Hindawi
Wireless Communications and Mobile Computing
Volume 2018, Article ID 8539307, 12 pages
https://doi.org/10.1155/2018/8539307

Research Article

Reliability Analysis for Multipath Communications in Mobile Cloud Computing Architectures

Shiyong Li, Wei Sun, Yaming Zhang, and Haiou Liu

School of Economics and Management, Yanshan University, Qinhuangdao 066004, China

Correspondence should be addressed to Wei Sun; wsun@ysu.edu.cn

Received 4 April 2018; Accepted 20 May 2018; Published 19 June 2018

Academic Editor: Fuhong Lin

Mobile cloud computing (MCC) has gained much attention from both academia and industry in recent years. It can support new types of services, such as m-commerce, m-learning, and mobile healthcare, and enrich mobile users' experience and satisfaction by taking full advantage of cloud computing. In MCC architectures multipath communications can be achieved with multihomed mobile devices, so as to utilize multiple paths for data transmission in parallel. They can achieve better utilization of bandwidth resource, split traffic for load balancing, and enhance reliability, fault tolerance, and robustness for applications. However, little attention has been paid to model the reliability of multipath communications in case of path failure. In this paper we investigate the reliability of concurrent multipath communications in MCC architectures and propose two reliability models when paths are failure. One is for static path failure where the failed paths cannot recover for communication in some delay time. The other is for dynamic path failure where the failed paths can recover in some delay time. Finally, numerical results are given to illustrate the reliability of multipath communications.

1. Introduction

With the wide popularity of mobile devices and the explosion of mobile applications, e.g., business, health, games, entertainment, social networking, travel, and news, mobile cloud computing (MCC) is arising and developed as an integration of cloud computing (CC) into the mobile environment. MCC can support new kinds of services such as mobile commerce, m-government, m-learning, and mobile healthcare and promote mobile users to take full advantages of cloud computing. It has become a profitable business option for enterprise since it can reduce the development and implement of mobile applications. And it is used as a new technology for mobile users to achieve rich experience of many mobile services at low cost. Finally it provides a promising solution to achieve green IT for entrepreneurs, engineers, and researchers [1, 2].

MCC has been attracting the attentions from both academia and industry in recent years and some significant surveys are provided, e.g., [3–6]. These surveys offer an extensive summary and review of mobile cloud computing research and highlight the specific concerns in mobile cloud computing. They also present a taxonomy based on the key issues in this area and discuss the different approaches taken to tackle these issues. Furthermore, they give a critical analysis of challenges which have not yet been fully met and highlight some directions for future work. Recently a new computing paradigm, known as fog computing and further mobile fog computing, has been proposed as an improvement to the cloud computing. Fog computing expands the cloud services to the edge of cloud networks and makes computation, communication, and storage closer to edge devices and end-users [7]. In the research surveys [8–10], the authors overview and survey fog computing model architectures, key technologies, and applications. They also provide some challenges and open issues which are worth indepth study and research in further.

In MCC systems or fog computing for mobile applications (e.g., [11]), each mobile device can be multihomed, so as to improve its throughput by allocating the application data over several paths simultaneously, which is known as *multipath communications* enabled by the promising multipath transmission technologies [12]. Generally, multipath communications can be classified into two types. The first one is *dynamic path communication* where a primary path is used for transmission and alternate paths are adopted in case of traffic saturation or link breakage on the primary path. The second one is *concurrent path communication* where traffic is split and distributed over multiple paths that are node-disjoint in parallel. It is obvious that both types of multipath communications are preferred to single-path cases in many applications as the former could achieve robustness and load balancing and improve reliability. However, fewer researchers pay attention to analyze the reliability of multipath communications and to model the relationship between the reliability and the number of paths. In this paper we consider concurrent multipath communications in MCC and evaluate the communication reliability when some independent paths for a source-destination pair fail during data transmission. We present two reliability models where the failed paths cannot and can recover after some delay time, respectively, and deduce the probability of successful communication for an application in each model.

We end this section with a short overview of the rest of this paper. Section 2 reviews related work on multipath communications technologies. Section 3 discusses concurrent multipath communications in MCC. Section 4 introduces the reliability models for concurrent multipath communications in MCC. Section 5 presents the numerical results to illustrate the reliability analysis. Finally, conclusions are summarized in Section 6.

2. Related Work

Recent years have seen the increasing attention in the field of multipath communications that utilize multiple paths in parallel and split traffic for load balancing [13–16] and for avoiding DDoS attack in MCC [12]. It seems obvious that using multipath communications could generally increase the available bandwidth for applications [17]. More importantly, they can bring enhancements to the connection persistence, reliability, and fault tolerance, e.g., [18, 19]. They have been found to be useful in many scenario such as communication security in MCC [12], fault-aware resource allocation [20], high-availability virtual communication [21], connection management for identifier-based network [22], and edge computing for vehicular networks [23].

Many multipath protocols have been proposed and applied into wired networks and wireless networks. In wired networks, Multipath TCP protocols, e.g., pTCP [24], mTCP [25], MPTCP [26], and energy efficient congestion control for Multipath TCP [27], are a set of extensions of regular TCP that allow one TCP connection to be spread across multiple paths between each pair of source and destination. By striping one flow's packets across multiple paths, they can enhance user experience through improved resilience to network failure and higher throughput. Stream Control Transmission Protocol (SCTP) [28] standardized by the Internet Engineering Task Force (IETF) is a transport protocol that introduces support for transmission over multiple paths. In an SCTP multihomed association, each endpoint can include more than one IP address. Then, at the initialization time, endpoints exchange the lists of their IP addresses. After the destination is multihomed, one of its multiple destination addresses is chosen as the primary path and the others as secondary paths. During data transmission, if the primary path fails, the source will choose an alternative path to resume sending its packets. Its variants which use SCTP multihoming, e.g., Westwood SCTP with partial reliability (W-PR-SCTP) [17], concurrent multipath transfer [29], load-sharing SCTP (LS-SCTP) [30], independent per-path congestion control SCTP (IPCC-SCTP) [31], and application-layer multipath transport control [32], allow the protocols to distribute traffic over more than one path and use multiple end-to-end paths to carry packets from the same connection and with the same source-destination endpoints. Recently, Coudron [33] reviewed the latest developments in multipath communication technologies and presented some novel approaches for multipath communications. Obviously, using multipath communications improves the performance of well-known bandwidth-hungry applications and enhances reliability, robustness, and fault tolerance for applications. Furthermore, multipath protocols have also been applied to file download and resource allocation in peer-to-peer networks, e.g., BitTorrent, eDonkey, and Gnutella. For example, multipath communication schemes have been presented to realize reasonable resource allocation in [34].

In wireless ad hoc networks, ad hoc on-demand distance vector backup routing (AODV-BR) [35] is a protocol that uses backup nodes to provide fault tolerance. The protocol allows multiple paths between a source and its destination per one route discovery, without additional network load. Another protocols, e.g., ad hoc on-demand multipath distance vector (AOMDV) protocol [36] and optimized AOMDV routing protocol [37], also have a hop-by-hop approach to compute the primary route and multiple backup routes in each route discovery. Moreover, some other multipath protocols based on AODV were also proposed, such as ad hoc on-demand distance vector multipath (AODVM) protocol [38] and node-disjoint multipath routing (NDMR) protocol [39]. Meanwhile, other examples of backup route technique were also presented and multiple paths can be maintained between two nodes, e.g., [40, 41], which are derived from the dynamic MANET on-demand (DYMO) protocol. Using these protocols, the built routes and backup routes for each pair of source and destination can be link-disjoint or node-disjoint, which helps the construction of highly robust end-to-end communication for applications. Recently, in order to build reliable routing, some trust routing schemes were proposed in ad hoc networks, e.g., [42–45], which are the extensions of popular on-demand routing protocols such as the dynamic source routing (DSR) [46]. These proposed routing schemes can behave well in warding off black hole and changing behavior attacks.

Computer networks are known to be fundamental to communications systems. Therefore, it is very important to develop the principles of reliability and availability analysis for computer networks. Shooman [47] developed reliability and availability prediction and optimization methods and applied these techniques to a selection of fault-tolerant systems. Later, Abd-El-Barr [48] introduced the design and

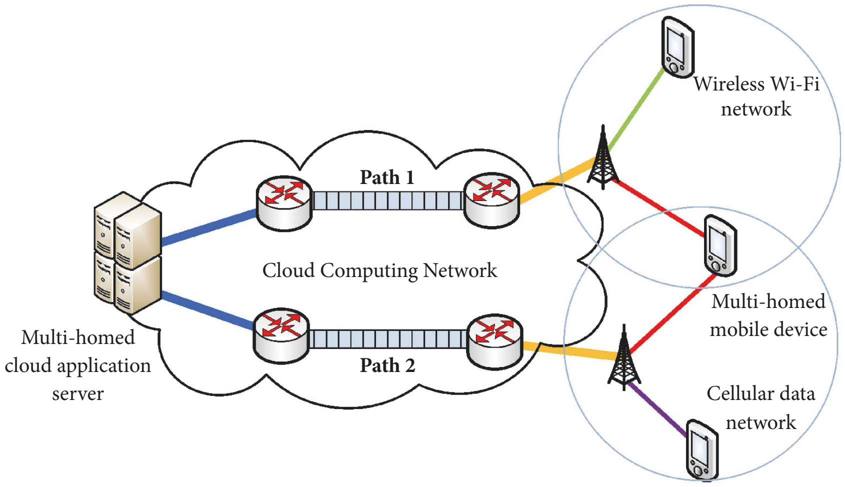


Figure 1: An example of multipath communications in a mobile cloud network (a copy from [12]).

analysis of reliable and fault-tolerant computer systems and discussed the main issues related to redundancy, including hardware, software, time, and information redundancies. Lin et al. [49] investigated an evaluation method for network reliability in ad hoc networks and gave some numerical examples to illustrate the performance. In this paper we consider reliability for concurrent multipath communications in MCC architectures and present two kinds of reliability models: one is static for path failure and the other is dynamic for path failure and recovery. We also give some numerical examples to illustrate the performance.

3. Multipath Communications in MCC

Multipath communications have become very attractive since they can achieve better robustness and reliability than single-path cases. Among these schemes, concurrent multipath routing schemes where paths for a source-destination pair do not share any common links gain a lot of attention. As shown in Figure 1 (a copy from [12]), in MCC systems each mobile device is multihomed through the promising multipath technologies, such as MPTCP and SCTP. There are multiple paths between each pair of mobile user and the server. This improves the user's throughput by allocating the application data over several paths simultaneously. More importantly, this bring enhancements to the connection persistence, security, reliability, and fault tolerance.

Further, we consider the different types of multipath communications. In the work [50] a multipath routing scheme modified from single-path AODV was proposed for MANET so as to reduce the effect of frequent communication failures. The proposed scheme is basically proposed for highly dynamic ad hoc networks where communication failures occur frequently and designed to compute not only node-disjoint paths but also fail-safe paths between each source-destination pair [51]. In this work different types of multiple paths are reviewed, which are shown in Figure 2 (a copy from [50]).

For a source-destination pair, node-disjoint paths do not share any nodes in common, except the source and destination, while link-disjoint paths do not have any links in common; however, they may share some intermediate nodes on the paths. Unlike node-disjoint and link-disjoint paths, fail-safe path between the source-destination pair bypasses at least one intermediate node on the primary path, which is the shortest path between the source and destination [50]. Thus, fail-safe paths can share both nodes and links in common, just as shown in Figure 2.

Among the three kinds of multipath scenarios for a source-destination pair, paths are independent from each other in the first case and do not own any common nodes or links. The paths are regarded to be *concurrent*. Thus, communication failure on one of them has no influence on others. However, in the second case, two paths share some common nodes which are regarded as *hot-nodes* for forwarding data packet. Failure on one of the shared nodes can result in communication failures on multiple paths and even failure of the communication progress between the source and destination. The third case is the most complicated one. Paths share nodes and links in common, which can enhance the robustness and reliability of communication. When some shared nodes are failure, the source can continue to communicate the destination by bypassing them. Reliability analysis of communication in link-disjoint or fail-safe case is more complicated than that in node-disjoint case since they share common nodes. Thus, as an attempt to analyze the reliability of multipath communications theoretically, we concentrate on concurrent multipath communications and present two reliability models for them.

In this paper, we consider a network consisting of a set of sources and destinations, whereby each source can send data to its destination over multiple independent paths. Thus an application can be completed as long as there exists at least an available path between the pair of source and its destination. Here, the paths for a source-destination pair are all assumed to be concurrent and node-disjoint; that is, they

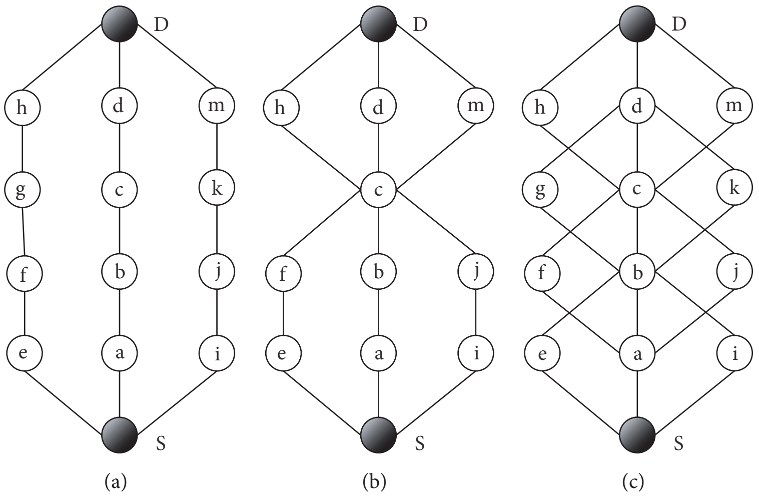


Figure 2: Different types of multiple paths: (a) node-disjoint, (b) link-disjoint, and (c) fail-safe.

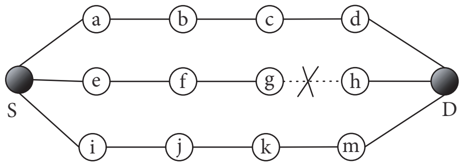


Figure 3: Static failure.

do not share any common node or link with each other, as shown in Figure 2(a).

4. Reliability Models

In this section we develop analytical models to evaluate the reliability of concurrent multipath communications in MCC in the face of path failures which may be caused by attacks on nodes or heavy congestion on bottleneck links on the paths. We assume that the communication for an application between two nodes can be completed successfully so long as there is at least one available path which is not failed. Our analysis begins by considering the simple case: the paths for a source-destination pair have static failures.

4.1. Static Failure. Firstly, we consider static failure where the failed paths cannot recover for communication after some delay time. As an example shown in Figure 3, there are three node-disjoint paths between the source S and destination D. At some time, the path e → f → g → h fails due to attacks on node g or heavy congestion on link g → h. Then the source will choose the remaining ones for communication and continue sending packets to the destination.

Let N be the number of all available node-disjoint paths for a source-destination pair, $M(\leq N)$ be the number of node-disjoint paths that the pair actually chooses and uses during data transmission, and $K(\leq N)$ be the number of failed paths for the pair. That is, among the available node-disjoint paths that the pair builds and maintains, the pair only chooses M of them for communication. Meanwhile, some of the paths may fail during the maintenance.

Let $P(n, m, k)$ be the probability that a set of k paths selected at random from n paths contains a specific subset of m paths. It is easy to obtain that

$$P(n, m, k) = \frac{C_k^m}{C_n^m}, \tag{1}$$

when $k \geq m$, and $P(n, m, k) = 0$ when $k < m$, where

$$C_a^b = \binom{a}{b} = \frac{a!}{b!\,(a-b)!}. \tag{2}$$

Thus, for a source-destination pair, the probability that an application can be completed successfully is

$$\mathbf{P} = 1 - P(N, M, K) = 1 - \frac{C_K^M}{C_N^M}. \tag{3}$$

Obviously,

$$\begin{gathered}\frac{P(N, M, K)}{P(N-1, M, K)} = 1 - \frac{M}{N} \leq 1, \\ \frac{P(N, M+1, K)}{P(N, M, K)} = \frac{1-(N-K)}{(N-M) \leq 1},\end{gathered} \tag{4}$$

and

$$\frac{P(N, M, K)}{P(N, M, K-1)} = 1 + \frac{M}{(K-M)} > 1 \tag{5}$$

when $K \geq M$. Hence, an increase in the number of available paths N for the pair of source and destination or the number of paths M actually used by the source can increase the probability of successful communication for the application. Similarly, a decrease in the number of failure paths K can also increase the probability.

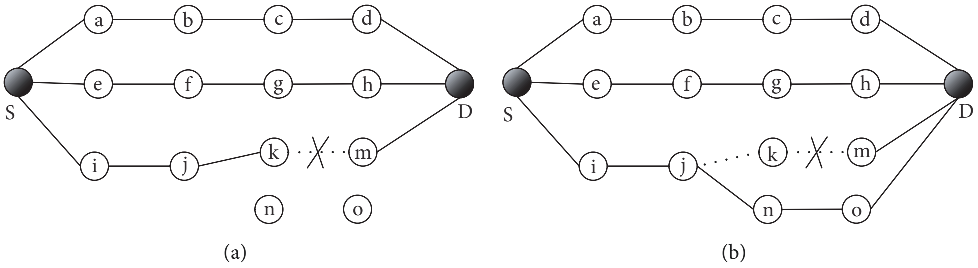


Figure 4: Dynamic failure: (a) before recovery; (b) after recovery.

4.2. *Dynamic Failure and Recovery.* Our previous model assumes that once the paths fail, they do not recover after some time. However, the nodes on the failed paths can take repairing and recovering actions so that new available paths can be established after some delay time. Hence, we extend the model to the case where the failed paths can take some repairing actions and recover the ability of communication for applications.

As an example shown in Figure 4, among the three node-disjoint paths for the pair of source S and destination D, the path i → j → k → m fails because of attacks on node k or heavy congestion on link k → m; then after some time source S detects it and reestablishes a new available path, i.e., i → j → n → o.

We assume that for a source-destination pair there is a failure delay or an attack delay D_f which is the difference in time from when an available path is first established to the time when the path is failed because of attacks on nodes or heavy congestion on bottleneck links on the path. Also there is a recovery delay D_r that equals the difference in time between when the source discovers the failed path to the time when it reestablishes a new available path.

Since there are so many types of attacks in networks, e.g., black hole attacks, rushing attack, and worm attack [50], we do not yet have a detailed understanding of how the failure and recovery processes will perform. Therefore, we do not have models that accurately capture the distributions of D_f (failure delay) and D_r (recovery delay). However, we are interested in gaining preliminary insight into how the failure of paths affects the reliability of concurrent multipath communications. We realize this insight by modeling the framework as a closed queueing system with a finite customer population. In the queueing system customers arrive at the server(s), obtain service, and then, after a certain delay, return to get serviced again. Thus, the number of jobs active in the queueing system equals the number of paths under attack that are to be failed. The recovery process removes jobs from the system and attacks cause in the path filed, resulting in placing jobs back in the system.

As an interesting method to evaluate the denial of service (DoS) attacks in computer networks, a two-dimensional embedded Markov chain model is presented in [52] to characterize the network under DoS attacks. The arrivals of the regular request packets and the attack packets are both Poisson processes, and they are independent of each other. Thus, similar to the queueing analysis for attacks in [52], we suppose that both D_f and D_r are exponentially distributed variables with respective rates λ and μ.

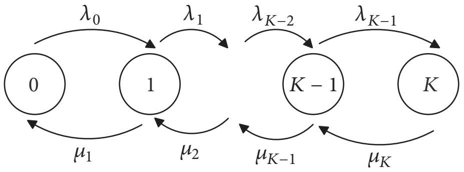


Figure 5: State transition diagram.

We are interested in two variants of modeling the failed path recovery process. In the first, the ability to detect and recover the failed paths is performed sequentially. This would occur when the detection and recovery of failed paths is made one after another by the source. We refer to this variant as the centralized recovery process. Alternatively, the other one is distributed recovery process, where recovery of failed paths can be performed in parallel. This would occur when each path can independently perform its recovery process. Similarly, the failure process can be centralized, where available paths for one source are failed one after another, or distributed, where all available paths would be failed in parallel.

For a source-destination pair, we define a random variable $F(t)$ to be the number of failure paths on which the nodes are under attacks or the links have heavy congestion at time t. Let K be the maximal number of failure paths; thus $F(t)$ is up to K, i.e., $0 \leq F(t) \leq K$.

Given that both the failure and the recovery process can be either centralized or distributed, there are four different scenarios. Each scenario is indeed a queueing model with $K+1$ states where the process resides in state i when there are i paths that are failed because of attacks on nodes. The state transition diagram of each of the four models can be shown in Figure 5. When the paths failure is centralized, the transition rate from state i to $i+1$ is λ; while the paths failure is distributed, the rate is $(K-i)\lambda$. When the paths recovery is centralized, the transition rate from state i to $i-1$ is μ; while in the distributed case, the rate is $i\mu$.

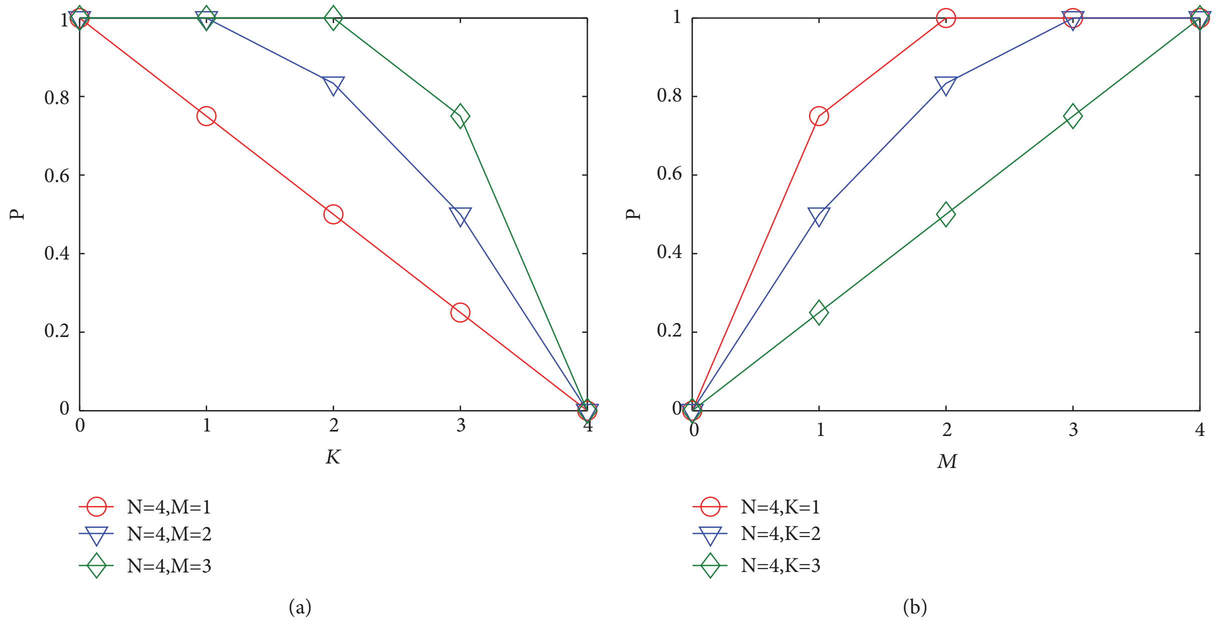


Figure 6: Reliability in the static failure case: (a) the relationship between **P** and K; (b) the relationship between **P** and M.

Let $\rho = \lambda/\mu$; then the probability $\pi_i = \Pr[F(t) = i]$ in the four scenarios can be summarized as follows:

(a) centralized failure, centralized recovery

$$\pi_i = \frac{1-\rho}{1-\rho^{K+1}}\rho^i, \tag{6}$$

(b) centralized failure, distributed recovery

$$\pi_i = \frac{\rho^i/i!}{\sum_{j=0}^{K}(\rho^j/j!)}, \tag{7}$$

(c) distributed failure, centralized recovery

$$\pi_i = \frac{\rho^i/(K-i)!}{\sum_{j=0}^{K}(\rho^j/(K-j)!)}, \tag{8}$$

(d) distributed failure, distributed recovery

$$\pi_i = \frac{\rho^i/i!(K-i)!}{\sum_{j=0}^{K}(\rho^j/j!(K-j)!)}. \tag{9}$$

Notice that in the four scenarios of failure and recovery process the probability π_i depends on both the failure rate ρ on paths and the maximal number of failure paths K.

Let N be the number of all *available* node-disjoint paths for the pair of source and destination and $M(\leq N)$ be the number of node-disjoint paths that the pair *actually chooses* for communication. Thus, the probability that an application between the source and destination can be completed successfully is

$$\mathbf{P} = \sum_{i=0}^{K}\pi_i(1-P(N+i-K,M,i)), \tag{10}$$

where $P(N+i-K,M,i) = C_i^M/C_{N+i-K}^M$ when $i \geq M$ and 0 otherwise.

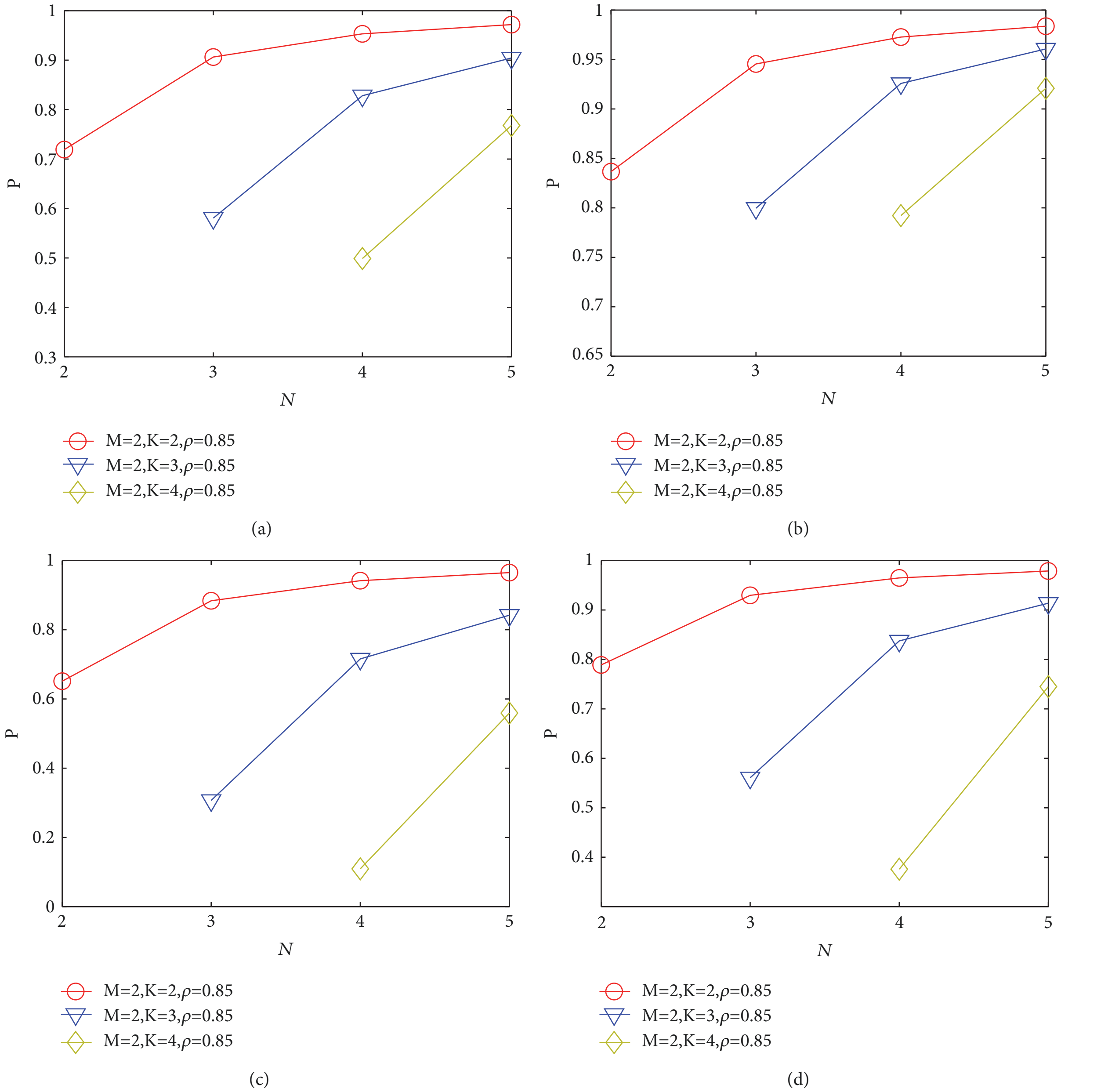
Intuitively, an increase in failure rate ρ decreases the successful probability **P**. For a fixed failure rate ρ, not surprisingly, increasing the number of available paths N or the number of actually used paths M or decreasing the maximal number of failure paths K can increase the successful probability **P**.

5. Numerical Examples and Analysis

In this section we consider a scenario of concurrent multipath communication as shown in Figure 2(a) and give some numerical examples to illustrate the reliability models for concurrent multipath communications. We also present analysis for the relationships between the successful probability **P** and the parameters N, M, K, and ρ.

5.1. Static Failure. Suppose that there are four available node-disjoint paths between each source and its destination. The communication for an application between the source and destination can be completed successfully even if there is only one available path which is not failed. Obviously in Figure 6, an increase in the maximal number of failure paths K can decrease the probability of successful communication for the application using concurrent multiple paths, while an increase in the number of actually used paths M can increase the probability. For example, the successful probability **P** is increased from 0.5 to 0.8333 when an increase in the number of actually used paths M from 1 to 2 for fixed number of available paths $N = 4$ and maximal number of failure paths $K = 2$.

5.2. Dynamic Failure and Recovery. In this part we further consider the concurrent multipath communication shown



(a)

(b)

(c)

(d)

Figure 7: The relationship between **P** and N in the dynamic failure and recovery case: (a) centralized failure, centralized recovery; (b) centralized failure, distributed recovery; (c) distributed failure, centralized recovery; (d) distributed failure, distributed recovery.

in Figure 2(a) and investigate the relationships between **P** and N, M, K, and ρ when the failed paths can recover for communication after some delay time. In each example, the reliability performances in the four scenarios are listed in sequence as follows: (a) centralized failure, centralized recovery; (b) centralized failure, distributed recovery; (c) distributed failure, centralized recovery; (d) distributed failure, distributed recovery.

5.2.1. Relationship between **P** *and N.* Suppose for the pair of source and destination the number of actually used paths M is 2, the maximal number of failure paths K varies from 2 to 4, and the failure rate ρ is 0.85. As shown in Figure 7, in each scenario, for fixed M, K, and ρ, an increase in the number of available paths N for the pair of source and destination remarkably improves the successful probability **P**, since the likelihood for each source to select multiple available paths for communication increases. And the reliability performance is better when the failure process is centralized and the recovery process is distributed than that when the failure process is distributed and the recovery process is centralized. For example, when $N = 4, M = 2, K = 3, \rho = 0.85$, the successful probability **P** is 0.9258 in the former while it is only 0.7159 in the latter.

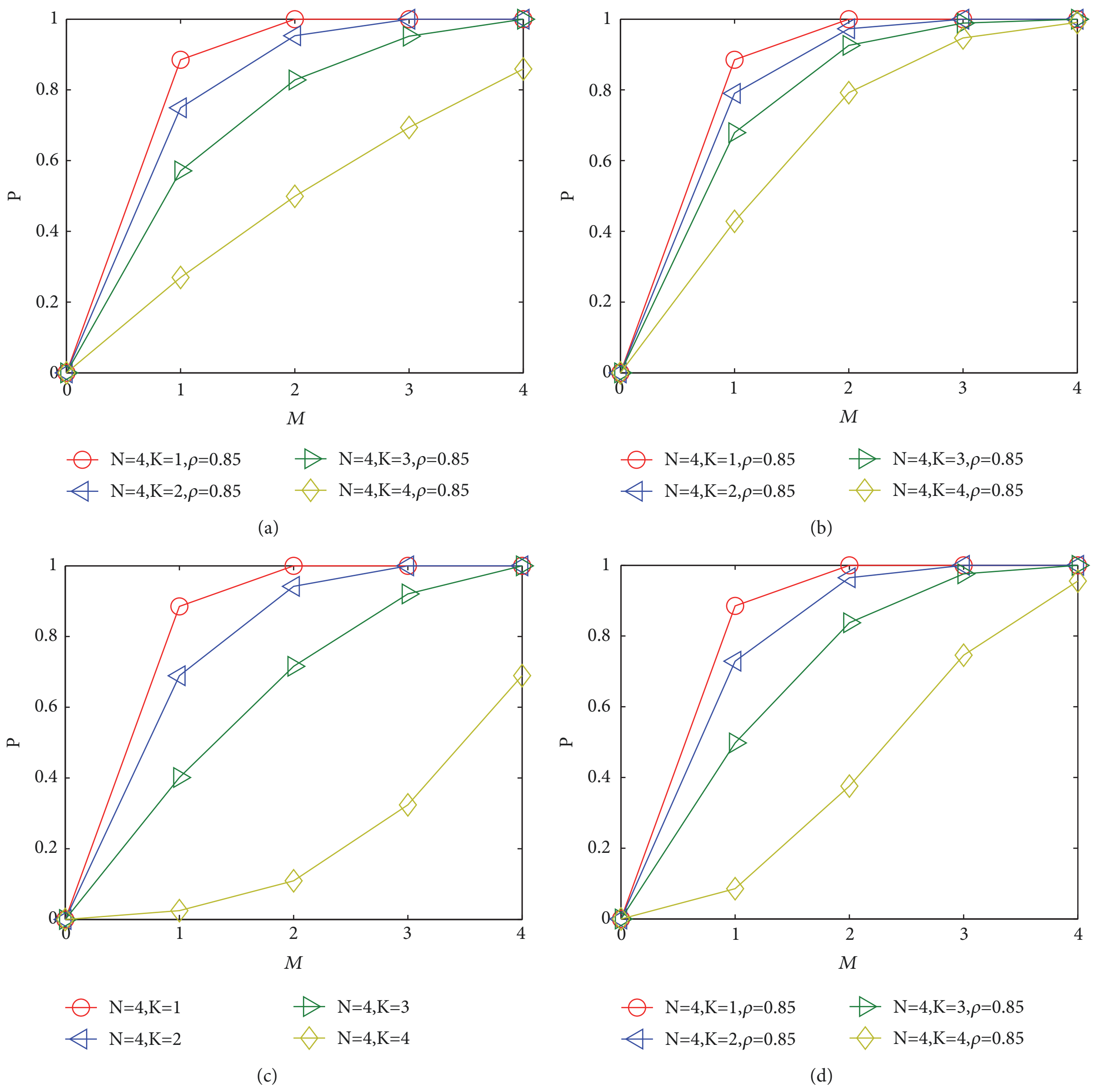
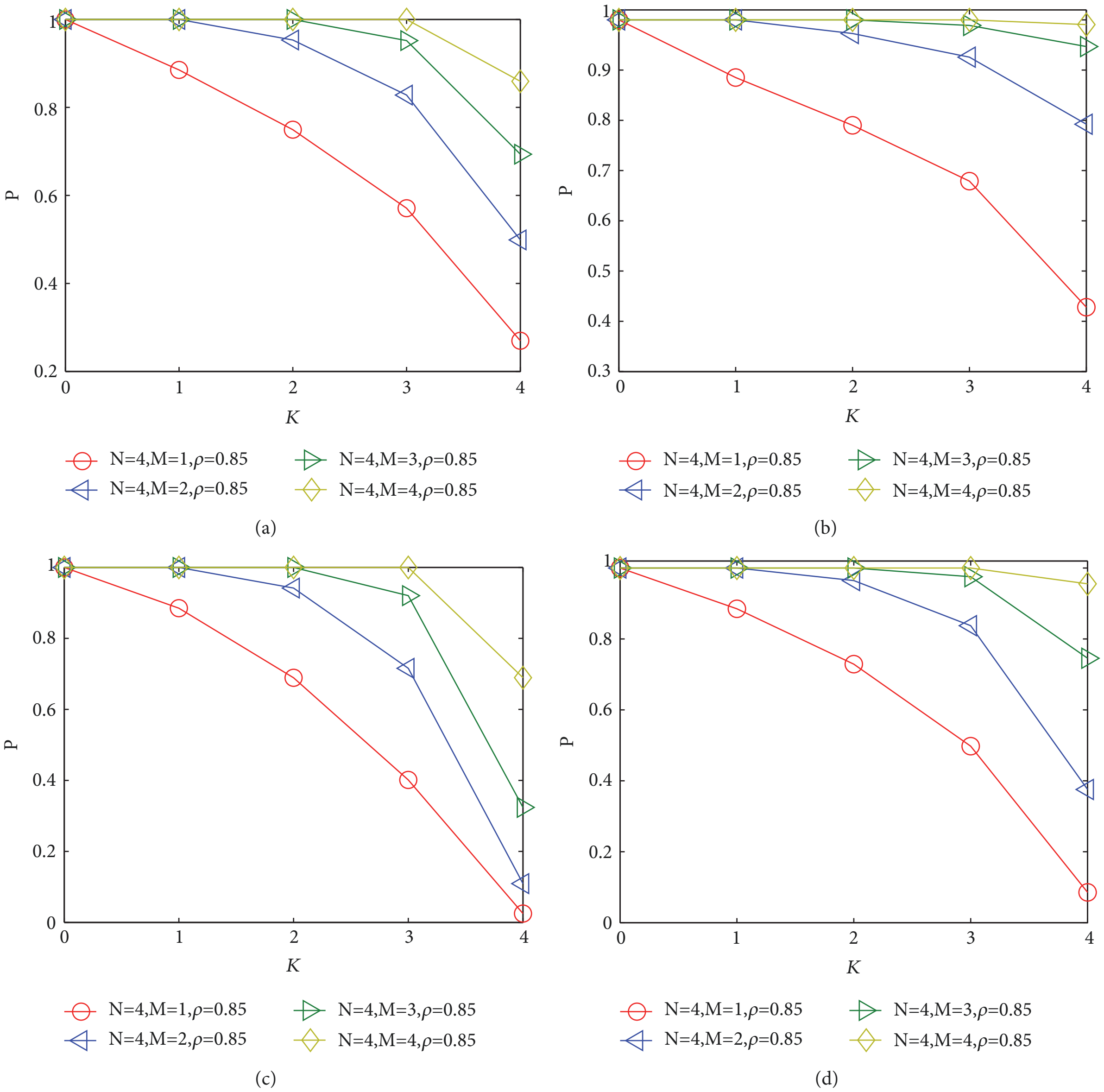


FIGURE 8: The relationship between **P** and M in the dynamic failure and recovery case.

5.2.2. Relationship between **P** *and M.* Suppose for the pair of source and destination the number of available paths N is 4, the maximal number of failure paths K varies from 1 to 4, and the failure rate ρ is 0.85. As shown in Figure 8, for fixed N, K, and ρ, the successful probability **P** significantly increases with an increase in the number of paths that the pair of source and destination actually chooses for communication. Obviously, applications are most likely to be completed when the failure process is centralized and the recovery process is distributed and they are least likely to be completed when the failure is distributed and the recovery is centralized. That is, the reliability performance of the former is better than that of the latter. For example, when $N = 4, M = 3, K = 3, \rho = 0.85$, the successful probability **P** is 0.9889 in the former while it is only 0.9204 in the latter. This result can be understood intuitively by comparing the respective birth-death processes of the system in the aforementioned two cases. In the former one, the upward transition rate is λ and the downward transition rate is $i\mu$, which is larger for state with larger i, whereas in the latter, the upward transition rate is $(K - i)\lambda$, which is larger for state with smaller i and the downward transition rate is μ.

5.2.3. Relationship between **P** *and K.* Suppose for the pair of source and destination the number of available paths N is 4, the number of actually used paths M varies from 1 to 4, and the failure rate ρ is 0.85. As shown in Figure 9, the probability **P** significantly decreases with an increase in the maximal number of failure paths K. Similarly, among the four different cases for path failure and recovery, the second one



(a)

(b)

(c)

(d)

Figure 9: The relationship between **P** and K in the dynamic failure and recovery case.

is the best while the third one is the worst under the same network condition. Thus, in order to improve the likelihood of successful communication, distributed effective detection methods are highly suggested such that the failed paths can recover in a distributed way.

5.2.4. Relationship between **P** *and ρ.* Suppose for the pair of source and destination the number of available paths N is 4, the number of actually used paths M is 2, and the maximal number of failure paths K varies from 2 to 4. In Figure 10, we plot the probability **P** varying along with ρ. Obviously, **P** decreases as ρ grows. As ρ approximates to 1, **P** diminishes less when the failure process is centralized and the recovery process is distributed than that when the failure is distributed and the recovery is centralized or distributed. Thus, applications are most likely to be completed when the failure process is centralized and the recovery process is distributed.

From the results above in the four scenarios of failure and recovery process, we can obtain that reliability achieves much better when the recovery process is distributed; thus in order to improve the likelihood of successful communication between the source and destination, distributed effective detection methods are highly suggested such that the failed paths can recover in a distributed way.

6. Conclusions

MCC is regarded as an integration of cloud computing into the mobile environment. It provides a powerful tool to the user when and where it is needed irrespective of user movement, hence supporting new kinds of mobile applications

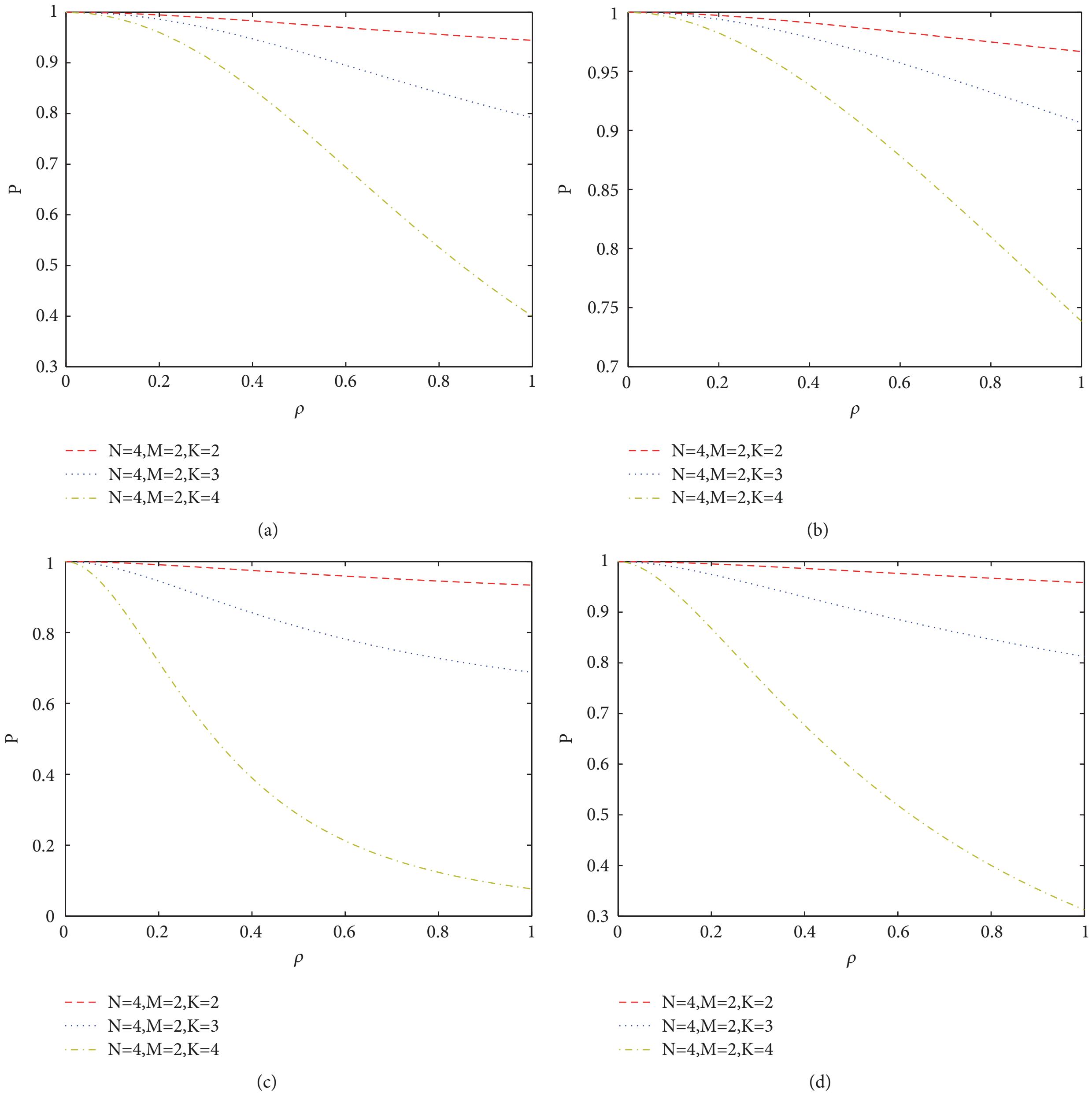


Figure 10: The relationship between **P** and ρ in the dynamic failure and recovery case.

such as m-commerce, mobile healthcare, and mobile social networking. In MCC systems each mobile device can be multihomed so that there are multiple paths between each pair of user and the server. It has been agreed that using concurrent multipath communications could improve the connection persistence, reliability, and fault tolerance between each pair of source and destination. Thus we consider concurrent multipath communications in MCC architectures and investigate the communications reliability when the paths are failed due to attacks. We obtain two kinds of reliability models when the failed paths cannot and can recover after some delay time, respectively. Our analysis demonstrates that using concurrent multipath communications generally improves the likelihood of successful communication for an application. Meanwhile, when communication paths are failed, distributed effective detection and quick recovery schemes should be highly guaranteed, so as to ensure high reliability requirements for communications of mobile applications.

Data Availability

The authors confirm that the data supporting the findings of this study are available within the article.

Conflicts of Interest

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

Acknowledgments

The authors would like to thank the support from the National Natural Science Foundation of China (nos. 71671159, 71301139, and 71271186), the Humanity and Social Science Foundation of the Ministry of Education of China (no. 16YJC630106), the project funded by Four Batch of Talents Program in Hebei Province, the Natural Science Foundation of Hebei Province (nos. G2018203302, G2016203236, G2016203220), the project funded by Hebei Education Department (nos. BJ2017029, BJ2016063), and Hebei Talents Program (no. A2017002108).

References

[1] M. Ali, "Green cloud on the horizon," in *Proceedings of the 1st International Conference on Cloud Computing (CloudCom '09)*, pp. 451–459, Manila, Philippines, 2009.

[2] L. Yang, J. Cao, Y. Yuan, T. Li, A. Han, and A. Chan, "A framework for partitioning and execution of data stream applications in mobile cloud computing," *Performance Evaluation Review*, vol. 40, no. 4, pp. 23–32, 2013.

[3] A. Abunaser and S. Alshattnawi, "Mobile cloud computing and other mobile technologies: Survey," *Journal of Mobile Multimedia*, vol. 8, no. 4, pp. 241–252, 2013.

[4] H. T. Dinh, C. Lee, D. Niyato, and P. Wang, "A survey of mobile cloud computing: Architecture, applications, and approaches," *Wireless Communications and Mobile Computing*, vol. 13, no. 18, pp. 1587–1611, 2013.

[5] A. Khan, M. Othman, S. A. Madani, and S. U. Khan, "A survey of mobile cloud computing application models," *IEEE Communications Surveys and Tutorials*, vol. 16, no. 1, pp. 393–413, 2014.

[6] Y. Wang, I.-R. Chen, and D.-C. Wang, "A survey of mobile cloud computing applications: perspectives and challenges," *Wireless Personal Communications*, vol. 80, no. 4, pp. 1607–1623, 2015.

[7] F. Song, Z.-Y. Ai, J.-J. Li et al., "Smart collaborative caching for information-centric IoT in fog computing," *Sensors*, vol. 17, no. 11, p. 2512, 2017.

[8] P. Hu, S. Dhelim, H. Ning, and T. Qiu, "Survey on fog computing: architecture, key technologies, applications and open issues," *Journal of Network and Computer Applications*, vol. 98, pp. 27–42, 2017.

[9] O. Osanaiye, S. Chen, Z. Yan, R. Lu, K.-K. R. Choo, and M. Dlodlo, "From cloud to fog computing: a review and a conceptual live VM migration framework," *IEEE Access*, vol. 5, pp. 8284–8300, 2017.

[10] R. Roman, J. Lopez, and M. Mambo, "Mobile edge computing, Fog et al.: a survey and analysis of security threats and challenges," *Future Generation Computer Systems*, vol. 78, pp. 680–698, 2018.

[11] L. F. Bittencourt, J. Diaz-Montes, R. Buyya, O. F. Rana, and M. Parashar, "Mobility-aware application scheduling in fog computing," *IEEE Cloud Computing*, vol. 4, no. 2, pp. 26–35, 2017.

[12] Y. Cao, F. Song, Q. Liu, M. Huang, H. Wang, and I. You, "A LDDoS-Aware energy-efficient multipathing scheme for mobile cloud computing systems," *IEEE Access*, vol. 5, pp. 21862–21872, 2017.

[13] S. Li, W. Sun, and C. Hua, "Fair resource allocation and stability for communication networks with multipath routing," *International Journal of Systems Science*, vol. 45, no. 11, pp. 2342–2353, 2014.

[14] S. Li, W. Sun, and N. Tian, "Resource allocation for multi-class services in multipath networks," *Performance Evaluation*, vol. 92, pp. 1–23, 2015.

[15] F. Song, Y. Zhang, Z. An, H. Zhou, and I. You, "The correlation study for parameters in four tuples," *International Journal of Ad Hoc and Ubiquitous Computing*, vol. 19, no. 1-2, pp. 38–49, 2015.

[16] S. Li, W. Sun, and C. Hua, "Optimal resource allocation for heterogeneous traffic in multipath networks," *International Journal of Communication Systems*, vol. 29, no. 1, pp. 84–98, 2016.

[17] M. Fiore, C. Casetti, and G. Galante, "Concurrent multipath communication for real-time traffic," *Computer Communications*, vol. 30, no. 17, pp. 3307–3320, 2007.

[18] F. Song, H. Zhou, S. Zhang, H. Zhang, and I. You, "The throughput critical condition study for reliable multipath transport," *Computer Science and Information Systems*, vol. 10, no. 2, pp. 567–587, 2013.

[19] F. Song, R. Li, and H. Zhou, "Feasibility and issues for establishing network-based carpooling scheme," *Pervasive and Mobile Computing*, vol. 24, pp. 4–15, 2015.

[20] X. Zhang, Q. Chen, Z. Shi, and J. Liang, "Fault-Aware resource allocation for heterogeneous data sources with multipath routing," *Scientific Programming*, vol. 2017, Article ID 9749581, 12 pages, 2017.

[21] S. Sirisutthidecha and K. Maichalernnukul, "High-availability virtual communication for cloud access," *KSII Transactions on Internet and Information Systems*, vol. 10, no. 8, pp. 3455–3473, 2016.

[22] F. Song, Y.-T. Zhou, K. Kong, Q. Zheng, I. You, and H.-K. Zhang, "Smart collaborative connection management for identifier-based network," *IEEE Access*, vol. 5, pp. 7936–7949, 2017.

[23] K. Wang, H. Yin, W. Quan, and G. Min, "Enabling collaborative edge computing for software defined vehicular networks," *IEEE Network*, vol. 32, pp. 1–6, 2018.

[24] H.-Y. Hsieh and R. Sivakumar, "A transport layer approach for achieving aggregate bandwidths on multi-homed mobile hosts," in *Proceedings of the IEEE MOBICOM 2002*, Atlanta, Ga, USA, September 2002.

[25] M. Zhang, J. Lai, A. Krishnamurthy, L. Peterson, and R. Wang, "A transport layer approach for improving end-to-end performance and robustness using redundant paths," in *Proceedings of the USENIX*, Boston, Mass, USA, 2004.

[26] A. Ford, C. Raiciu, S. Barre, and J. Iyengar, Architectural Guidelines for Multipath TCP Development, draft-ietf-mptcp-architecture-00, 2010.

[27] W. Wang, X. Wang, and D. Wang, "Energy efficient congestion control for multipath TCP in heterogeneous networks," *IEEE Access*, vol. 6, pp. 2889–2898, 2017.

[28] R. Stewart, Q. Xie, K. Morneault, and C. Sharp, "Stream Control Transmission Protocol (SCTP)," RFC 2960, IETF, 2000.

[29] J. R. Iyengar, P. D. Amer, and R. R. Stewart, "Concurrent multipath transfer using SCTP multihoming over independent end-to-end paths," *IEEE/ACM Transactions on Networking*, vol. 14, no. 5, pp. 951–964, 2006.

[30] A. Abd El Al, T. Saadawi, and M. Lee, "LS-SCTP: A bandwidth aggregation technique for stream control transmission protocol," *Computer Communications*, vol. 27, no. 10, pp. 1012–1024, 2004.

[31] G. Ye, T. N. Saadawi, and M. Lee, "IPCC-SCTP: an enhancement to the standard SCTP to support multi-homing efficiently," in *Proceedings of the IEEE International Conference on Performance, Computing, and Communications (ICPCC '04)*, pp. 523–530, Phoenix, Ariz, USA, 2004.

[32] W. Zhang, W. Lei, Y. Guan, G. Li, and L. Yang, "Considerations for application-layer multipath transport control," *International Journal of Communication Systems*, vol. 30, no. 17, Article ID e3343, 2017.

[33] M. Coudron, *Novel approaches for multipath communications [Thesis for Doctor of Dissertation]*, University Pierre and Marie CURIE, 2016.

[34] S. Li and W. Sun, "A mechanism for resource pricing and fairness in peer-to-peer networks," *Electronic Commerce Research*, vol. 16, no. 4, pp. 425–451, 2016.

[35] S.-J. Lee and M. Gerla, "AODV-BR: Backup routing in ad hoc networks," in *Proceedings of the IEEE Wireless Communications and Networking Conference (WCNC '00)*, pp. 1311–1316, IEEE, Chicago, Ill, USA, September 2000.

[36] M. K. Marina and S. R. Das, "Ad hoc on-demand multipath distance vector routing," *Wireless Communications and Mobile Computing*, vol. 6, no. 7, pp. 969–988, 2006.

[37] Y. Yuan, H. Chen, and M. Jia, "An optimized ad-hoc on-demand multipath distance vector (AOMDV) routing protocol," in *Proceedings of the IEEE Asia-Pacific Conference on Communications*, pp. 569–573, Perth, Australia, October 2005.

[38] Z. Ye, S. V. Krishnamurthy, and S. K. Tripathi, "A routing framework for providing robustness to node failures in mobile ad hoc networks," *Ad Hoc Networks*, vol. 2, no. 1, pp. 87–107, 2004.

[39] X. Li and L. Cuthbert, "On-demand node-disjoint multipath routing in wireless ad hoc networks," in *Proceedings of the IEEE Conference on Local Computer Networks (LCN '04)*, pp. 419-420, Tampa, Fla, USA, November 2004.

[40] J. J. Gálvez and P. M. Ruiz, "Design and performance evaluation of multipath extensions for the DYMO protocol," in *Proceedings of the 32nd IEEE Conference on Local Computer Networks (LCN '07)*, pp. 885–892, October 2007.

[41] G. Koltsidas, F. Pavlidou, K. Kuladinithi, A. Timm-Giel, and C. Gorg, "Investigating the performance of multipath protocol for ad-hoc networks," in *Proceedings of the Annual IEEE International Symposuim on Personal, Indoor and Radio Communications (PIMRC '07)*, pp. 1–5, 2007.

[42] A. A. Pirzada, A. Datta, and C. McDonald, "Incorporating trust and reputation in the DSR protocol for dependable routing," *Computer Communications*, vol. 29, no. 15, pp. 2806–2821, 2006.

[43] S. Peng, W. Jia, G. Wang, J. Wu, and M. Guo, "Trusted routing based on dynamic trust mechanism in mobile ad-hoc networks," *IEICE Transaction on Information and Systems*, vol. E93-D, no. 3, pp. 510–517, 2010.

[44] J. Wang, Y. Liu, and Y. Jiao, "Building a trusted route in a mobile ad hoc network considering communication reliability and path length," *Journal of Network and Computer Applications*, vol. 34, no. 4, pp. 1138–1149, 2011.

[45] M. Sajwan, D. Gosain, and A. K. Sharma, "CAMP: cluster aided multi-path routing protocol for wireless sensor networks," *Wireless Networks*, 2018.

[46] R. Misra and C. R. Mandal, "Performance comparison of AODV/DSR on-demand routing protocols for ad hoc networks in constrained situation," in *Proceedings of the IEEE International Conference on Personal Wireless Communications (PWC '05)*, pp. 86–89, 2005.

[47] M. L. Shooman, *Reliability of Computer Systems and Networks: Fault Tolerance, Analysis, and Design*, John Wiley & Sons, Inc., New York, NY, USA, 2002.

[48] M. Abd-El-Barr, *Design and Analysis of Reliable and Fault-Tolerant Computer Systems*, World Scientific, Singapore, 2006.

[49] F. Lin, Y. Chen, J. An, and X. Zhou, "An evaluation method for network reliability in ad-hoc networks," in *Proceedings of the 4th International Conference on Multimedia Information Networking and Security (MINES '12)*, pp. 628–631, Nanjing, China, November 2012.

[50] B. Vaidya, S.-S. Yeo, D.-Y. Choi, and S. Han, "Robust and secure routing scheme for wireless multihop network," *Personal and Ubiquitous Computing*, vol. 13, no. 7, pp. 457–469, 2009.

[51] L. Reddeppa Reddy and S. V. Raghavan, "SMORT: Scalable multipath on-demand routing for mobile ad hoc networks," *Ad Hoc Networks*, vol. 5, no. 2, pp. 162–188, 2007.

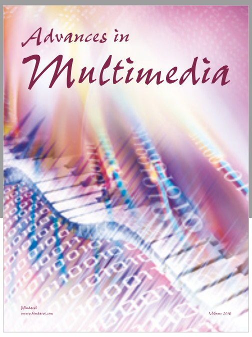
[52] Y. Wang, C. Lin, Q.-L. Li, and Y. Fang, "A queueing analysis for the denial of service (DoS) attacks in computer networks," *Computer Networks*, vol. 51, no. 12, pp. 3564–3573, 2007.

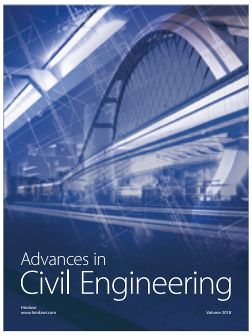
Journal of
Engineering

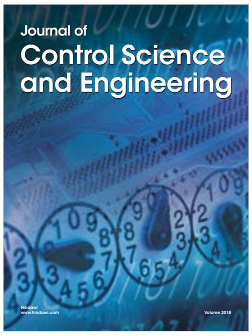
The Scientific
World Journal

International Journal of
Rotating
Machinery

Journal of
Sensors

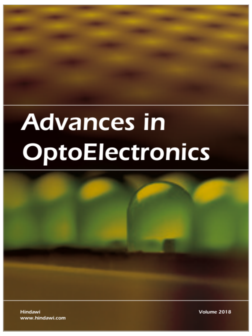

Advances in
Multimedia


Advances in
Civil Engineering


Journal of
Control Science
and Engineering

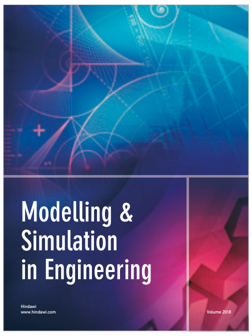
Journal of
Robotics

Journal of
Electrical and Computer
Engineering

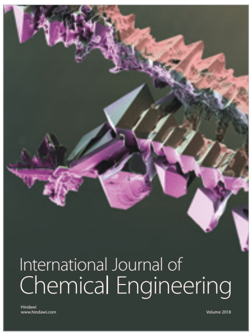

Advances in
OptoElectronics

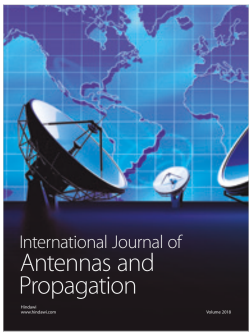
VLSI Design

International Journal of
Navigation and
Observation

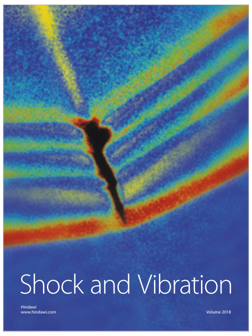

Modelling &
Simulation
in Engineering

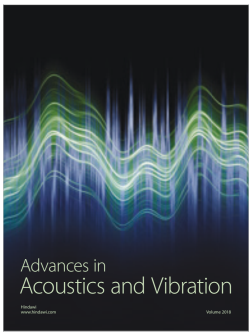
International Journal of
Aerospace
Engineering


International Journal of
Chemical Engineering


International Journal of
Antennas and
Propagation

Active and Passive
Electronic Components


Shock and Vibration


Advances in
Acoustics and Vibration