Hindawi
Wireless Communications and Mobile Computing
Volume 2018, Article ID 8404219, 11 pages
https://doi.org/10.1155/2018/8404219

Research Article

Security Enhancement for Multicast over Internet of Things by Dynamically Constructed Fountain Codes

Qinghe Du[1,2], **Ying Xu**[1,2], **Wanyu Li**[1,2] **and Houbing Song**[3]

[1]*School of Electronic and Information Engineering, Xi'an Jiaotong University, Xi'an 710049, China*
[2]*National Simulation Education Center for Communications and Information Systems, Xi'an 710049, China*
[3]*Department of Electrical, Computer, Software, and Systems Engineering, Embry-Riddle Aeronautical University, Daytona Beach, FL 32114, USA*

Correspondence should be addressed to Qinghe Du; duqinghe.xjtu@gmail.com

Received 14 August 2017; Revised 28 October 2017; Accepted 7 November 2017; Published 8 February 2018

Academic Editor: Zhipeng Cai

The Internet of Things (IoT) is expected to accommodate every object which exists in this world or likely to exist in the near future. The enormous scale of the objects is challenged by big security concerns, especially for common information dissemination via multicast services, where the reliability assurance for multiple multicast users at the cost of increasing redundancy and/or retransmissions also benefits eavesdroppers in successfully decoding the overheard signals. The objective of this work is to address the security challenge present in IoT multicast applications. Specifically, with the presence of the eavesdropper, an adaptive fountain code design is proposed in this paper to enhance the security for multicast in IoT. The main novel features of the proposed scheme include two folds: (i) dynamical encoding scheme which can effectively decrease intercept probability at the eavesdropper; (ii) increasing the transmission efficiency compared with the conventional nondynamical design. The analysis and simulation results show that the proposed scheme can effectively enhance information security while achieving higher transmission efficiency with a little accredited complexity, thus facilitating the secured wireless multicast transmissions over IoT.

1. Introduction

The development of the Internet of Things (IoT) [1] paradigm is regarded as one of the most important revolutions in the information area. IoT is a global infrastructure of interconnected networks consisting of all kinds of information sensing device like radio frequency identification devices (RFID), sensors, and other distributed smart objects. The aim is to interconnect all kinds of smart objects with Internet via different wireless access network, so that the system can automatically identify, locate, trace, and monitor the objects [2]. The basic features of IoT are smart-sensing, smart-storing, smart-exchanging, and smart-analyzing for the information [3], the core of which is the information exchange. Hence, the pivotal technologies of IoT cover a wide range including LAA [4], D2D [5–7], and multicast [8–10].

Multicast [11] is one of the most important services which is required to be supported in IoT [12, 13]. In IoT [14] applications where the message must get through multiple devices/nodes or a major equipment shutdown is required (e.g., for urgent reasons), the sending node must be able to confirm that its message was received by all the members of the multicast group while assuring security from eavesdroppers. In the IoT, the major challenge compared with traditional multicast system is that it not only supports end-user devices, but also involves large-scale machine-type communications (MTC) and other low-power devices [12]. Thus, multicast in the IoT needs to have the capacity of accommodating different kinds of devices and dealing with high speed rate or erupted traffic. Moreover, the little overhead of the devices results in more complex situation in the aspect of security.

The objective of this paper is to address the security challenge present in the IoT applications which are required to support confirmed, network-wide (spanning all links within the system) multicast. Inspired by these reasons, there has been a significant increase in the demands of wireless multicast networks. Wireless multicast [15] is one

of the most important services which gives a highly efficient mean of transmitting message from a single source to multiple location separated receivers [16]. Accordingly, wireless multicast, as a critical part of wireless communications network, provides higher bandwidth utilization in many applications, including remote teleconferencing and highway wireless traffic updating [17]. However, there are many new challenges in multicast systems mainly including two aspects. On the one hand, wireless multicast services often lead to feedback implosion problem [18]. On the other hand, according to the retransmission-based error control, retransmission overhead and unnecessary retransmissions grow up quickly as the number of multicast objects increases [19]. Accordingly, the main challenge in wireless multicast networks is guarantying secure and reliable transmission for various multicast services.

Fountain code [20] is regarded as an emerging and reliable technology which is appropriate for reliable wireless multicast networks due to its rate-less feature [21]. In other words, introducing fountain code into multicast system has strong scalability evidenced by two folds. On the one hand, compared with the fixed-rate forward error correction (FEC) code, the number of encoding symbols that can be generated from the data is potentially limitless for all multicast objects. On the other hand, the transmitter (BS) has no need to change the encoding mode while the number of objects, the objects locations, or objects channel conditions change. In some way, the fountain-encoding mode in multicast systems can be seen as a kind of "adaptive rate" encoding mode with no requirement of the real-time channel state feedback (CSI). Moreover, it is worth mentioning that fountain-code-based multicast schemes are more adaptable to massive data distribution services rather than real-time ones with strict requirements of bite rates, which are essentially useful for IoT for common information dissemination.

When integrating multicast services in IoT, a critically important indicator is information security in the presence of eavesdropper. Given the open wireless transmission environments and independent packet loss status across multicast objects, security assurance becomes essentially challenging. Recent research showed that fountain code [20] can be applied to effectively enhance the security. Specifically, by introducing a fountain encoder in wireless multicast networks, BS keeps multicasting encoding packets until all multicast objects give feedback indicating recovery of the entire coded block [20]. Then, via designs maximally benefiting the physical layer signals for legitimate objects, which in fact statistically degrade the signal quality overheard by the eavesdropper, the legitimate object can accumulate sufficient number of coded packets for complete decoding before the eavesdropper does with a high probability [20]. While enhancing security by applying fountain code opens a promising research area, the specific design for secure fountain code applied in the multicast services in IoT has not been sufficiently studied. First, compared with unicast transmissions, extra transmissions and complex wireless channel condition make it more difficult for secure transmissions in multicast services. Second, current research mainly studied the resource allocation rather than online fountain code construction. Hence, it has the urgent necessity to develop the specific and secure fountain codes scheme which can be practically applied to the IoT services.

According to the aforementioned problems, a novel fountain-encoding scheme for wireless multicast services has been developed in this paper, which dynamically selects the encoding rules for every multicast objects according to the feedback messages from them. During each slot, these feedback messages refer to the acknowledge (ACK) signals fed back from the multicast objects which succeed in receiving the fountain packets. Based on these ACK signals, BS can regenerate the decoding processes towards these corresponding multicast objects and, respectively, updates their index set of decoded data packet. Therefore, the key to the proposed scheme is that, on the basis of its existing information, BS conducts the dynamical fountain-encoding scheme which makes for increasing the decoding rates for the multicast objects. In this manner, the multicast objects can complete decoding first so as to ensure the secure multicast services in the presence of eavesdropper. On the contrary, if the eavesdropper also wiretaps as many fountain packets as the multicast objects do, the confidential data transmitted by BS are intercepted. The analytical and simulation results both show that the intercept probability of the proposed scheme is much lower than traditional nonadaptive encoding schemes. It is worth mentioning that this study does not address the perfect secrecy of data streams in physical layer [20]. Moreover, the proposed scheme achieves higher transmission efficiency of BS for wireless multicast services while imposing a little accredited complexity for multicast networks.

The remainder of this paper is organized as follows. Section 2 presents the system model of the wireless multicast services. Section 3 introduces the proposed encoding scheme as well as the decoding process in detail. The performance analysis of the proposed scheme is demonstrated in Section 4. Then Section 5 presents the simulation setup and simulation results among the proposed scheme and the traditional ones. Finally, this paper is concluded in Section 6.

2. System Model

In this section, the system model of wireless multicast services is proposed first. Then the transmission model based on the fountain code for wireless multicast system is illustrated. Finally, this section generally reviews the encoding principles and decoding process for fountain codes.

As depicted in Figure 1, the system model of wireless multicast network considers a cellular cell with radius R. BS is situated in the center of the cellular cell and multicast objects denoted as M are randomly located in different positions in the cell. Meantime, the unauthorized eavesdropper locates at the edge of the cell. The position of each objects is independent and identically distributed. The position for the ith object is jointly determined by the distance from BS denoted as d_i and the angle between object-BS and horizontal axis denoted as θ_i. The distance between the ith and jth objects denoted as $d_{i,j}$ is expressed as

$$\left(d_{i,j}\right)^2 = d_i^2 + d_j^2 - 2d_i d_j \cos\left(\theta_i - \theta_j\right). \tag{1}$$

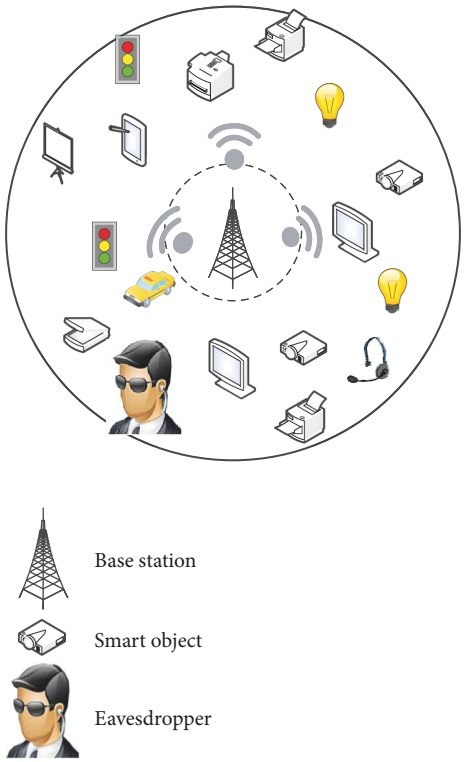

Figure 1: System model for wireless multicast network in Internet of Things.

During each slot, BS broadcasts fountain packet to all multicast objects that is located in different positions. The wireless link between any two nodes comprises the large-scale fading, small-scale fading, and additive Gauss white noise (AWGN) in the receiver. The large-scale fading caused by path loss is modeled as

$$\mathrm{PL}\left(d_{i,j}\right) = d_{i,j}^{-\eta} \tag{2}$$

where η represents the path loss exponent. Besides, the small-scale fading induced by multipath fading is modeled as the block flat Rayleigh fading. That is to say, the channel coefficients remain constant during one slot and change independently during different slots. The channel coefficient h_{ij} is assumed as a circularly symmetric complex Gaussian random variable, namely, $h_{i,j} \sim \mathcal{CN}(0, 1)$. Additive Gaussian white noise denoted as ω is assumed with the variance N_0. For the ith object, the symbol it receives during T_s slot is expressed as

$$y_i^{T_s} = \sqrt{P_s d_{s,i}^{-\eta}} h_{s,i} x_{f_{T_s}} + n_i. \tag{3}$$

where P_s denotes the transmit power of BS; $d_{s,i}$ represents the distance between the BS and the ith object; $h_{s,i}$ denotes the Rayleigh fading channel coefficients for the transmission link between BS and the ith object; n_i denotes the received noise for the ith object; $x_{f_{T_s}}$ represents the fountain packet transmitted by BS during T_s slot. We assume that the power of the fountain packet is 1. Consequently, the received SNR for the ith object can be defined as

$$\gamma_i^{T_s} = \frac{P_s \left|h_{s,i}\right|^2 d_{s,i}^{-\eta}}{N_0}. \tag{4}$$

Once $d_{s,i}$ is fixed, $\gamma_i^{T_s}$ obeys the exponential distribution with the parameter of $\lambda_i = (N_0 d_{s,i}^{\eta})/P_s$.

Figure 2 illustrates the detailed fountain-encoded transmission scheme for multicast network. Firstly BS conducts the fountain-encoding procedure and delivers the packet to all objects. Meanwhile, the eavesdropper attempts to intercept the transmitted packet. BS continues to broadcast the fountain packets at each time slot so that all objects (including the eavesdropper) intend to receive enough fountain packets to decode the original files. If all the multicast objects obtain enough fountain packets and successfully recover the files, the feedback information is sent to BS from all objects to terminate the encoding procedure and transmission. At this time, the security of multicast transmission can be ensured as long as the eavesdropper does not intercept sufficient fountain packets to recover the original file.

3. Dynamically Constructed Fountain Code

In this section, the Dynamically Constructed Fountain Code (DC Fountain Code) is introduced in detail. The implementation mechanism of the DC Fountain Code is illustrated as depicted in Figure 3. Specifically, the innovative points of the DC Fountain Code are shown in two sides: the transmission scheme in multicast networks described in Section 3.1 and the dynamical fountain-encoding mechanism in the transmitter. The detailed principles and process of the DC Fountain Code are introduced by the following subsections.

3.1. Transmission Scheme of BS. The transmission process of BS is depicted in Figure 3 during each time slot. Remarkably, the large data file is divided into K equal-length data packets before introducing the fountain encoder. According to the dynamical fountain-encoding scheme illustrated in Section 3.2, BS conducts the dynamical fountain-encoding procedure. Then after the CRC encoding at the data link layer and the channel encoding at the physical layer, BS delivers the fountain packet to each multicast object through the wireless channels. Meantime, in the wireless channel, the delivered fountain packet are easy to be intercepted by the eavesdropper (Eve). Because of the different channel conditions of the multicast objects, the fountain packets can hardly be received by all objects at one time. Those objects which successfully receive the fountain packet are required to send ACK signals back to BS. After receiving the ACK signals, BS "simulates" the decoding procedure and records the index set of decoded data packets denoted as D_i from the objects whose ACK signal is received by BS. Finally, if the element number of set D_i of all objects equals K (K denotes the number of all data packets), BS stops encoding process. Contrarily, if the

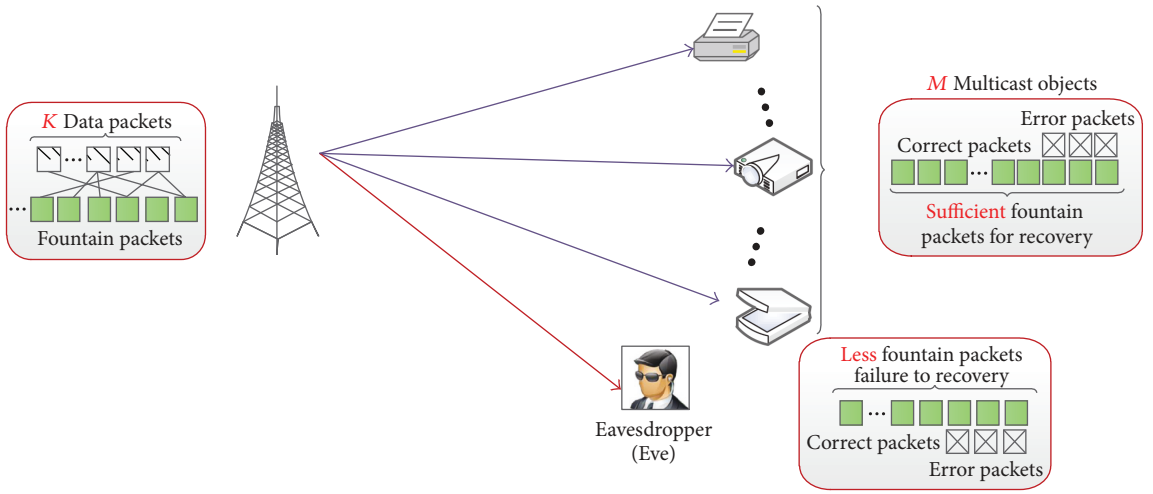

Figure 2: Fountain-encoded transmission model for multicast system.

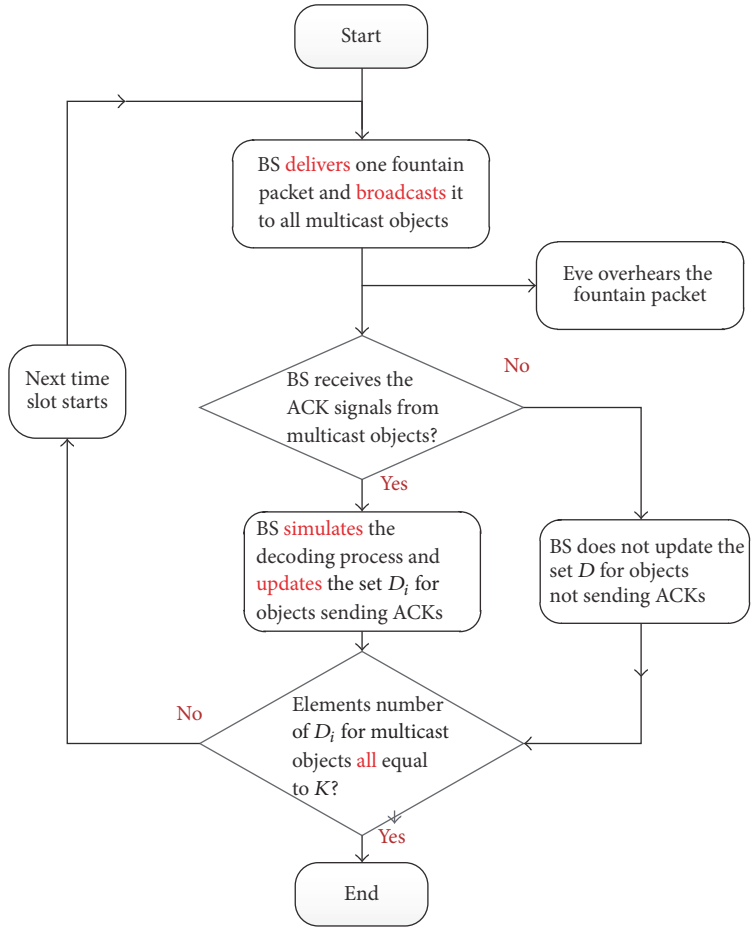

Figure 3: The transmission flow chart for BS during one transmitting slot.

element number of set D_i for at least one object is less than K, BS continues the fountain-encoding process at next time slot and repeats these process introduced above.

It is worth mentioning that only ACK signals are required to be sent back to BS from objects during each time slot and BS automatically "simulates" the decoding process and records the set D_i for them. This transmission scheme leads to less feedback intercept in the multicast channels.

3.2. Dynamically Constructed Fountain-Encoding Scheme. This part proposes the dynamically constructed fountain-encoding process and it is the key innovation of this paper

(1) BS records the rowers for full-0-lines and full-1-lines of matrix P and respectively stores them in matrix ln_0 and ln_1.
(2) Determine whether the matrix ln_1 is empty.
If ln_1 is not empty
∗ Encoding rules are as follows:
(a) Randomly choose **one** element from ln_1 denoted as S_c.
(b) Take out **all** elements from ln_0 denoted as $S_{0,1}, S_{0,2}, \ldots, S_{0,t}$
(c) The encoded fountain packet is the exclusive-or of:

$$x_{f_{T_s}} = S_c \oplus S_{0,1} \oplus S_{0,2} \oplus \cdots \oplus S_{0,t},$$

where $x_{f_{T_s}}$ denotes the encoded fountain packet during T_s-th slot.
else
∗ Switch to Step (3).
(3) Determine whether the length of ln_0 is smaller than $K/4$.
If length (ln_0) $\leqslant K/4$
∗ Encoding rules follow Algorithm 2.
else
∗ Encoding rules follow Algorithm 3.

Algorithm 1: DC fountain-encoding procedures (1).

(1) Compute the sum of each row as P_line. Find the maximum value in P_line and records one of the corresponding rowers as S_max.
(2) Traverse K lines to search for several lines whose rowers are denoted as $S_{r,1}, S_{r,2}, \ldots, S_{r,n}$ to meet the following conditions:
(i) Assume the matrix made by $S_{r,1}, S_{r,2}, \ldots, S_{r,n}$ and S_max is defined as P_temp. The sum of each column for P_temp must be less than 2.
(3) The encoded fountain packet is the exclusive-or of:

$$x_{f_{T_s}} = S\_\max \oplus S_{r,1} \oplus S_{r,2} \oplus \cdots \oplus S_{r,n},$$

where $x_{f_{T_s}}$ denotes the encoded fountain packet during T_s-th slot.

Algorithm 2: DC fountain-encoding procedures (2).

after introducing the transmission procedure of BS. Without loss of generality, here a certain transmitting slot is taken as an example.

First, BS records the indexes of the decoded data packets for each multicast object. According to the number of decoded data packets, the "encoding structure matrix" denoted as $P_{K\times M}$ is generated, where K denotes the number of data packets and M denotes the number of multicast objects. The initial value of the elements in P is set to 1. The element of $P_{K\times M}$, denoted as p_{ij}, is the decoding indicator and its value equals 1 (0) if the jth multicast object has (not) decoded the ith data packet. Moreover, the index set of total data packets is denoted as $\{S_1, S_2, \ldots, S_K\}$. The rowers of the matrix P exactly represent the index set of data packet and hence can also be described as $\{S_1, S_2, \ldots, S_K\}$.

According to the value and the state of P, the dynamical fountain-encoding scheme is presented in Algorithms 1–3. At the beginning of each time slot, the rowers of full-0-lines and full-1-lines are recorded and, respectively, stored in the matrix ln_0 and ln_1. Then according to judging whether ln_1 is empty, BS chooses different encoding rules. When ln_0 is not empty, the main encoding rule is to choose all the recovered data packets with one unrecovered data packet to encode and the encoded packet is the bit-wise XOR sum over all chosen data packets, which suggests a core insight into security transmission: as long as one unrecovered data packet which is connected to the transmitted fountain packet was not intercepted by Eve, the subsequent encoded packet cannot be decoded correctly. Thus the overhear process cannot be achieved successfully. When ln_1 is empty, next step is to judge whether the length of ln_0 is smaller than $K/4$. The threshold value $K/4$ is obtained from the simulation that results in a better performance.

If the length of ln_0 is less than $K/4$ as depicted in Algorithm 2, BS computes the sum of each row as P_line and then records the maximum value and the corresponding rowers in P_line. BS traverses K lines to search for several lines to form a new matrix whose sum of each column must be less than 2. In this way, it is ensured that through traversing the matrix P, the data packet which is corresponding to the most serious channel can be selected and retransmitted in order to increase the transmission efficiency. As introduced in Algorithm 3, if the length of ln_0 is larger than $K/4$, the key of the encoding process aims at choosing enough data packets which can be simultaneously decoded for most multicast objects in an acceptable complexity.

(1) Remove the full-0-lines from P.
(2) Compute the sum of each row as P_line. Find the minimum value in P_line and records the corresponding rowers stored in S_min.
(3) Assume the matrix made by S_min is defined as P_temp. If the sum of each column in P_temp is larger than 1, repeat the next step.
(4) Find the maximum value of the sum of each column in P_temp and records one of the corresponding columns as $C_{\max}$. Choose the rowers from that column whose elements is non-zero and stored as $R_{\max}$. Then find the maximum value of the sum of each row in the matrix made by $R_{\max}$ and delete the corresponding row from S_min.
(5) Assume the rowers of S_min is denoted as $S_{r,1}, S_{r,2}, \ldots, S_{r,m}$. The encoded fountain packet is the exclusive-or of:
$$x_{f_{T_s}} = S_{r,1} \oplus S_{r,2} \oplus \cdots \oplus S_{r,m},$$
where $x_{f_{T_s}}$ denotes the encoded fountain packet during T_s-th slot.

Algorithm 3: DC fountain-encoding procedures (3).

3.3. Decoding Process. The decoding process of Dynamically Constructed Fountain Code is similar to the general fountain code. The decoding process in the receiver is as follows [22]:

(a) If there exists fountain packet that only includes one data packet, then this data packet can be decoded because the fountain packet is exactly the copy of it.
(b) Subtract the recovered data packet from the fountain packets which comprise the data packet.
(c) Delete the recovered data packet from fountain packets and subtract the degree from corresponding fountain packets.

4. Performances Analysis

In this part, the implementation complexity is analyzed first. Additionally, this section analyzes the theoretical performances roughly from two aspects consisting of the intercept probability for Eve as well as the transmission efficiency for BS towards the proposed scheme.

4.1. Analysis of Implementation Complexity. According to Figure 3, BS conducts the analogs of decoding operations for multicast objects which send the feedback of ACK signals within the same transmitting slot and, respectively, upgrades their corresponding index set of decoded data packets. These operations are increasing in multiples with multicast group size, which are additional to BS to complete thus imposing extra complexity for BS. In addition, since multicast objects just need to send back ACK signals to BS, the feedback overhead for channels is lower without causing channel congestions compared with retransmission-based schemes. Moreover, the proposed scheme effectively avoids the retransmission overhead due to unnecessary retransmission in contrast with retransmission-based error control schemes.

4.2. Analysis of Intercept Probability for Eve. For multicast transmission system as discussed in Figure 2, one extreme case is that M multicast objects receive the fountain packets in a synchronized pace. That is to say, all objects succeed in receiving or fail to receive the fountain packets during each transmitting slot which means the fountain-encoding scheme in BS simply consists of Step (1) and Step (2) described in Algorithm 1. In this way, all multicast objects are regarded as one "group objects" (GO) which is similar to unicast system where BS sends fountain packets to group objects while Eve attempts to wiretaps them. As to this extreme case, it is easy to infer that BS broadcasts the minimum number of fountain packets resulting in highest transmission efficiency for BS and Eve is least likely to overhear as many fountain packets leading to minimum intercept probability. In a sum, the extreme case discussed above is equivalent to the best case referring to the lower bound of successfully intercept probability.

According to the encoding scheme discussed in Step (1) and Step (2) of Algorithm 1, the confidential data are intercepted when Eve obtains sufficient fountain packets once BS stops broadcasting fountain packets. This underlying essence provides enlightenment that Eve must successfully receive the fountain packet as long as group objects succeed in receiving it during the same slot. Conversely, there may be two cases for Eve when group objects fail to receive. Inspired by this idea, here the mapping relations between received SNR and packet error rate (PER) to give the analytical derivations below are used.

Firstly, the received SNR in group objects and Eve can be described as $\gamma_{\mathrm{BO}} = \rho|h_{\mathrm{BO}}|^2$ and $\gamma_{\mathrm{BE}} = \rho|h_{\mathrm{BE}}|^2$ in which $\rho = P_s/N_0$ is system SNR and $|h_{\mathrm{BO}}|^2$ and $|h_{\mathrm{BE}}|^2$, respectively, obey the exponential distribution with mean $d_{\mathrm{BO}}^{-\eta}$ and $d_{\mathrm{BE}}^{-\eta}$.

By referring to (14), group objects would lose packet in case of $\gamma \in (0, \gamma_{\mathrm{pn}})$ for link BS $\rightarrow$ GO and the probability of loss packet can be depicted as

$$P_{\gamma_{\mathrm{BO}} \in (0, \gamma_{\mathrm{pn}})} = 1 - \exp\left(\frac{-\widetilde{t}}{d_{\mathrm{BO}}^{-\eta}}\right), \tag{5}$$

where γ_{pn} is a mode-dependent parameter from [23].

When $\gamma \geqslant \gamma_{\mathrm{pn}}$ GO loses packet with the probability of

$$P_{\gamma_{\mathrm{BO}} \geqslant \gamma_{\mathrm{pn}}} = a_n \exp\left(-g_n \gamma_{\mathrm{BO}}\right) \cdot \exp\left(\frac{-\widetilde{t}}{d_{\mathrm{BO}}^{-\eta}}\right) \tag{6}$$

and correspondingly the probability of *not* losing packet can be inferred as

$$\overline{P}_{\gamma_{\mathrm{BO}} \geq \gamma_{\mathrm{pn}}} = \exp\left(\frac{-\widetilde{t}}{d_{\mathrm{BO}}^{-\eta}}\right) \cdot \left[1 - a_n \exp\left(-g_n \gamma_{\mathrm{BO}}\right)\right] \quad (7)$$

where $\widetilde{t} = \gamma_{\mathrm{pn}}/\rho$.

Concluding from (5), (6), and (7), the upper and lower bounds of *not* losing packet for link BS $\rightarrow$ GO can be, respectively, described as

$$\begin{aligned} \overline{P}_{\mathrm{BO,Up}} &= \exp\left(\frac{-\widetilde{t}}{d_{\mathrm{BO}}^{-\eta}}\right); \\ \overline{P}_{\mathrm{BO,Low}} &= \exp\left(\frac{-\widetilde{t}}{d_{\mathrm{BO}}^{-\eta}}\right)\left[1 - a_n \exp\left(-g_n \gamma_{\mathrm{pn}}\right)\right], \end{aligned} \quad (8)$$

where (8) is derived from (7) in case of $\gamma_{\mathrm{BO}} \rightarrow \infty$ and $\gamma_{\mathrm{BO}} \rightarrow \gamma_{\mathrm{pn}}$.

Accordingly, the upper and lower bounds of packet loss for link BS $\rightarrow$ GO are described as

$$\begin{aligned} P_{\mathrm{BO,Low}} &= 1 - \overline{P}_{\mathrm{BO,Up}} = 1 - \exp\left(\frac{-\widetilde{t}}{d_{\mathrm{BO}}^{-\eta}}\right); \\ P_{\mathrm{BO,Up}} &= 1 - \overline{P}_{\mathrm{BO,Low}} \\ &= 1 - \exp\left(\frac{-\widetilde{t}}{d_{\mathrm{BO}}^{-\eta}}\right)\left[1 - a_n \exp\left(-g_n \gamma_{\mathrm{pn}}\right)\right]. \end{aligned} \quad (9)$$

Similar to the link BS $\rightarrow$ GO, the derivation for link BS $\rightarrow$ Eve can be obtained by substituting $d_{\mathrm{BO}}, \gamma_{\mathrm{BO}}$ for $d_{\mathrm{BE}}, \gamma_{\mathrm{BE}}$ in the equations above. Due to page limits, here they are directly presented as

$$\begin{aligned} \overline{P}_{\mathrm{BE,Up}} &= \exp\left(\frac{-\widetilde{t}}{d_{\mathrm{BE}}^{-\eta}}\right); \\ P_{\mathrm{BE,Low}} &= 1 - \exp\left(\frac{-\widetilde{t}}{d_{\mathrm{BE}}^{-\eta}}\right); \\ \overline{P}_{\mathrm{BE,Low}} &= \exp\left(\frac{-\widetilde{t}}{d_{\mathrm{BE}}^{-\eta}}\right)\left[1 - a_n \exp\left(-g_n \gamma_{\mathrm{pn}}\right)\right]; \\ P_{\mathrm{BE,Up}} &= 1 - \exp\left(\frac{-\widetilde{t}}{d_{\mathrm{BE}}^{-\eta}}\right)\left[1 - a_n \exp\left(-g_n \gamma_{\mathrm{pn}}\right)\right], \end{aligned} \quad (10)$$

where the first two equations in (10) are obtained under the case of $\gamma_{\mathrm{BE}} \rightarrow \infty$ and the last two equations in (10) are derived for the case $\gamma_{\mathrm{BE}} \rightarrow \gamma_{\mathrm{pn}}$.

Therefore, the lower bound for intercept probability is formulated as (11). Substituting (8), (9), and (10) into (11), the closed-form expression of the upper bound for intercept probability in Eve can be obtained.

$$\begin{aligned} P_{\mathrm{Intercept}} = \sum_{s=0}^{K} \Big[& C_{K+s-1}^{K-1} \left(\overline{P}_{\mathrm{BO,UP}} \cdot \overline{P}_{\mathrm{BE,UP}}\right)^{K-1} \\ & \cdot \left(P_{\mathrm{BO,Low}} P_{\mathrm{BE,Low}}\right)^{s} + C_{K+s-1}^{K-1} \left(\overline{P}_{\mathrm{BO,UP}} \cdot \overline{P}_{\mathrm{PE,UP}}\right)^{K-1} \\ & \cdot \left(P_{\mathrm{BO,Low}} \overline{P}_{\mathrm{BE,UP}}\right)^{s} \Big]. \end{aligned} \quad (11)$$

4.3. Analysis of Transmission Efficiency for BS. Based on the clarifications of performance indexes in Section 5.1, the transmission efficiency of BS is generally defined as the average of K/N_{min} after a sufficient number of transmission attempts, in which N_{min} denotes the number of fountain packets transmitted by BS. Combining with (9), the minimum number of transmitted fountain packets can be described as

$$N_{\mathrm{min}} = K \cdot \left(1 + P_{\mathrm{BO,Low}}\right). \quad (12)$$

The upper bound of transmission efficiency for BS denoted as $\mathrm{TE}_{\mathrm{Up}}$ is described as

$$\mathrm{TE}_{\mathrm{Up}} = \frac{K}{N_{\mathrm{min}}} = \frac{1}{1 + P_{\mathrm{BO,Low}}}. \quad (13)$$

By substituting (9) into (13), the closed-form expression of the upper bound for transmission efficiency of BS can be obtained.

5. Simulation Evaluation

This section, respectively, presents the simulation setup and simulation results for evaluating the Dynamically Constructed Fountain Code.

5.1. Simulation Setup. The simulation is built in a circle with radius $R = 1$. The location of BS is in the center of the cell while the positions of M multicast objects are random. Besides, we assume that in the area of the circle with radius of 0.01 locates no objects. As we introduced in Section 2, the path loss exponent η of multicast channel is 2.6 and Rayleigh fading yields the complex Gaussian distribution with zero mean and variance 1. As one variable factor, transmit SNR which is denoted as $\rho = P_s/N_0$ varies from 10 dB to 35 dB. The number of multicast objects is another variable factor which range from 2 to 100. As to the location of Eve, we assume that it is on the circumference of a radius of 1 without loss of generality. Thus, the distance from Eve to BS is set to 1. Moreover, the total number of data packets denoted as K is 128. For simplicity, the packet error rate (PER) is approximated as [24]

$$\mathrm{PER}_n(\gamma) \approx \begin{cases} 1, & \text{if } 0 < \gamma < \gamma_{\mathrm{pn}} \\ a_n \exp\left(-g_n \gamma\right), & \text{if } \gamma \geqslant \gamma_{\mathrm{pn}}, \end{cases} \quad (14)$$

where γ is received SNR and n denotes mode index. The fitting parameters of different transmission modes can be found in [23]. In the simulation, it adopts 16-QAM modulation and the coding rate is set to 9/16. By referring to [23, Tables II], the fitting parameters are listed as follows:

$$a_n = 50.1222,$$
$$g_n = 0.6644, \quad (15)$$
$$\gamma_{\text{pn}} = 7.7021.$$

From (14) and (15), the mapping equation from the received SNR to channel PER is easy to obtain under Rayleigh fading channels.

In addition, three performance indexes are noted to evaluate and analyze the performance of the proposed scheme as well as the counterparts:

(a) Intercept probability for Eve: the number of data packets which are successfully recovered by Eve when BS stops sending packets is recorded and denoted as N_{eve}. If N_{eve} equals to K, the total confidential file is successfully intercepted by Eve; otherwise, the interception is failed. Hence, after sufficient transmission attempts, the intercept probability can be defined as the ratio between the number of successful eavesdropping times and the total number of transmission.

(b) Recovering proportion for Eve: is defined as the average of N_{eve}/K after sufficient attempts of transmission when BS stops encoding and transmitting.

(c) Transmission efficiency of BS: the number of fountain packets which has been transmitted until BS stops sending is recorded and denoted as $N_{\min}$. The transmission efficiency of BS is defined as the average of $K/N_{\min}$ after sufficient attempts of transmission.

Moreover, the following two schemes are introduced as baseline schemes for comparison:

(i) Due to the rate-less feature, LT codes [24] have been introduced into multicast system. The distribution of the degree of LT codes is

$$\rho(d) = \begin{cases} \frac{1}{K}, & \text{if } d = 1 \\ \frac{1}{d(d-1)}, & \text{if } d = 2, 3, \ldots, K, \end{cases} \quad (16)$$

where K denotes the number of total data packets in BS. The distribution of degree is random and the choice of random d data packets is uniform.

(ii) The optimal fountain code based on maximizing the average number of recovered data packets is discussed in [25]. We call it Max-Error-Driven Fountain Code (MED Fountain Code). The degree of MED Fountain Code is defined by

$$d^*(K, \theta) = \left\lceil \frac{K + 1 - \theta}{\theta} \right\rceil, \quad (17)$$

where K represents the number of total data packets and θ is the data packets that have not been recovered. Note that $\lceil \delta \rceil$ denotes the minimum integer that is larger than or equal to δ.

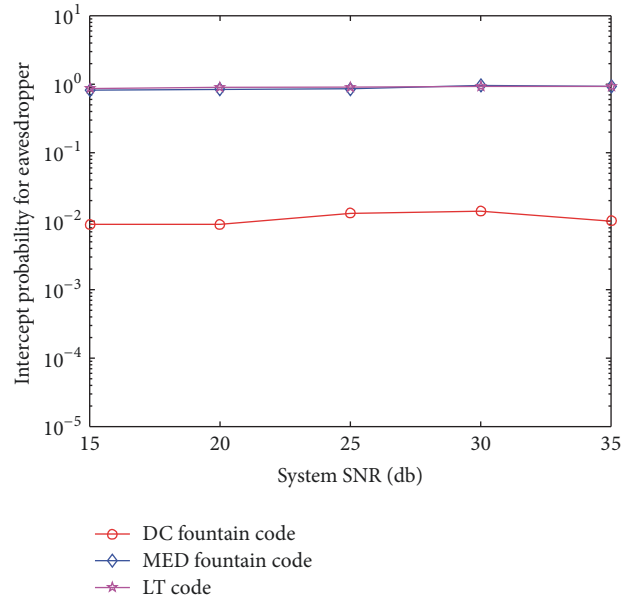

Figure 4: Intercept probability comparison between the proposed scheme and baseline schemes, where the number of multicast objects is set to 100 and system SNR varies from 15 to 35 dB.

5.2. Simulation Results. This section makes comparisons of the performances of the Dynamically Constructed Fountain Code and two baseline schemes. The performance compared is in terms of the intercept probability for Eve, transmission efficiency, and the recovering proportion for Eve.

First, the number of multicast objects is set to 100 and the number of transmissions is conducted by 10^4. Figures 4 and 5 show the performance among the DC Fountain Code, MED Fountain Code, and LT Code with system SNR ranging from 10 dB to 35 dB.

In Figure 4, the intercept probability for DC Fountain Code is far lower than those of the other two schemes. The reason is that the dynamical fountain-encoding aims at selecting different encoding rules according to different conditions while the other two schemes utilize fixed encoding rules. From Figure 5, it is demonstrated that the transmission efficiency of BS increases with the increasing of the system SNR in the proposed scheme, which is slightly superior to two baseline schemes. Notably, the improvement of transmission efficiency indicates another advantage to the proposed scheme.

In Figures 6–8, the system SNR is set to 20 dB and transmission attempts are conducted by 10^4. These figures demonstrate the performance compared among the dynamical fountain code and two baseline schemes with the number of multicast objects varying from 2 to 100. In Figure 6, the intercept probability of the proposed scheme is equal to 0 as the number of multicast objects is less than 10. When the number of multicast objects rises above 10, all curves increase while the proposed scheme is still lower than other two baselines. Hence, it indicates that the proposed scheme keeps higher security than the other two. From Figure 7, the recovering proportion of the proposed scheme is lower

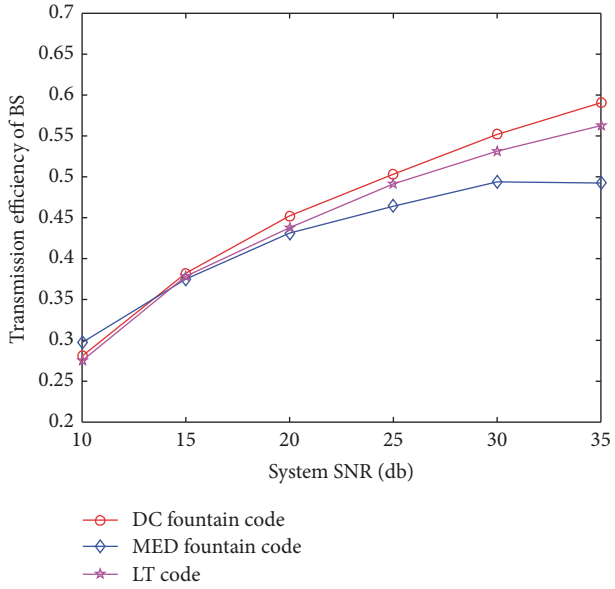

Figure 5: Transmission efficiency comparison between the proposed scheme and baseline schemes, where the number of multicast objects is set to 100 and system SNR varies from 10 to 35 dB.

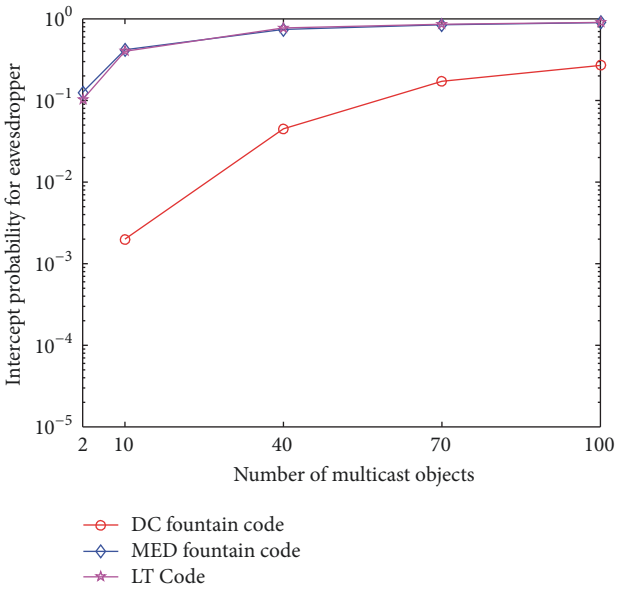

Figure 6: Comparison of Eve's recovering proportion between the proposed scheme and baseline schemes, where the system SNR is set to 20 dB and the number of multicast objects varies from 2 to 100.

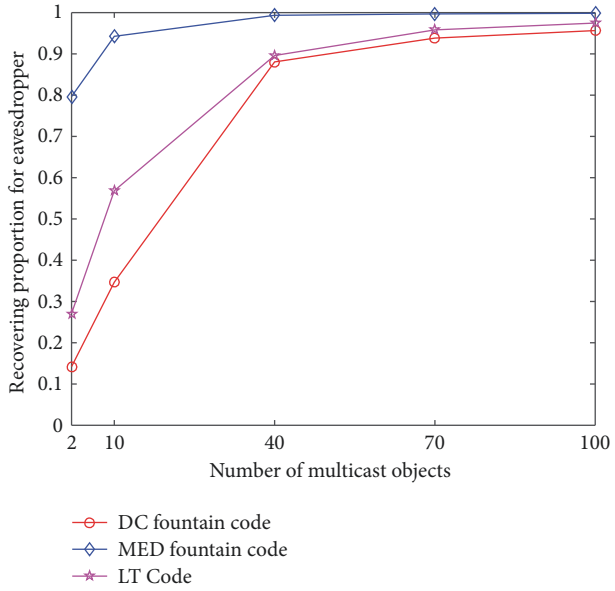

Figure 7: Intercept probability comparison between the proposed scheme and baseline schemes, where the system SNR is set to 20 dB and the number of multicast objects varies from 2 to 100.

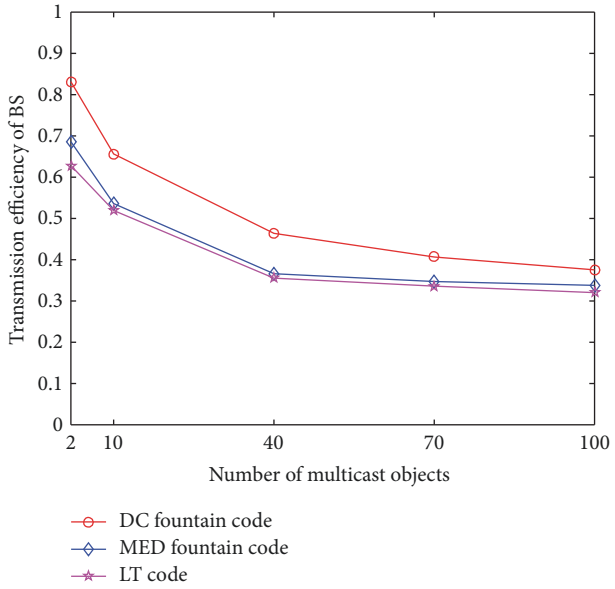

Figure 8: Transmission efficiency comparison between the proposed scheme and baseline schemes, where the system SNR is set to 20 dB and the number of multicast objects varies from 2 to 100.

than two baselines schemes. When the number of multicast objects exceeds 40, the recovering proportion of the proposed scheme keeps pace with MED Fountain Code. Figure 8 shows that all curves drop while the proposed curve is still higher than others with the number of objects varying from 2 to 10. Besides, the transmission efficiency for the proposed scheme still remains higher than 0.1 for other two baseline schemes as the number of multicast objects increases above 10.

5.3. Comparison of Simulation and Analysis. In Section 4.2, we made some assumption that M multicast objects receive the fountain packets in a synchronized pace. Thus, to make an effective comparison between simulation results and the theoretical analysis, all multicast objects are set to the same received SNR. The total number of data packets denoted as K is 16 and system SNR varies from 15 dB to 35 dB.

Figure 9 demonstrates the intercept probability comparison between the theoretical analysis and simulation

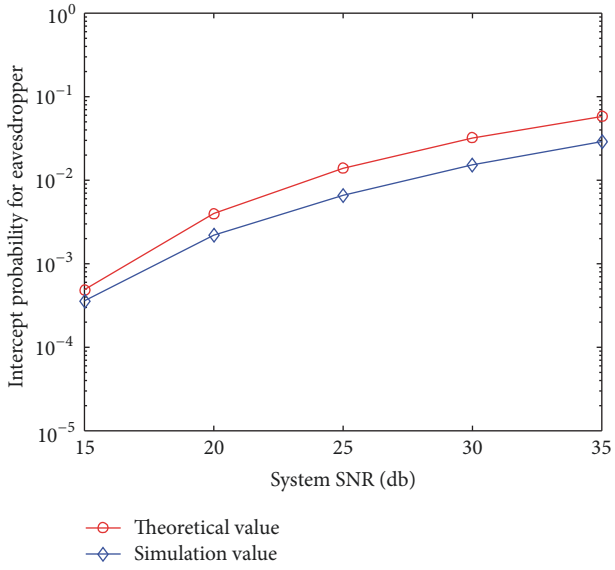

FIGURE 9: Intercept probability comparison between the theoretical analysis and simulation, where the system SNR varies from 15 dB to 35 dB.

results. The simulation results are about 40% lower than the theoretical value of the upper bound. With the system SNR varying, the two curves increase in the same degree.

6. Conclusions

This paper presented a novel fountain-encoding scheme aimed at achieving data security in the multicast system of the Internet of Things, which can dynamically change the encoding rules in order to reduce the intercept probability. By requiring multicast objects to provide feedback on ACK signals, the transmitter simulates the decoding procedures and records the index of recovered data packets. Based on these recorded information, the transmitter completes the dynamical fountain-encoding design which targets increasing the decoding rates of the multicast objects. In this manner, multicast objects can complete decoding quickly while the eavesdropper hardly overhears enough fountain packets to decode the original data, which effectively reduces the intercept probability for Eve. In addition, the performance analysis and simulation results are also performed to demonstrate that the proposed scheme outperforms the traditional nondynamical fountain-encoding schemes with the lower intercept probability and higher transmission efficiency while imposing a little accredited complexity for multicast networks.

Parameters in Analysis

M: The number of multicast objects
K: The number of total data packets
ρ: System SNR
η: Path loss exponent
a_n, g_n, γ_{pn}: Fitting parameters of (14)
γ_{BO}/γ_{BE}: The received SNR from BS to *group objects* (all multicast objects)/*Eve*
h_{BO}/h_{BE}: The Rayleigh fading channel coefficient between BS and *group objects*/*Eve*
d_{BO}/d_{BE}: The distance between BS and *group objects*/*Eve*
$P_{BO,Up}/P_{BE,Up}$: The upper bound of the probability of loss packet from BS to *group objects*/*Eve*
$\overline{P}_{BO,Up}/\overline{P}_{BE,Up}$: The upper bound of the probability of *not* loss packet from BS to *group objects*/*Eve*
$P_{Intercept}$: The lower bound of intercept probability in Eve.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

Acknowledgments

The research work reported in this paper is supported by the National Natural Science Foundation of China under the Grant nos. 61461136001 and 61671371, the National Science and Technology Major Project under Grant no. 2016ZX03001016-005, Key Research and Development Program of Shaanxi Province under Grant no. 2017ZDXM-GY-012, and Fundamental Research Funds for the Central Universities.

References

[1] "The internet of things," ITU Internet Reports 2005. [Online]. Available: http://www.itu.int/pub/S-POL-IR.IT-2005/e.

[2] D. Singh, G. Tripathi, and A. J. Jara, "A survey of internet-of-things: future vision, architecture, challenges and services," in *Proceedings of the IEEE World Forum on Internet of Things (WF-IoT '14)*, pp. 287–292, Republic of Korea, March 2014.

[3] J. Ma, "Internet-of-Things: Technology evolution and challenges," in *Proceedings of the 2014 IEEE MTT-S International Microwave Symposium, IMS 2014*, USA, June 2014.

[4] Q. Cui, Y. Gu, W. Ni, and R. P. Liu, "Effective capacity of licensed-assisted access in unlicensed spectrum for 5g: from theory to application," *IEEE Journal on Selected Areas in Communications*, vol. 35, no. 8, pp. 1754–1767, 2017.

[5] Q. Du, M. Liu, Q. Xu, H. Song, L. Sun, and P. Ren, "Interference-constrained routing over P2P-share enabled multi-hop D2D networks," *Peer-to-Peer Networking and Applications*, vol. 10, pp. 1–17, 2017.

[6] Q. Du, H. Song, Q. Xu, P. Ren, and L. Sun, "Interference-controlled D2D routing aided by knowledge extraction at cellular infrastructure towards ubiquitous CPS," *Personal and Ubiquitous Computing*, vol. 19, no. 7, pp. 1033–1043, 2015.

[7] Z. Su, Y. Hui, and S. Guo, "D2D-based content delivery with parked vehicles in vehicular social networks," *IEEE Wireless Communications Magazine*, vol. 23, no. 4, pp. 90–95, 2016.

[8] Z. Cai, Z.-Z. Chen, and G. Lin, "A 3.4713-approximation algorithm for the capacitated multicast tree routing problem," *Theoretical Computer Science*, vol. 410, no. 52, pp. 5415–5424, 2009.

[9] Z. Cai, R. Goebel, and G. Lin, "Size-constrained tree partitioning: approximating the multicast k-tree routing problem," *Theoretical Computer Science*, vol. 412, no. 3, pp. 240–245, 2011.

[10] Q. Du and X. Zhang, "Statistical QoS provisionings for wireless unicast/multicast of multi-layer video streams," *IEEE Journal on Selected Areas in Communications*, vol. 28, no. 3, pp. 420–433, 2010.

[11] X. Xu, J. Liu, and X. Tao, "Mobile edge computing enhanced adaptive bitrate video delivery with joint cache and radio resource allocation," *IEEE Access*, vol. 5, pp. 16406–16415, 2017.

[12] G. Araniti, M. Condoluci, P. Scopelliti, A. Molinaro, and A. Iera, "Multicasting over emerging 5G networks: challenges and perspectives," *IEEE Network*, vol. 31, no. 2, pp. 80–89, 2017.

[13] O. Bamasag and K. Y. Toumi, "Efficient multicast authentication in internet of things," in *Proceedings of the 2016 International Conference on Information and Communication Technology Convergence, ICTC 2016*, pp. 429–435, Republic of Korea, October 2016.

[14] Y. Hui, Z. Su, and S. Guo, "Utility based data computing scheme to provide sensing service in internet of things," *IEEE Transactions on Emerging Topics in Computing*, vol. PP, pp. 1-1, 2017.

[15] 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, 14th IEEE International Conference on Smart City and 2nd IEEE International Conference on Data Science and Systems, HPCC/SmartCity/DSS 2016*, pp. 1037–1044, Australia, December 2016.

[16] M. Condoluci, G. Araniti, T. Mahmoodi, and M. Dohler, "Enabling the iot machine age with 5g: machine-type multicast services for innovative real-time applications," *IEEE Access*, vol. 4, pp. 5555–5569, 2016.

[17] B. K. Wadih and M. S. Reza, "A novel machine-to-machine communication strategy using rateless coding for the internet of things," *IEEE Internet of Things Journal*, vol. 3, no. 6, pp. 937–950, 2016.

[18] W. Xu, S. Li, C.-H. Lee, Z. Feng, and J. Lin, "Optimal secure multicast with simultaneous wireless information and power transfer in presence of multiparty eavesdropper collusion," *IEEE Transactions on Vehicular Technology*, vol. 65, no. 11, pp. 9123–9137, 2016.

[19] Q. Yu and C. N. Zhang, "A secure multicast scheme for wireless sensor networks," in *Proceedings of the 2012 3rd FTRA International Conference on Mobile, Ubiquitous, and Intelligent Computing, MUSIC 2012*, pp. 158–163, Canada, June 2012.

[20] H. Niu, M. Iwai, K. Sezaki, L. Sun, and Q. Du, "Exploiting fountain codes for secure wireless delivery," *IEEE Communications Letters*, vol. 18, no. 5, pp. 777–780, 2014.

[21] K. F. Hayajneh and S. Yousefi, "Towards a smart universe: One droplet at a time," in *Proceedings of the 12th IEEE International Wireless Communications and Mobile Computing Conference, IWCMC 2016*, pp. 200–204, Cyprus, September 2016.

[22] M. Luby, "LT codes," in *Proceedings of the 43rd Annual IEEE Symposium on Foundations of Computer Science (FOCS '02)*, pp. 271–280, Vancouver, Canada, November 2002.

[23] Q. Liu, S. Zhou, and G. B. Giannakis, "Cross-layer combining of queuing with adaptive modulation and coding over wireless links," in *Proceedings of the MILCOM 2003 - 2003 IEEE Military Communications Conference*, pp. 717–722, USA, October 2003.

[24] Q. Liu, S. Zhou, and G. B. Giannakis, "Queuing with adaptive modulation and coding over wireless links: cross-layer analysis and design," *IEEE Transactions on Wireless Communications*, vol. 4, no. 3, pp. 1142–1153, 2005.

[25] X. Zhang and Q. Du, "Adaptive low-complexity erasure-correcting code-based protocols for QoS-driven mobile multicast services over wireless networks," *IEEE Transactions on Vehicular Technology*, vol. 55, no. 5, pp. 1633–1647, 2006.