Route Selection Based on Connectivity-Delay-Trust in Public Safety Networks

Jinchuan Tang, *Student Member, IEEE,* Gaojie Chen, *Member, IEEE,* and Justin P. Coon, *Senior Member, IEEE*

***Abstract*—Recently, the mission-critical push-to-talk (MCPTT) system has emerged as the new broadband technology for public safety networks. In this paper, we propose a route selection method based on the connectivity, delay, and trust in the MCPTT system to offer the best connectivity-delay-trust performance. To begin with, the connection probability between a pair of user equipments (UEs) has been analyzed with the interference from other MCPTT groups. Then, the timeliness probability is studied to capture the level of confidence for the delay requirement. Moreover, the trust probability is calculated by a beta reputation system to prevent potential attacks from malicious nodes and ensure secure interactions among the forwarding UEs. By combining three probabilistic results, we investigate the optimal path route selection method based on the Dijkstra's algorithm to find the path, which can meet the requirement of the MCPTT system. The simulation results validate our models and theoretical analysis. The results provide a useful insight in designing the MCPTT system for 5G public safety and disaster relief networks.**

***Index Terms*—Mission-critical, connectivity, delay, trust, route selection.**

I. Introduction

A. Background and motivation

As introduced in the 3rd Generation Partnership Project (3GPP) *Release 13*, mission-critical push-to-talk (MCPTT) provides an enhanced arbitrated method by which two or more users can engage in the mission-critical group communications based upon 3GPP evolved packet system (EPS) services [1]. Floor control is provided in the mission-critical group communications to regulate the access to shared channels and arbitrate transmission request contentions. When multiple requests occur, one UE is guaranteed to talk (i.e. take the floor) while others are either rejected or queued based on the priorities of the users in contention. Overriding the current talker by a higher priority user and limitation of talk time promote the chances for other users to use the service. Further development of mission-critical services such as mission-critical video and mission-critical data created an opportunity to reuse base functionality documented in the stage one requirements for MCPTT [2]. Although mission-critical service on LTE will be primarily targeting public service agencies (PSAs), i.e. police, fire brigade, ambulance, it is still capable of general commercial applications for other industries and service departments such as utility companies and railway stations.

The users from different mission-critical organizations communicate in separate groups for different tasks by using their MCPTT UEs. In many practical off-network scenarios, responders are dispatched to investigate an area that is far away from their affiliated group. To report the situations back to this group in the formats of text messages, recorded voice or video clips, the leading UEs from nearby groups can cooperate to forward the messages in an ad hoc fashion [3]–[5]. To yield a reliable, fast and secure path, the models related to connectivity, delay, and trust need to be addressed for route selection.

B. Related work

Network connectivity is an essential requirement to guarantee reliable communications among UEs. Due to the underlying dynamics of fading and interference [6], the link quality between two wireless node has been studied statistically. The connection probability or the outage probability has been used to study a link quality under the fading channel statistically. The outage probability for cooperative relay network in the presence of inter-cell interference was analyzed in [7]. The probability of full connectivity of high density random networks in confined geometries was developed in [8]. The use of D2D relays as a disaster relief solution and their network performance were studied in [9]. In [10], a systematic cooperative routing scheme named CRCPR was proposed to provide greater robustness against node mobility-induced link breaks. Meanwhile, geographical constraints [11] and some task properties such as rescue missions inside houses on fire could make the group communications exhibit clustering behavior. The interference and outage in clustered wireless ad hoc networks modeled by Matérn cluster and modified Thomas cluster processes were studied in [11]. The performance of modified Thomas clusters in D2D networks based on the distance probability density function was analyzed in [12]. The performance of Matérn clusters based on the newly discovered distance probability density function was addressed in [13]. In [14], a communication-aware route selection strategy was proposed to yield high throughput for ongoing data transmissions. However, it did not consider the clustering behavior of group communications. Meanwhile, the quality of inter-cluster communications in MCPTT networks depends on the call activities of UEs within each cluster, and the call activities are related to the call delay modeling of MCPTT networks. Therefore, the connectivity analysis should be linked to the delay modeling to achieve more accurate results.

This work was supported by EPSRC grant number EP/N002350/1 ("Spatially Embedded Networks").

J. Tang and J. P. Coon are with the Department of Engineering Science, University of Oxford, Parks Road, Oxford, UK, OX1 3PJ, Emails: {jinchuan.tang and justin.coon}@eng.ox.ac.uk.

G. Chen is with the Department of Engineering, University of Leicester, Leicester, UK, LE1 7RH, Email: gaojie.chen@leicester.ac.uk.

During route selection, choosing the forwarding UEs with low latency is desired. The queueing for utilizing the shared resource blocks in the MCPTT group communications decides that the service for forwarding the messages is not always immediately available. Consequently, the guaranteed deadline requirement from classic real-time systems is infeasible and a timeliness probabilistic model is proposed to capture the level of confidence for the delay requirement [15]. The *timeliness probability* is defined to be the probability that a transmission request needs to wait for at most a given time threshold τ until the resources blocks are available. To study the transmission request delay in each cluster head for message forwarding, the trunking theory is used. Two major classes of trunked radio systems named lost call cleared (LCC) and lost call delayed (LCD) systems were studied in [16]. The former does not provide a queue for requests. The latter, however, allows a transmission request to the queue, in a buffer, and wait until a server is available, which fits the flow control for MCPPT service. Meanwhile, a probabilistic metric was proposed in [15], where the Gaussian distribution was used to approximate the distribution of end-to-end delay. The interflow and intraflow interferences have been considered in [17] to reduce packet losses and retransmissions for shorter delay.

Secure message delivery is very crucial to the mission-critical service since nodes may not cooperate or act maliciously towards the message forwarding, which can cause the received message to be confused or beyond comprehension. Secure sockets layer (SSL) and some other traditional cryptographic tools attach a message authentication code to the transmitted data so that the UE at the destination can detect the malicious behaviors of forwarding UEs such as data tampering [18]. However, by using SSL alone, it is still very challenging for the UE at the destination to locate the malicious forwarding UE(s) along a path and report them back to the source via a different path where the behaviors of the UEs along the new path also need to be confirmed. Hence, to determine whether a neighboring node will assist to forward the messages in a timely manner, trust establishment schemes have been proposed [18], [19]. Trust exploits the fact that a source UE can monitor the forwarding operation of the neighboring UEs due to the broadcast nature of radio. Based on an accumulated number of observations on whether each time the forwarding is successful, the source UE can choose to trust one neighboring UE in the future forwarding operations. Given the number of observations on the forwarding operations over a link, the trust probability of a link can be formulated based on the beta probability density functions which have been actively used in Bayesian inference [20]. An early study on the trust establishment in a mobile ad hoc network was conducted in [21], where the forwarded packet was buffered and checked with the original message for a match. A passive monitoring of forwarded data traffic to estimate the behavior of a node without buffer was proposed in [19]. The proximity based trust and experience-based trust modelings in random wireless networks were proposed in [22]. The selective packet drop behavior in the selfish relay has been studied in [23] for route selection, which ignored the effects of connectivity and delay.

C. Contributions and paper structure

To the best of our knowledge, this is the first paper to propose a route selection method based on *connection, timeliness*, and *trust* probabilities for mission-critical group communications. The contributions of the paper are:

1) We characterized the connection probability among the UEs in an MCPTT system in the presence of the interference coming from other MCPTT clusters.
2) We proposed a robust trust probability which considered the confidence of the trust as a result of the number of iterations in a beta reputation system.
3) We firstly proposed a route selection method which simultaneously considered the connection, timeliness, and trust probabilities for route selection in an MCPTT public safety network.

As a result, the proposed route selection method could provide a useful guideline to design the MCPTT system for 5G public safety and disaster relief networks.

The rest of the paper is structured as follows: Table I gives the notation and symbols that we use throughout the paper. Section II begins with a description of the system model and addresses the probabilistic models for connection, delay, and trust of a given link. Section III focuses on the route selection based on the three probabilistic models mentioned above. Section IV gives the simulation results and discussion, and Section V concludes the paper.

II. System Model

A. Network layout

As shown in Fig. 1, K number of mission-critical groups are randomly distributed on the plane. We focus on choosing a multi-hop to forward messages from one communication group to another in a mission-critical public safety network working in the off-network mode. We assume that each group forms a cluster with radius R, and there are m_i members and one group leader within cluster i. The group leader is fixed at the cluster center, and the group members are uniformly distributed within the cluster. The group leaders' UEs work as cluster heads and are automatically authorized as the member of other groups. Thus, the cluster head is capable of forwarding messages from one group to another. The spatial distribution of UEs during each hop is assumed to be mutually independent. According to the standard in [24], the talker is in charge of the flow arbitration, and the floor request queue will be transferred from the former talking UE to the new talking UE in the off-network mode. The flow control module for each cluster is assumed to use $M/M/1$ queuing system, where two Ms, in turn, denote the memoryless Poisson distribution of the call requests process and exponential distribution of the call holding time [16], [25], and the number 1 indicates that a single server exists for the queue because at most one UE within a group is allowed to transmit at a time. During the busy time, the call requests from a user in cluster i are assumed to be Poisson distributed with an average rate of λ_{u_i} calls per minute, and a user in any cluster holds a call for τ_{hold} seconds in average. The holding time is assumed to be exponentially distributed [25]. The entire number of users in cluster i is

TABLE I: Notation and Symbols

Symbol	Description
R	Radius of a cluster
λ_{u_i}	Mean call rate per user in cluster i
τ_{hold}	Average call holding time of a user
P_d	Transmit power of each UE
G_e	Gain due to coding and antennas
I_j	Interference measured at UE j
P_{kj}	Received power at UE j from UE k
d_{kj}	Pairwise distance between UEs k and j
η	Path loss exponent
$\lvert h_{kj}\rvert^2$	Instant power of Rayleigh fading
E_k	Event: the head transmits in active cluster k
$\overline{\mathrm{E}}_k$	Event: a member transmits in active cluster k
$\mathcal{L}_I^h(s \mid a_{kj})$	Laplace transform of the interference from heads k to j given E_k
$\mathbb{P}\{\cdot\}$	Probability of an event
Q_i	Event: a call is delayed in cluster i
$\mathbb{P}\{Q_k\}$	Blocking probability in cluster k
ζ	SINR threshold
H_{ij}	Connection probability from cluster heads i to j
C	Indices of all clusters
A_i	Traffic intensity
μ	Mean service rate
N	Number of servers
W_i	Delay of a user in cluster i
τ	Delay threshold in a cluster
D_j, D_{ij}	Timeliness probability from cluster heads i to j
$\alpha_{ij}-1$	Number of successful interactions from heads i to j
$\beta_{ij}-1$	Number of failed interactions from heads i to j
θ_{ij}	Probability of successful interactions
T_{ij}^{mean}	Mean trust probability from cluster heads i to j
$\mathcal{O}$	Observed interactions between heads i and j
c	Confidence interval of θ_{ij}
T_{ij}^{robust}	Robust trust probability from cluster heads i to j
$\mathbf{H}/\mathbf{D}/\mathbf{T}$	Probability matrices of connectivity/delay/trust
$H_t/D_t/T_t$	Thresholds of connection/timeliness/trust
$\mathbf{R}$	Link cost matrix
J	End-to-end path
l_i	Index of forwarding cluster head i

m_i+1. Therefore, $(m_i+1)\lambda_{u_i}$ is the total mean call arrival rate. The transmit power of each UE is P_d. The gain due to coding, transmitting antenna and receiving antenna is G_e. We assume that all channels experience block Rayleigh fading and the channels remain constant over one block but vary independently from one block to another. The corresponding channel gains are independently exponentially distributed with unit mean.

B. Connectivity modeling

The connectivity is a study of the link performance in the presence of path loss, multipath fading, interference, and noise. By taking connectivity into consideration, a path with qualified link performance will be used for route selection.

1) Signal to interference-plus-noise ratio (SINR): The receiver of a UE captures not only the signal but also the interference from the UEs who are transmitting simultaneously [26]. The total interference power measured at a receiving UE j is given by

$$I_j = \sum_{k\in L} P_{kj} = \sum_{k\in L} G_e \ell(d_{kj}) |h_{kj}|^2 P_d, \tag{1}$$

where L denotes the set of interferers; P_{kj} is the received interference power at UE j from the UE $k \in L$; $\ell(d_{kj}) = (\lambda/4\pi)^2 d_{kj}^{-\eta}$, where λ represents the carrier wavelength, d_{kj} is the pairwise distance between UEs k and j, and η is the path loss exponent; $|h_{kj}|^2$ is the instant power of Rayleigh fading. The SINR of receiving signal from UE i at UE j is given by

$$\mathrm{SINR}_{ij} = \frac{P_{ij}}{N_0 + I_j}, \tag{2}$$

where N_0 is the additive white Gaussian noise (AWGN) power at each UE. Next, we characterize an average interference based on the spatial distributions of the simultaneous transmitting UEs within the clusters.

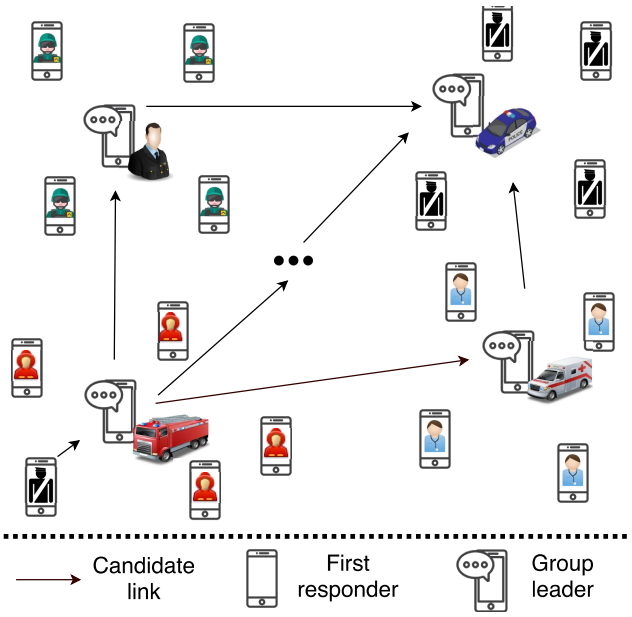


Fig. 1: A mission-critical public safety scenario.

2) Interference from one cluster: According to the floor control in the MCPTT group communications, the UEs of a cluster work in a delay and served manner so that at most one UE is transmitting on the shared resource blocks. For simplicity of notation, we let a cluster and the cluster head inside have the same index. Given that a cluster k is active due to a UE is transmitting, let E_k denote the event that cluster head k is transmitting and $\overline{\mathrm{E}}_k$ denote the event that a cluster member of k is transmitting. The Laplace transform of the interference from cluster heads k to j given E_k is written as

$$\mathcal{L}_I^h(s \mid a_{kj}) = \frac{1}{1 + sG_e\ell(a_{kj})P_d}, \tag{3}$$

where a_{kj} is the distance between cluster heads k and j as shown in Fig. 2. When the members of cluster k need to transmit, at most one UE is active. Hence, the Laplace transform of the interference from a member, which is uniformly distributed in cluster k, to the head of cluster j given $\overline{\mathrm{E}}_k$ is written as

$$\mathcal{L}_I^m(s \mid a_{kj}) = \int_0^R \int_0^{2\pi} \frac{1}{1 + sGd(a_{kj}, b_k, \theta_k)^{-\eta}} \frac{b_k}{\pi R^2} \mathrm{d}b_k \mathrm{d}\theta_k, \tag{4}$$

where $d(a_{kj}, b_k, \theta_k) = \sqrt{a_{kj}^2 + b_k^2 - 2a_{kj}b_k\cos\theta_k}$ is the distance between a member of cluster k and the head of cluster j by using the Law of Cosines as shown in Fig. 2, and b_k is

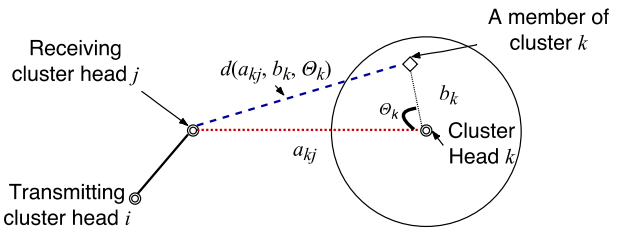


Fig. 2: The interference is coming from the head or member of cluster k when cluster head i is transmitting a message to cluster head j.

the distance between cluster head k and a possible location of a member of cluster k; $G = G_e P_d (\lambda/4\pi)^2$.

A closed-form expression for (3) exists as $\eta = 2$, which is given by

$$\mathcal{L}_I^m(s \mid a_{kj}) = 1 + \frac{Gs}{R^2}\Bigg(\ln(2Gs) - \ln\Big(Gs + R^2 - a_{kj}^2 + \sqrt{(Gs + (R - a_{kj})^2)(Gs + (R + a_{kj})^2)}\Big)\Bigg). \tag{5}$$

For $\eta > 2$, instead of using (4), $\mathcal{L}_I^m(s \mid a_{kj})$ can also be achieved by numerically evaluating a single integral, which is written as

$$\mathcal{L}_I^m(s \mid a_{kj}) = \int_{a_{kj}-R}^{a_{kj}+R} \frac{f_{R_d}(x \mid a_{kj})}{1 + sGx^{-\eta}} \mathrm{d}x, \tag{6}$$

where

$$f_{R_d}(r_d \mid R_y) = \frac{c(r_d)}{\pi R^2}, \tag{7}$$

$$c(r_d) = \begin{cases} 2\pi r_d, & 0 \le r_d \le R - R_y \\ 2\pi r_d - c_1(r_d), & R - R_y < r_d \text{ and } r_d^2 \le R^2 - R_y^2 \\ c_1(r_d), & R^2 - R_y^2 < r_d^2 \\ 0, & \text{otherwise,} \end{cases} \tag{8}$$

and $c_1(r_d)$ is defined by (9) at the top of the next page.

The Laplace transform of the interference from cluster k to cluster head j is written as

$$\mathcal{L}_I(s \mid a_{kj}) = \mathbb{P}\{Q_k\}\big[\mathcal{L}_I^h(s \mid a_{kj})\mathbb{P}\{\mathrm{E}_k\} + \mathcal{L}_I^m(s \mid a_{kj})\mathbb{P}\{\overline{\mathrm{E}}_k\}\big] + \mathbb{P}\{\overline{Q}_k\}, \tag{10}$$

where $\mathbb{P}\{\cdot\}$ denotes the probability of an event. Assuming that the head and members of cluster k statistically have equal opportunities to access the resource blocks, $\mathbb{P}\{\mathrm{E}_k\} = 1/(1 + m_k)$. $\mathbb{P}\{Q_k\}$ is the blocking probability that the resource blocks have already been occupied by another UE when a UE requests its transmission. A detail discussion about blocking probability is given in Section II-C2. Therefore, the Laplace transform of the interference in (10) considers both the spatial distributions and transmission activities of UEs within clusters, and it is used to characterize the connection probability as follows.

3) Connection probability: The connection probability of a link is the likelihood that the SINR of the link is higher than a predetermined threshold $\zeta = 2^t - 1$ with link spectrum efficiency t. The connection probability from cluster heads i to j, can be written as

$$H_{ij} = \mathbb{P}\{\mathrm{SINR}_{ij} > \zeta\} = \exp\left(-\frac{\zeta \mathrm{N}_0}{g(d_{ij})}\right) \prod_{k \in C \setminus i,j} \mathcal{L}_I\left(\frac{\zeta}{g(d_{ij})} \,\middle|\, a_{kj}\right), \tag{11}$$

where C denotes the indices of all clusters.

According to (10), the number of UEs and their transmission requests within a cluster will affect the amount of interference to other links; consequently, it will affect the connection probability given by (11). Meanwhile, the request to transmit a message will be queued if the resource blocks are not immediately available. Therefore, it is of great importance to study the delay in an MCPTT network for route selection.

C. Delay modeling

1) The lost call delayed (LCD) system: The flow control in MCPTT group communications can be modeled as an LCD system where the incoming transmission request is held in a queue until an in-progress transmission terminates and the resources blocks become free [16]. The blocking probability is used to characterize the likelihood that the resources blocks are already in use when a new call request happens. If no resource blocks are immediately available after a call request to a cluster, it will be helpful to know the level of confidence that a call can be served within τ seconds.

2) Blocking probability: Let Q_i denote the event that a call is delayed in the queue of cluster head i. The blocking probability of cluster head i is given by the Erlang C formula as following:

$$\mathbb{P}\{Q_i\} = \frac{\frac{A_i^N}{N!}\frac{N}{N - A_i}}{\left(\sum_{n=0}^{N-1} \frac{A_i^n}{n!}\right) + \frac{A_i^N}{N!}\frac{N}{N - A_i}}, \tag{12}$$

where $A_i = (m_i + 1)\lambda_{u_i}/\mu$ is the traffic intensity, $\mu = 1/\tau_{hold}$ is the mean service rate, and τ_{hold} is the average duration of a call; N is the number of servers. $0 < A_i < 1$ is required so that the system is stable; otherwise, it would result in a queue which grows unboundedly. For the group communications of MCPTT, the resource blocks are utilized by a UE per unit time. Therefore, the number of servers N for a queue is one. Consequently, $\mathbb{P}\{Q_i\} = A_i$, and (10) is expanded as

$$\mathcal{L}_I(s \mid a_{kj}) = A_i\left[\frac{\mathcal{L}_I^h(s \mid a_{kj})}{1 + m_i} + \frac{m_i \mathcal{L}_I^m(s \mid a_{kj})}{1 + m_i}\right] + 1 - A_i. \tag{13}$$

3) Timeliness probability: Meanwhile, if no resource blocks are immediately available, the call will be delayed. In steady-state, the delay time for a call request in the queue obeys exponential distribution [25]. Let the random variable W_i denote the delay of a user in cluster i, the probability of a call waiting for more than τ seconds in the queue is given by

$$\mathbb{P}\{W_i > \tau \mid Q_i\} = e^{-\frac{N - A_i}{\tau_{hold}}\tau} = e^{-\frac{1 - A_i}{\tau_{hold}}\tau}, \tag{14}$$

$$c_1(r_d) = \begin{cases} 2r_d \arcsin \frac{\sqrt{4R_y^2 r_d^2 - (R_y^2 - R^2 + r_d^2)^2}}{2R_y r_d}, & (-R_y + R - r_d)(-R_y - R + r_d)(-R_y + R + r_d) \geq 0 \\ 0, & \text{otherwise.} \end{cases} \tag{9}$$

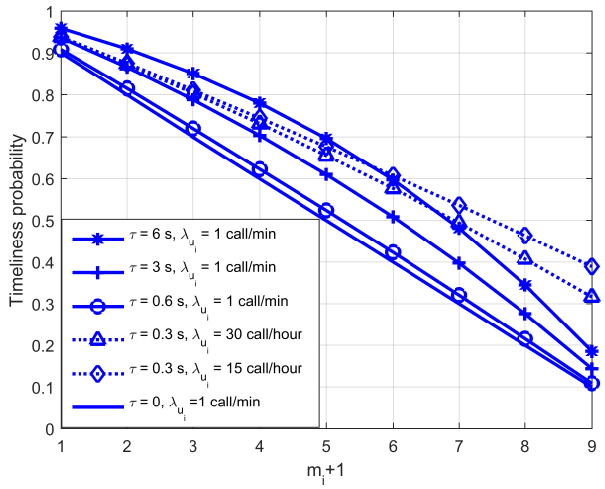


Fig. 3: The timeliness probability of cluster i under different parameters, and $\tau_{hold} = 6$ s.

where τ is the delay time of interest. Hence, the timeliness probability that a caller needs to wait for at most τ seconds to be served is given by

$$\begin{aligned} D_i &= \mathbb{P}\{W_i \leq \tau\} \\ &= 1 - \mathbb{P}\{W_i > \tau \mid Q_i\}\mathbb{P}\{Q_i\} \\ &= 1 - A_i e^{-\frac{1-A_i}{\tau_{hold}}\tau}. \end{aligned} \tag{15}$$

Thus, we define the timeliness probability from cluster heads i to j as $D_{ij} = D_j$. Apparently, if the selected threshold τ is 0, the timeliness probability will be solely decided by $1 - A_i$, which is a linear function of m_i. Fig. 3 gives the timeliness probabilities in cluster i under different values of delay threshold (τ) and the average number of calls per unit time (λ_{u_i}). It is clear that as the number of users increases, the timeliness probability drops heavily. The timeliness probability can be grown by either increasing τ or decreasing λ_{u_i}.

D. Trust modelling

Trust is an expectation of technically competent role performance. It is expected to play a major role for secure message forwarding. As we seen in Fig. 4, an attacker (or a misbehaving node) can modify the messages while it is forwarding. This would create confusion and misjudgment at the receiver. To rate the trustworthiness of a link, we adopted the beta reputation system to the binary rating on whether each forwarding operation (interaction) is redeemed to be successful or not.

1) Beta reputation system and mean trust probability: The expression for the posterior probability estimation of binary events can be represented as beta distribution functions [20]. Let $\alpha_{ij} - 1$ denote the number of previously successful

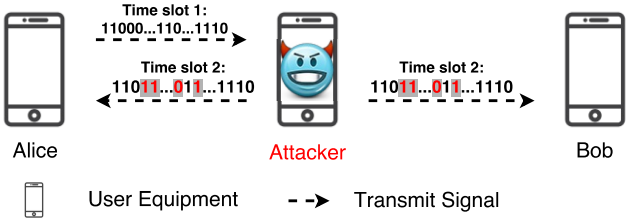


Fig. 4: Data tampering attack by the forwarding UE.

direct forwarding operations from cluster heads i to j, while $\beta_{ij} - 1$ denote the number of previously failed operations. The probability density function of observing the successful forwarding operations in the future is a beta function given by

$$f(\theta_{ij} \mid \alpha_{ij}, \beta_{ij}) = \frac{{\theta_{ij}}^{\alpha_{ij}-1}(1-\theta_{ij})^{\beta_{ij}-1}}{\text{Beta}(\alpha_{ij}, \beta_{ij})}, \tag{16}$$

where

$$\text{Beta}(\alpha_{ij}, \beta_{ij}) = \frac{\Gamma(\alpha_{ij})\Gamma(\beta_{ij})}{\Gamma(\alpha_{ij} + \beta_{ij})}, \tag{17}$$

$\theta_{ij} \in [0, 1]$ denotes the probability of observing successful forwarding operations in the future, and shape parameters $\alpha_{ij}, \beta_{ij} > 0$. The *mean trust probability* from cluster heads i to j is the probability expectation value of the reputation function, which is written as

$$T_{ij}^{\text{mean}} = \text{E}[\theta_{ij} \mid \mathcal{O}] = \frac{\alpha_{ij}}{\alpha_{ij} + \beta_{ij}}, \tag{18}$$

where $\mathcal{O}$ denotes the information about the observed interactions between cluster heads i and j until now. When the number of interactions is very large, T_{ij}^{mean} is the accurate mean trust probability.

2) Confidence of trust and robust trust probability: In an MCPTT network, two cluster heads may have very few interactions due to lack of forwarding interest, early stage of a network running, and network topology changes. Thus, adequate observations are missing to calculate the accurate mean trust probability. The confidence intervals of trust can be used to infer the robustness of the trust from a limited number of observations.

A confidence interval c of θ_{ij} makes sure that the θ_{ij} will lie in a probability range with $c \times 100\%$ certainty. According to [27], the Bayesian-based lower confidence bound for θ_{ij} is given by

$$T_{ij}^{\text{lower}} = \text{Beta}^{-1}\left(\frac{1-c}{2}; \alpha_{ij}, \beta_{ij}\right), \tag{19}$$

where $\text{Beta}^{-1}(\text{c}; \text{a}, \text{b})$ is the c-th quantile function of a beta distribution, i.e. a beta inverse cumulative distribution function, with shape parameters a and b. Compared with traditional confidence interval estimators such as the normal approximation and the Clopper & Pearson approach, Bayesian

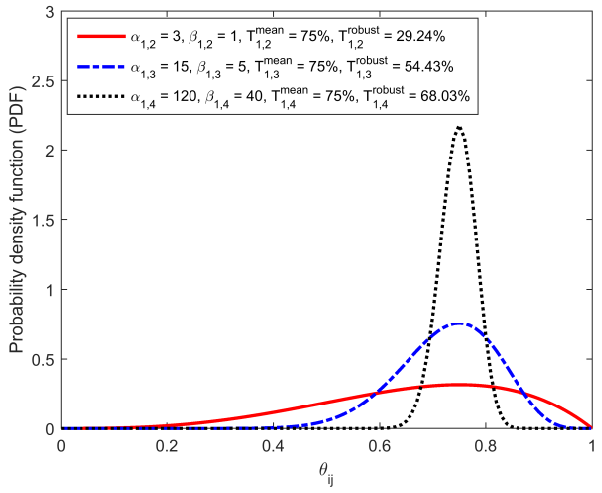


Fig. 5: The distribution of observing successful forwarding operations in the future after the observations so far given by $(\alpha_{ij}, \beta_{ij})$.

confidence technique is more capable of providing a mean level of coverage close to the nominal level even for a small-to-intermediate number of interactions [27][1]. Since the accurate mean trust probability can reach as low as T_{ij}^{lower} for a given confidence interval c, we define this lower bound as the *robust trust probability* T_{ij}^{robust}. As a result of the above discussion, we have formulated two trust probabilities, namely, mean and robust trust probabilities. The latter has considered the uncertainty existed in the proportion of success interactions in a small number of observations.

Fig. 5 gives the confidence of the trust under a different number of forwarding operations. It is clear that although the mean trust probabilities are the same, the robust trust probabilities vary. Thus, the robust trust probabilities can help to differentiate the links with the same mean trust probabilities. Meanwhile, robust trust can also give different ranking results when the mean trust probabilities are not the same. For example, compared $(\alpha_{1,5} = 13, \beta_{1,5} = 4)$ with $(\alpha_{1,6} = 21, \beta_{1,6} = 7)$, we have $T_{1,5}^{\text{mean}} = 0.7647 > T_{1,6}^{\text{mean}} = 0.75$. But $T_{1,5}^{\text{robust}} = 0.5435 < T_{1,6}^{\text{robust}} = 0.5774$, which implies that the link from cluster heads 1 to 6 is more robust than the link from cluster heads 1 to 5 in terms of trust even though the latter has a better mean trust probability.

III. Route Selection

In this section, we consider a route selection method where the selection process explicitly takes into account the connectivity, delay, and trust of an MCPTT network. We assume that the connection, timeliness, and trust probabilities of each link are exchanged among the cluster heads. The cryptographic primitives are used to authenticate and protect the integrity of the data [21]. In many multi-criteria route selection algorithms, the criteria are normally weighted and mapped to the costs of the links. Although the measurements of the connectivity, delay, and trust are all probability values, the distributions of them are different. Hence, it is challenging to find proper weights to the probabilities. To make progress, we propose the following steps to achieve the costs of links for route selection.

Step 1: Based on the exchanged probability values regarding the connectivity, delay, and trust among the cluster heads, the source cluster head forms three adjacency matrices, which are given by

$$\begin{aligned} \mathbf{H} &= (H_{ij}) \in [0,1]^{K\times K}, \\ \mathbf{D} &= (D_{ij}) \in [0,1]^{K\times K}, \\ \mathbf{T} &= (T_{ij}\ ) \in [0,1]^{K\times K}, \end{aligned} \tag{20}$$

where each element of the matrices represents the relationships between two links regarding connection, timeliness, and trust probabilities; the elements on the diagonal of the matrices in (20) are set to be one.

Step 2: Define H_t, D_t, and T_t as the thresholds of the connection, timeliness, and trust probabilities, respectively. To define the thresholds that are appropriate to the environment, a general guideline is given as follows for reference: Threshold H_t can be calculated based on the pairwise connection probability in (13) with the exchanged information on clusters and their locations. Among the calculated connection probabilities, the threshold is chosen such that a predefined percentage of the nodes scores above that threshold. Threshold D_t can be obtained by (15), where the average duration of a call τ_{hold} is achieved by previous experience. Threshold T_t can be given by (19) with the anticipated interactive results on α and β that is controlled by risk assessment. A criterion from the connectivity, delay, and trust is specified as the basic criterion for route selection, and the route selection is also constrained by the thresholds of other two criteria.

Step 3: For the route selection strategy based on connectivity, the following requirements must be satisfied: If $T_{ij} \le T_t$ or $D_{ij} \le D_t$, the cost of the directional link i, j will be 0; otherwise, the cost of the same link will be H_{ij}. The resultant adjacency matrix for the cost of links is given by

$$\mathbf{R} = (R_{ij}) \in [0,1]^{K\times K}, \tag{21}$$

where

$$R_{ij} = \begin{cases} H_{ij}, & T_{ij} > T_t \text{ and } D_{ij} > D_t \\ 0, & \text{otherwise.} \end{cases} \tag{22}$$

The similar method will apply to delay or trust if either of them is the basic criterion for route selection.

We propose to find a path with the maximum end-to-end probabilities. For a given path $J = \{l_1, l_2, ..., l_n\}$, l_1 is the index of source forwarding UE, and l_n is the index of final (destination) forwarding UE; n is the number of forwarding UEs involved, and $n \ge 2$. The end-to-end probability of a route is the product of every independent probability of the links consisting of the path. The end-to-end connection,

[1]As the CPUs in UEs become powerful, the computation time of the above bounds is trivial. Meanwhile, normal approximation and the Clopper & Pearson approach will be good candidates if a comparatively small level of accuracy is acceptable for route selection.

timeliness, and trust probabilities of a path are respectively defined as

$$p_{H_J} = \prod_{i=1}^{n-1} H_{l_i l_{i+1}},\ p_{D_J} = \prod_{i=1}^{n-1} D_{l_i l_{i+1}}, \text{ and } p_{T_J} = \prod_{i=1}^{n-1} T_{l_i l_{i+1}}. \tag{23}$$

Many route algorithms have been proposed to find the shortest path [25]. Among these algorithms, the Dijkstra's algorithm is designed to find a path with the minimum sum of link costs. To find a path with the maximum multiplication of probabilities with the Dijkstra's algorithm, we input $-\log \mathbf{R}$ with the indices of source and destination cluster heads to the Dijkstra's algorithm. The steps of the route selection method and the interface of the Dijkstra's algorithm are summarized in Algorithms 1 and 2, respectively.

Algorithm 1: The steps of the route selection method.

Data: $\mathbf{H}, \mathbf{D}, \mathbf{T}, H_t, D_t, T_t, l_1$, and l_n.
Result: Path J.
if *Connectivity-based* **then**
  $\mathbf{R} = \mathbf{H}$;
  for $i, j = 0 \rightarrow K$ **do**
    if $T_{ij} \leq T_t$ *or* $D_{ij} \leq D_t$ **then**
      $R_{ij} = 0$;
    end
  end
else if *Delay-based* **then**
  $\mathbf{R} = \mathbf{D}$;
  for $i, j = 0 \rightarrow K$ **do**
    if $T_{ij} \leq T_t$ *or* $H_{ij} \leq H_t$ **then**
      $R_{ij} = 0$;
    end
  end
else
  $\mathbf{R} = \mathbf{T}$;
  for $i, j = 0 \rightarrow K$ **do**
    if $H_{ij} \leq H_t$ *or* $D_{ij} \leq D_t$ **then**
      $R_{ij} = 0$;
    end
  end
end
J =Dijkstra $(-\log \mathbf{R}, l_1, l_n)$;

Algorithm 2: The interface of Dijkstra's algorithm.

function J =Dijkstra $(\mathbf{C}, l_1, l_n)$;
Input : $\mathbf{C}$: adjacency cost matrix; l_1: index of source; l_n: index of destination.
Output: J: the path with minimum end to end costs.

IV. Simulation and Discussions

In this section, we provide simulations to validate the route selection method detailed above. The parameters used in the simulation are given by Table II. The given link spectrum efficiency and bandwidth offer a target rate of 1.2 Mbps for group communications, which aims to fulfill the speed requirement for forwarding recorded messages and even holding a high-definition video call (720p, 30 frames/sec by H.264 profile). The average holding time of 6 seconds is long enough for sending approximately three pictures of the scenes taken by an eight-megapixel mobile phone each time at 1.2 Mbps. There are 16 MCPTT clusters deployed on the plane. The cluster 1 at $(0, 0)$ needs to send the messages to cluster 16 at $(1000, 1000)$. The rest of the clusters are randomly deployed and could cooperate to forward the messages. For a given snapshot of the randomly deployed clusters, the route selection method is run to get a series of cluster heads for forwarding messages. The connection, timeliness, and trust probabilities of the links are exchanged among the cluster heads by cryptographic tools [21]. The simulations results are obtained by averaging over 10^4 independent Monte Carlo trials.

Fig. 6 shows the route selection results for a snapshot of a randomly deployed MCPTT clusters. The route selection is

TABLE II: System Parameters

Parameter	Value
Area	1 km × 1 km
Transmission bandwidth B	20 MHz
Duplex mode	Half duplex
Thermal noise power density	-174 dBm/Hz
Cluster radius R	155 m
Transmitting power level P_d	11 dBm
Coding gain	0 dB
Transmitting antenna gain	0 dBi
Receiving antenna gain	0 dBi
Transceiver noise figure	9 dB
Link spectrum efficiency	0.06 bit/s/Hz
Carrier frequency	2 GHz
Path loss exponent η	2.7
Waiting threshold per hop τ	100 ms
Number of servers	1
Average holding time	6 seconds
Mean call rate of a user λ_u	1 call/min
Route selection algorithm	Dijkstra's
Simulation iterations	10^4

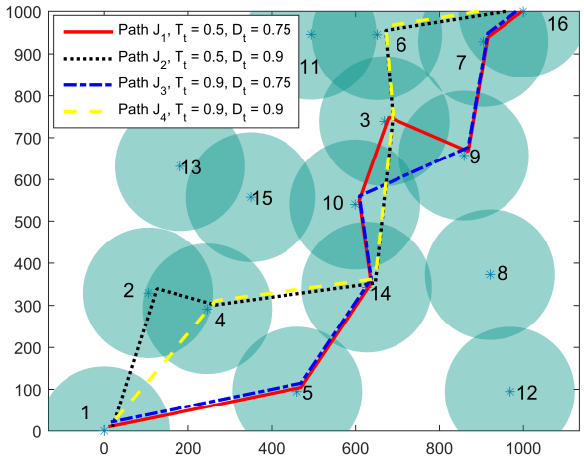


Fig. 6: The route selection results based on connectivity and constrained by T_t and D_t for a snapshot of a randomly deployed MCPTT clusters. The trust is calculated based on the mean trust probability.

based on the link connection probabilities and constrained by T_t and D_t. Table III gives the coordinates of the cluster heads and the number of cluster members. The selected paths and their end-to-end connection probabilities are listed as follows:

- Path $J_1 = \{1, 5, 14, 10, 3, 9, 7, 16\}$, and $P_{H_{J_1}} = 0.9532$.
- Path $J_2 = \{1, 4, 14, 3, 6, 16\}$, and $P_{H_{J_2}} = 0.8975$.
- Path $J_3 = \{1, 5, 14, 10, 9, 7, 16\}$, and $P_{H_{J_3}} = 0.9512$.
- Path $J_4 = \{1, 4, 14, 3, 6, 16\}$, and $P_{H_{J_4}} = 0.8926$.

Compared J_1 with J_2, the higher the threshold D_t, the smaller the end-to-end connection probability. This is because, as D_t increases, the cluster heads who can form paths with better end-to-end connection probabilities may not be chosen if the consisting links by the heads could not satisfy a higher timeliness probability threshold. The similar discussion could be applied to J_3 and J_4. J_2 and J_4 which are forking from cluster 1 to cluster 2 and 4 separately imply cluster head 4 could not be chosen as forwarding head as $T_t = 0.9$, because $P_{H_{J_2}} > P_{H_{J_4}}$ and the rest links of the two paths are the same. The same applies to the forking from cluster head 10 to cluster head 3 and 9 for J_1 and J_3.

Fig. 7 gives the route selection results for a snapshot of a randomly deployed MCPTT clusters. The route selection is based on link timeliness probabilities and constrained by T_t and H_t. $H_{1,16}$ is set to be smaller than H_t so that there is no direct route from source to destination. Thus, the delay and trust among the forwarding UEs need to be considered. According to (15), the delay of the links to cluster i is relying on m_i. The paths and their end-to-end timeliness probabilities are listed as follows:

- Path $J_1 = \{1, 11, 16\}$, and $P_{D_{J_1}} = 0.8283$.
- Path $J_2 = \{1, 4, 3, 16\}$, and $P_{D_{J_2}} = 0.7539$.
- Path $J_3 = \{1, 2, 15, 6, 16\}$, and $P_{D_{J_3}} = 0.6416$.
- Path $J_4 = \{1, 12, 16\}$, and $P_{D_{J_4}} = 0.8283$.

From J_1 to J_3, one can easily see that the end-to-end timeliness probability is decreasing as H_t is increasing. It further implies that if there are several clusters which have the same least number of cluster members and also meet the thresholds requirements for route selection, one route formed by them with the least number of hops will be selected. Besides, the reason that J_1 is selected when $T_t = 0.5, H_t = 0.75$ instead of J_4, although they have the same number of users within, is due to the implementation of Dijkstra's algorithm.

Fig. 8 gives the route selection results based on link trust probabilities and constrained by D_t and H_t. Among the given paths, J_1 and J_2 are selected based on mean trust probabilities and J_3 and J_4 are based on robust trust probabilities with $c = 0.95$. J_1 and J_3 shows that two-hop routes are available for route selection, and the route via cluster 14 gives the best end-to-end trust probabilities for both the mean and robust trust probability formulations. J_2 and J_4 show that the routes selected given by the mean and robust trust probabilities could also give different results even though their values of D_t and H_t are the same.

Fig. 9 gives the averaged end-to-end connection and timeliness probabilities after route selections. The proposed route selections are based on connection probabilities and constrained by T_t only (i.e. $D_t = 0$). The average number of users

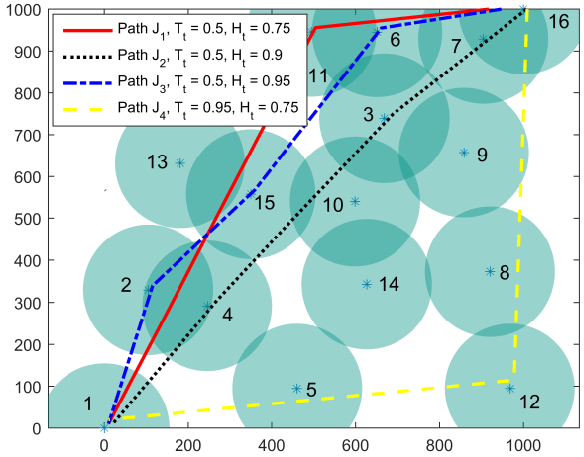


Fig. 7: The route selection results based on link timeliness probabilities and constrained by T_t and H_t for a snapshot of a randomly deployed MCPTT clusters. The trust probability is the same as mean trust probability. The trust is calculated based on the mean trust probability, and $H_{1,16} < H_t$.

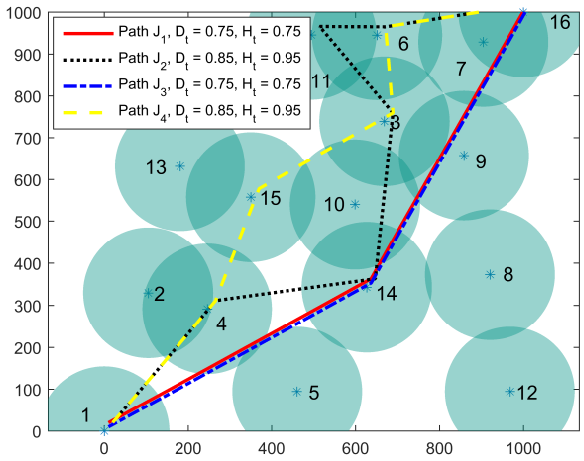


Fig. 8: The route selection is based on link trust probabilities and constrained by D_t and H_t for a snapshot of a randomly deployed MCPTT clusters, and $H_{1,16} < H_t$.

within each cluster is 2. For a snapshot of the random clusters, an increasing number of cluster heads coming consecutively from clusters 2 to 15 are labeled as malicious, and the route selections are performed. A head k is regarded as malicious if both T_{jk} and T_{kj} are less than T_t for any $j \neq k$. To compare, a benchmark of route selection solely based on connectivity [14] is given. When there is only one malicious node on the plane, the end-to-end connection probability for both the benchmark and the proposed route selection method are around 97.5%. As all cluster heads in clusters 2 to 15 become malicious nodes, there is a 5% performance drop in the end-to-end connection probability for the proposed method. Although, the benchmark achieves the best end-to-end connection probability, it does not

TABLE III: Coordinates of Cluster Heads and Number of Cluster Members

Node i	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
x (m)	0	105	669	246	461	651	905	920	858	599	495	968	181	627	350	1000
y (m)	0	330	739	292	95	945	929	373	657	541	946	95	632	343	558	1000
m_i	1	1	1	1	3	1	3	3	3	2	1	1	3	1	2	1

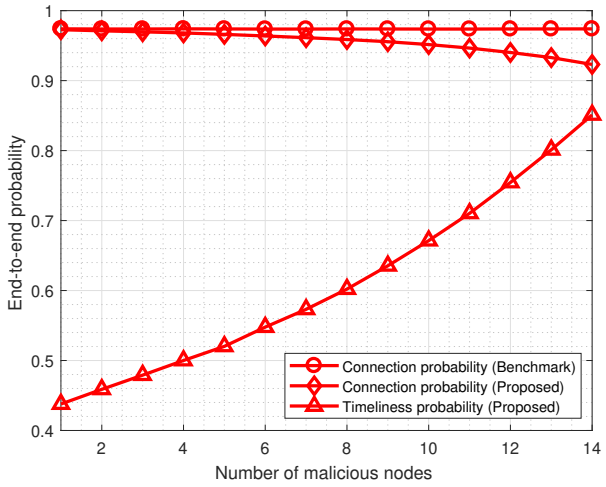


Fig. 9: The averaged end-to-end connection and timeliness probabilities after route selections based on connectivity and constrained by T_t only. $\eta = 2$.

consider the malicious node which makes the path susceptible to attacks. Fig. 9 also shows that the end-to-end connection and timeliness probabilities decreases and increases respectively as the number of malicious cluster heads increases. This is because, as the number of malicious cluster heads increases, the cluster heads who can form paths with better end-to-end connection probabilities has a high chance to become malicious. Hence, they are not available for route selection. The increasing number of malicious cluster heads impose the reduction of the average number of hops for a selected path. For a given m_i, the delay for each cluster is the same. Therefore, as the average number of hops decreases, a higher end-to-end timeliness probability is achieved.

V. Conclusion

In this paper, we have proposed a novel route selection method based on connectivity, delay, and trust for a mission-critical public safety network. We have characterized the connection probability, where the amount of interference considered the statistics of call activities within each cluster. The robust trust probability based on the Bayesian-based lower confidence bound has been formulated. The simulations have shown that compared with single criterion route selection the proposed route selection method offers versatile solutions with different basic criteria and thresholds on connection, timeliness, and trust probabilities. The academic implications, limitations, and future studies are given as follows.

Academic implications: Firstly, this research has demonstrated that connectivity, delay, and trust are all crucial to the mission-critical system since the system is susceptible to connection outages, delays, and attacks. Secondly, by incorporating the delay model into interference and connection probability analysis, the effect of the activity of the group communications on the connectivity has been captured. Thirdly, the trust probability based on the lower confidence bound could provide a more robust result than the mean trust probability especially when the number of interactions is small.

Limitations: This paper considers three crucial criteria for route selection, although there might be other uncovered but important criteria for certain applications. If they can be formulated in a probabilistic form, then they can be fitted easily into the proposed route selection method in this paper. Moreover, the trust evaluation may not always be available since the observing UE could be busy while the next forwarding UE is forwarding its messages.

Future studies: In this paper, the group members are uniformly distributed within the clusters, but it would be interesting to study other types of clusters such as clusters with Gaussian distributed members. Meanwhile, it is worthwhile to investigate how to carry out the trust rating when the observing UE is busy and cannot witness the forwarding behavior of the next forwarding UE.

Thus, the proposed route selection method would be well suited to 5G public safety and disaster relief communication networks.

References

[1] J. Ventura-Jaume, L. Franck, and L. Girardeau, "A distributed floor control protocol for next generation PMR based on hybrid LTE and satellite networks," in *Proc. IEEE Global Humanitarian Technol. Conf. (GHTC)*. San Jose, CA, USA: IEEE, 2014, pp. 62–69.

[2] 3GPP, "Technical Specification Group Services and System Aspects; Mission Critical Push To Talk (MCPTT) over LTE; Stage 1 (Release 15)," 3GPP, TS 22.179, June 2017. [Online]. Available: http://www.3gpp.org/ftp//Specs/archive/22_series/22.179/22179-f00.zip (Accessed Mar. 6, 2018)

[3] T. Ozan, K. and F. Gianluigi, Eds., *Ad Hoc Wireless Networks: A Communication-Theoretic Perspective*. Chichester, West Sussex, UK: John Wiley & Sons Ltd, 2006.

[4] K. Ali, H. X. Nguyen, P. Shah, Q.-T. Vien, and N. Bhuvanasundaram, "Architecture for public safety network using D2D communication," in *Proc. IEEE Wireless Commun. Netw. Conf. Workshops (WCNCW)*. Doha, Qatar: IEEE, 2016.

[5] K. Ali, H. X. Nguyen, P. Shah, and Q.-T. Vien, "Energy efficient and scalable D2D architecture design for public safety network," in *Proc. Int. Conf. Advanced Commun. Syst. Inf. Security (ACOSIS)*. Marrakesh, Morocco: IEEE, 2016.

[6] B. Black, P. DiPiazza, B. Ferguson, D. Voltmer, and F. Berry, *Introduction to Wireless Systems*. Upper Saddle River, NJ, USA: Prentice Hall Press, 2008.

[7] G. Chen and J. A. Chambers, "Exact outage probability analysis for cooperative AF relay network with relay selection in presence of inter-cell interference," *Electron. Lett.*, vol. 48, no. 21, pp. 1346–1347, Oct. 2012.

[8] J. Coon, C. P. Dettmann, and O. Georgiou, "Full connectivity: corners, edges and faces," *J. Statistical Physics*, vol. 147, no. 4, pp. 758–778, Jun. 2012.

[9] A. Al-Hourani, S. Kandeepan, and A. Jamalipour, "Stochastic geometry study on device-to-device communication as a disaster relief solution," *IEEE Trans. Veh. Technol*, vol. 65, no. 5, pp. 3005–3017, May 2016.

[10] J. Bai, Y. Sun, C. Phillips, and Y. Cao, "Toward constructive relay-based cooperative routing in MANETs," *IEEE Syst. J.*, July 2017.

[11] R. K. Ganti and M. Haenggi, "Interference and outage in clustered wireless ad hoc networks," *IEEE Trans. Info. Theory*, vol. 55, no. 9, pp. 4067–4086, Sept. 2009.

[12] M. Afshang, H. Dhillon, and P. Chong, "Modeling and performance analysis of clustered device-to-device networks," *IEEE Trans. Wireless Commun.*, vol. 15, no. 7, pp. 4957–4972, July 2016.

[13] J. Tang, G. Chen, J. P. Coon, and D. E. Simmons, "Distance distributions for Matérn cluster processes with application to network performance analysis," in *Proc. IEEE Int. Conf. Commun. (ICC)*. Paris, France: IEEE, 2017.

[14] A. Fida, D. H. Pham, N. J. Tuah, and T. D. Ngo, "Communication-aware route selection in wireless sensor networks," in *Proc. 13th Int. Conf. Intell. Auton. Syst. (IAS)*. Padua, Italy: Springer, 2014, pp. 605–619.

[15] R. S. Oliver and G. Fohler, "Probabilistic estimation of end-to-end path latency in wireless sensor networks," in *Proc. Int. Conf. Mobile Adhoc Sensor Systems (MASS)*. Macau, China: IEEE, 2009, pp. 423–431.

[16] T. S. Rappaport, *Wireless Communications: Principles and Practice*, 2nd ed. Upper Saddle River, NJ: Prentice-Hall, 2002.

[17] M. Boushaba, A. Hafid, and M. Gendreau, "Source-based routing in wireless mesh networks," *IEEE Sys. J.*, vol. 10, no. 1, pp. 262–270, Mar. 2016.

[18] H. Imai, *Wireless communications security*. Norwood, MA, USA: Artech House, Inc., 2005.

[19] N. Marchang and R. Datta, "Light-weight trust-based routing protocol for mobile ad hoc networks," *IET Inf. security*, vol. 6, no. 2, pp. 77–83, June 2012.

[20] A. Jøsang and R. Ismail, "The beta reputation system," in *Proc. 15th Bled Conf. Electron. Commerce*, Bled, Slovenia, 2002, pp. 324–337.

[21] C. Zouridaki, B. L. Mark, M. Hejmo, and R. K. Thomas, "A quantitative trust establishment framework for reliable data packet delivery in manets," in *Proc. 3rd ACM Workshop Security of Ad Hoc Sensor Netw.* Alexandria, VA, USA: ACM, 2005.

[22] J. P. Coon, "Modelling trust in random wireless networks," in *Proc. Wireless Commun. Syst. (ISWCS)*. Barcelona, Spain: IEEE, 2014, pp. 976–981.

[23] A. B. Usman and J. Gutierrez, "A reliability-based trust model for efficient collaborative routing in wireless networks," in *Proc. 11th Int. Conf. Queueing Theory Netw. Appl. (QTNA)*. Wellington, New Zealand: ACM, 2016.

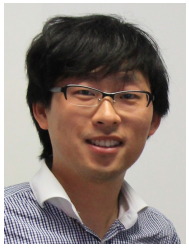
[24] 3GPP, "LTE; Mission Critical Push To Talk (MCPTT) media plane control; Protocol specifications (Release 13)," 3GPP, TS 24.380, May 2016. [Online]. Available: http://www.etsi.org/deliver/etsi_ts/124300_124399/124380/13.00.02_60/ts_124380v130002p.pdf (Accessed Mar. 6, 2018)

[25] D. P. Bertsekas and R. G. Gallager, *Data networks*, 2nd ed. Englewood Cliffs, NJ, USA: Prentice-Hall, Inc, 1992.

[26] G. Chen, Y. Gong, P. Xiao, and R. Tafazolli, "Dual antenna selection in self-backhauling multiple small cell networks," *IEEE Commun. Lett.*, vol. 20, no. 8, pp. 1611–1614, Aug. 2016.

[27] E. Cameron, "On the estimation of confidence intervals for binomial population proportions in astronomy: the simplicity and superiority of the Bayesian approach," *Publications of the Astronomical Society of Australia*, vol. 28, no. 2, pp. 128–139, June 2011.

Jinchuan Tang (S'17) received his B.Eng. degree in electronic information engineering from Chongqing University of Posts and Telecommunications in 2011. He worked as an Assistant Engineer in Huawei Technologies Co., Ltd. from 2011 to 2012. He obtained the M.Sc. degree with Distinction in wireless communications from the University of Southampton in early 2014. He is currently pursuing a DPhil degree under the supervision of Professor Justin P. Coon with the Department of Engineering Science, University of Oxford. His current research interests include optimum power allocation, random geometric networks, secure communication, and route selection in wireless networks.



Gaojie Chen (S'09 - M'12) received the B. Eng. Degree in electrical information engineering and the B.Ec. Degree in international economics and trade from Northwest University, China, in 2006, and the M.Sc. (Hons.) and Ph.D. degrees in electrical and electronic engineering from Loughborough University, U.K., in 2008 and 2012, respectively. From 2008 to 2009, he was a Software Engineering with DTmobile, Beijing, China, and a Research Associate with the School of Electronic, Electrical and Systems Engineering, Loughborough University, from 2012 to 2013. Then he was a Research Fellow with the 5GIC, University of Surrey, U.K., from 2014 to 2015. Then he was a Research Fellow at the University of Oxford, U.K., from 2015 to 2018. He is currently a Lecturer at the University of Leicester, U.K. His current research interests include information theory, wireless communications, IoT, cognitive radio, secrecy communication and random geometric networks.

Justin P. Coon (S'02 - M'05 - SM'10) received the B.Sc. degree (Hons.) in electrical engineering from the Calhoun Honours College, Clemson University, USA, and the Ph.D. degree in communications from the University of Bristol, U.K., in 2000 and 2005, respectively. In 2004, he joined as a Research Engineer with the Bristol-based Telecommunications Research Laboratory (TRL), Toshiba Research Europe Ltd., where he was involved in research on a broad range of communication technologies and theories, including single- and multi-carrier modulation techniques, estimation and detection, diversity methods, and system performance analysis and networks. He held the research manager position from 2010 to 2013, during which time he led all theoretical and applied research on the physical layer at TRL. He was a Visiting Fellow with the School of Mathematics, University of Bristol, from 2010 to 2012, where he held a reader position with the Department of Electrical and Electronic Engineering from 2012 to 2013. He joined the University of Oxford in 2013, where he is currently an Associate Professor with the Department of Engineering Science and a Tutorial Fellow of Oriel College. He is the Technical Manager of the EU FP7 project DIWINE. He has authored in excess of 100 papers in leading international journals and conferences, and is a named inventor on over 30 patents. His research interests include communication theory, information theory, and network theory. Dr Coon was a recipient of TRLs Distinguished Research Award for his work on block-spread CDMA, aspects of which have been adopted as mandatory features in the 3GPP LTE Rel-8 standard. He was also a co-recipient of two best paper awards at the ISWCS 2013 and the EuCNC 2014. He received the award for Outstanding Contribution in 2014. He has served as an Editor for the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS from 2007 to 2013, the IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY from 2013 to 2016. He has been serving as an Editor for the IEEE WIRELESS COMMUNICATIONS LETTERS since 2016 and the IEEE COMMUNICATIONS LETTERS since 2017.