IEEE 30th International Conference on Distributed Computing Systems (ICDCS)*, pp. 526–535, Genoa, Italy, June 2010.

[13] X. Chang, J. Wang, and V. Lee, "Modeling and optimal design of linear network coding for secure unicast with multiple streams," *IEEE Transactions on Parallel and Distributed Systems*, vol. 24, no. 10, pp. 2025–2035, 2013.

[14] J. Wang, J. Wang, K. Lu, Y. Qian, and N. Gu, "On the optimal linear network coding design for information theoretically secure unicast streaming," *IEEE Transactions on Multimedia*, vol. 18, no. 6, pp. 1149–1162, 2016.

[15] J. Wang, J. Wang, K. Lu, Y. Qian, B. Xiao, and N. Gu, "Optimal design of linear network coding for information theoretically secure unicast," in *Proceedings of the 30th IEEE International Conference on Computer Communications (INFOCOM)*, pp. 757–765, Shanghai, China, April 2011.

[16] E. Magli, M. Wang, P. Frossard, and A. Markopoulou, "Network coding meets multimedia: a review," *IEEE Transactions on Multimedia*, vol. 15, no. 5, pp. 1195–1212, 2013.

[17] J. Feldman, T. Malkin, A. R. Servedio, and C. Stein, "On the capacity of secure network coding," in *Proceedings of the 42nd Annual Allerton Conference on Communication, Control, and Computing*, 2004.

[18] N. Cai and R. W. Yeung, "Secure network coding on a wiretap network," *IEEE Transactions on Information Theory*, vol. 57, no. 1, pp. 424–435, 2011.

[19] Z. Wen, J. Wang, K. Lu, J. Zhou, Z. Gao, and Y. Zhu, "Optimal rate allocation and linear network coding design for secure multicast with multiple streams," in *Proceedings of the 18th IEEE International Conference on High Performance Computing and Communications*, pp. 1037–1044, Sydney, Australia, December 2016.

[20] B. M. Waxman, "Routing of multipoint connections," *IEEE Journal on Selected Areas in Communications*, vol. 6, no. 9, pp. 1617–1622, 1988.