IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received August 7, 2020, accepted August 29, 2020, date of publication September 3, 2020, date of current version September 22, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3021475

Can Multipath TCP be Robust to Cyber Attacks With Incomplete Information?

YUANLONG CAO[1], JING CHEN[1], QINGHUA LIU[1], GANG LEI[1], HAO WANG[1], AND ILSUN YOU[2], (Senior Member, IEEE)
[1]School of Software, Jiangxi Normal University, Nanchang 330022, China
[2]Department of Information Security Engineering, Soonchunhyang University, Asan 31538, South Korea

Corresponding author: Ilsun You (ilsunu@gmail.com)

This work was supported in part by the National Natural Science Foundation of China (NSFC) under Grant 61962026, and in part by the Soonchunhyang University Research Fund.

ABSTRACT Promoted by the advancements in the various wireless access technologies, modern mobile devices equipped with multiple network interfaces are rapidly becoming the norm, and this provides a driving force for the large-scale deployment of the Multipath Transmission Control Protocol (MPTCP) in the current and future Internet. However, the simultaneous use of multiple network paths for concurrent multipath data transmission can make MPTCP have a larger attack surface than the traditional single-path transport protocols, and this may be likely to pose a risk of MPTCP being much more susceptible to cyber attacks. In this paper, we present a measurement method to investigate the vulnerability and robustness of MPTCP under cyber attacks with incomplete network information, by considering the fact that most cyber attacks normally lack of real-time information with respect to various MPTCP attributes. We mathematically characterize cyber attacks with incomplete network information from the viewpoints of both the cyber attacker and the MPTCP communication system, and then we introduce a mixed attack strategy, by jointly considering the features of both the random attacks and the selective attacks, to evaluate the robustness of MPTCP.

INDEX TERMS Multipath TCP, cyber attacks, incomplete information, graph-theoretic model, robustness analysis.

I. INTRODUCTION

In the last few years, wireless communication technologies, such as wireless broadband technology, wireless Wi-Fi technology, Bluetooth technology and so on, have undergone unprecedented development [1], [2]. Significant results in the wireless communication area offer today's mobile users ubiquitous Internet connectivity and high-quality data transmission services. Furthermore, the latest advancements in the wireless communication technologies provide a great driving force for the large-scale use of multi-homed mobile devices in the current and future Internet. Such multi-homed mobile devices (e.g., smartphones, netbooks, and portable computers) are commonly configured with several wireless network interfaces and multiple different IP addresses [3], [4]. They can simultaneously use their own network interfaces to establish multiple communication paths to access Internet, and allocate application data traffic across these multiple paths aiming to improve transmission performance and maximize resource usage, enabled by the promising Multipath Transmission Control Protocol (MPTCP) [5].

The MPTCP is a set of extensions to the Transmission Control Protocol (TCP), allowing to efficiently exploiting multiple network paths between a pair of endhosts for concurrent multipath data transmission, while presenting a regular TCP session to applications [6]. Nowadays, the MPTCP is becoming the transmission technology of choice for the multi-homed mobile devices [7]. Figure 1 portrays a basic MPTCP use case scenario in a public network area (e.g., a waiting hall) in which a multi-homed MPTCP-based mobile device, that has been equipped with three network interfaces (the Cellular, Wi-Fi and Bluethooth interfaces), is connecting with a server through three network paths (the Cellular link, the Wi-Fi link, and the Bluetooth link). That means the mobile device and the server can exchange the information between each other by simultaneously making use of the three paths.

The associate editor coordinating the review of this manuscript and approving it for publication was Luis Javier Garcia Villalba.

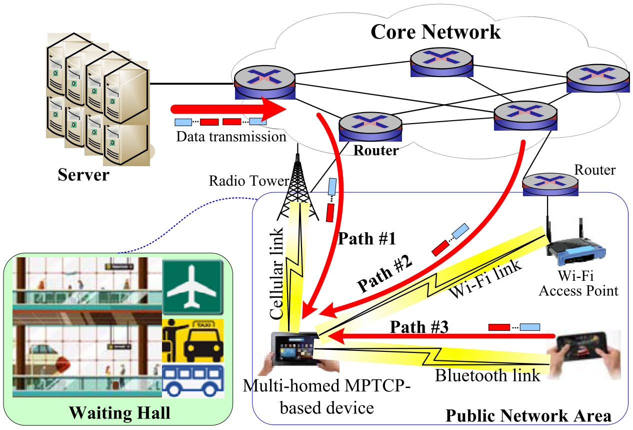


FIGURE 1. Multipath TCP communication in a public network area: a basic scenario.

In this case, the mobile device can aggregate the bandwidth of the three network links to possibly speed up the rate of data transmission, increase the end-to-end quality of service (QoS), and enhance the resilience of communication system, supported by the MPTCP technology. Due to its promising features of concurrent multipath transmission, the MPTCP technology is emerging as an important building block for the future Internet [8], [9].

Although the MPTCP technology has been received a high degree of attention and the continued interests in the MPTCP has resulted in many research publications, most of the researches in this area are concerned with the performance optimization of the MPTCP protocol itself, by using the optimized packet scheduling algorithms, congestion control mechanisms, path managing strategies, energy-saving methods, as well as promising network coding technologies and cross-layer activities, while the research on the invulnerability of MPTCP has rarely been reported. In fact, in MPTCP, allowing parallel data transmissions over multiple network links has the potential to increase the performance of data transmission; however, the multipathing paradigm with multiple TCP connections is likely to pose a risk of MPTCP being much more susceptible to cyber attacks [10]. This is because that most wireless networks used in MPTCP multipath transmission are short-range, high-speed but unlicensed wireless local area networks (i.e., public Wi-Fi networks), which are very prone to numerous kinds of cyber attacks [11].

Since MPTCP is not standardized to be more secure than the classic TCP [12], and, even more, it can become particularly vulnerable due to multiple TCP connections, therefore, the cyber attacks would be especially problematic for MPTCP. In MPTCP, each network path independently transfers data according to its own networking parameters (e.g., bandwidth, delay, etc.); however, the paths can mutually affect each other and interact with each other [13], [14], due to the MPTCP intrinsic natures of fully-reliable and in-order delivery. That is, if a network path in MPTCP experiences a cyber attack; it may become a poor-performing path (with huge transmission delay or high packet loss) or even an unavailable path (with short-term or complete network failures), and this would cause several negative behaviors to happen in multipath transmission, such as (i) inducing MPTCP to perform unnecessary retransmission in the unavailable path; (ii) resulting in out-of-order receipt of packets on the receiver side; (iii) affecting the performance robustness or/and structural robustness of MPTCP multipath transmission system. Although many efforts have been devoted to addressing the first two concerns, can MPTCP be robust against cyber attacks, especially from the perspective of attacks with incomplete information, is not yet well analyzed.

By jointly considering the fact that MPTCP would face network security implications and become particularly vulnerable due to some public networks used in the multipath transmissions can be extremely susceptible to attack, and the fact that most cyber attacks normally cannot fully understand the real-time network information with respect to the MPTCP communication system, in this paper, we present a method to measure the vulnerability and robustness of MPTCP under cyber attacks with incomplete network information. In particular, we aim to answer the following questions: (i) How robust the MPTCP is to the presence of cyber attacks, especially under the intentional attacks with incomplete information? And (ii) what is the performance penalty of MPTCP when the transmission paths within the MPTCP connection suffer from cyber attacks. The main contributions of our proposal are summarized as follows:

- It applies the graph theory to abstract the MPTCP communication system and mathematically characterizes the cyber attacks with incomplete information.
- It introduces a mixed attack strategy to investigate the vulnerability and robustness of MPTCP under a cyber attack with incomplete network information.

The reminder of the paper is organized as follows. Section II introduces the background and motivation of this paper. Section III proposes a methodology appropriate for investigating the vulnerabilities of MPTCP under cyber attacks with incomplete information. Section IV presents the robustness evaluation of MPTCP with different breadth parameters, precision parameters, and a mixed attack strategy, respectively. Section V highlights the limitations of the paper and discusses the open and interesting challenges. Section VI concludes the paper and gives our future work.

II. BACKGROUND AND MOTIVATION

As opposed to the single-path TCP, MPTCP can aggregate multiple network paths and simultaneously use these paths to exchange packets between endhosts. Figure 2 illustrates an overview of MPTCP, in which an MPTCP connection is established between Host A (act as MPTCP sender) and Host B (act as MPTCP receiver). With MPTCP, the two endhosts utilizes their own network interfaces (with different IP addresses) to establish multiple TCP connections (termed "MPTCP subflows") across potentially disjoint

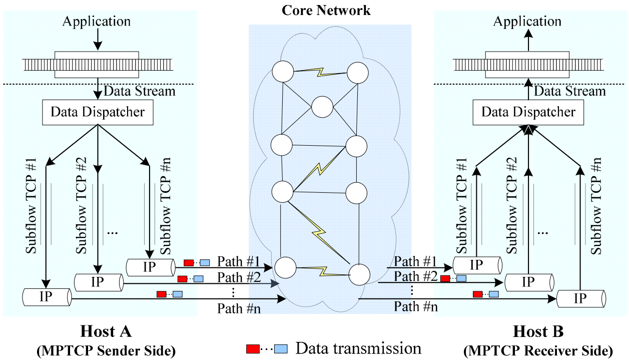


FIGURE 2. MPTCP overview.

network paths ($path\#1, path\#2, \cdots, path\#n$). At the sender side (Host A), once having application data traffic to be sent, MPTCP splits and dispatches the data traffic across these paths ($path\#1, path\#2, \cdots, path\#n$) simultaneously for concurrent multipath transmission. At the receiver side (Host B), the received but fragmented message can be reassembled in the receiver buffer for re-ordering and then flushed to upper layer in-order. The network paths in multipath transmission can be managed (e.g., creation, removal, reconnection) by MPTCP according to their own network condition.

With feature of multipathing service, MPTCP has obtained an ever-increasing number of researchers' interests. We here categorize the relevant literature into six groups: MPTCP scheduler optimization cases, MPTCP congestion control and fairness cases, MPTCP energy consumption cases, MPTCP with coding technique and cross-layer design cases, MPTCP partially reliable extension cases, and MPTCP security cases.

A. MPTCP SCHEDULER OPTIMIZATION CASES

Most of the researchers in this field have been devoted to optimizing the MPTCP scheduler. Saha *et al.* [8] proposed an agile MPTCP scheduler, called AMuSe, which allows MPTCP to perform near-optimally in terms of performance speed-up and reliability improvement in Dual-Band 802.11ad/ac wireless local area networks. Kimura *et al.* [15] provided a comprehensive analysis of MPTCP scheduler and then discussed both the lessons and opportunities of MPTCP packet scheduling methods. Xue *et al.* [16] considered the potentials of forward prediction model (FPM) and thereby designed a FPM-based scheduler and a dynamic feedback mechanism for MPTCP in lossy heterogeneous networks. Kimura *et al.* [17] presented three alternative packet scheduling decisions for MPTCP, which are called "largest congestion window (CW)-based scheduler", "smallest time (ST)-based scheduler", and "highest sending rate (SR)-based scheduler", respectively. Dong *et al.* [18] designed a novel packet loss-aware scheduler for MPTCP in order to enhance the MPTCP performance while significantly reducing extra bandwidth consumption in a high packet loss network condition. Le and Bui [19] developed a new MPTCP scheduler, which leverages per-path's forward delay as metric to send data.

B. MPTCP CONGESTION CONTROL AND FAIRNESS CASES

Apart from the optimization of MPTCP scheduler, there are also congestion control and fairness research aspects. Wei *et al.* [20] introduced a shared bottleneck-based congestion control mechanism for MPTCP in order to mitigate the out-of-order packet arrival problem, by detecting the shared bottlenecks and estimating the congestion level of each MPTCP subflow. Lı́źbben and Morgenroth [21] discussed the complex behaviors of MPTCP caused by the interaction of the loss-based congestion control and minimum Round-Trip Time (RTT) scheduling and then proposed several alternative congestion control algorithms for MPTCP as the corresponding countermeasure. Ferlin *et al.* [22] designed a practical shared bottleneck detection (PSBD)-based congestion control mechanism for MPTCP in order to make MPTCP flows remain fair to the TCP flows in a shared bottleneck scenario. Thomas *et al.* [23] presented a normalized multipath congestion control mechanism for MPTCP in order to achieve TCP-friendliness, by normalizing the throughput growth of individual MPTCP subflow. Zhao *et al.* [24] designed a fluid-based fairness-oriented algorithm in order to make MPTCP keep fairness to TCP and achieve congestion-balancing among MPTCP subflows.

C. MPTCP ENERGY CONSUMPTION CASES

Recently, there have been an increasing number of researchers who have been devoted to addressing the energy consumption problems in MPTCP. Zhao *et al.* [25], [26] introduced a flow-completion-time minimized congestion control mechanism to MPTCP in order to optimize the energy usage in datacenter networks. Wu *et al.* [27] presented an energy-efficient video flow rate allocation method in order to improve MPTCP energy efficiency while guaranteeing user-perceived quality for video streaming services. Wang *et al.* [28] designed an energy efficient congestion control algorithm for MPTCP, by jointly considering each path's RTT, loss rate, and energy efficiency. Kaup *et al.* [29] analyzed the battery power consumption in-depth when running MPTCP onto a power-constrained mobile phone, and then developed an energy consumption measuring and modeling study model for MPTCP. In particular, their research aimed to provide answers to the questions that how can MPTCP save energy in the best way. Our previous work [30] designed an application rate-aware energy saving-oriented subflow manager for MPTCP with goal of reducing the energy consumption in multipath transmissions while maintaining the performance level of MPTCP.

D. MPTCP WITH CODING TECHNIQUE AND CROSS-LAYER DESIGN CASES

Other researchers have concentrated their efforts on the MPTCP optimization by using network coding techniques and cross-layer designs, respectively. Xu *et al.* [31]

proposed a novel quality-based packet scheduling mechanism for MPTCP, by applying the promising pipeline coding technique, to tackle challenges specific to wireless multipath transmission. Cui *et al.* [32] introduced the emerging fountain coding (FC) technique to MPTCP, with consideration of the FC intrinsic random characteristics, and thereby designed a FC-based packet scheduling and transmission control algorithm for MPTCP. Xue *et al.* [33] revealed the unfair congestion control issue when applying the network coding techniques for MPTCP multipath transmission. As a remedy, the authors presented an end-to-end congestion control method to migrate unfairness among MPTCP subflows. Lim *et al.* [34] proposed a "MAC-MPTCP" cross-layer path manager, which leverages the networking parameter of MAC layer to estimate both the connectivity and transmission quality for each MPTCP path. Fukuyama *et al.* [35] presented a novel cross-layer design to tackle the packet loss problems in MPTCP wireless transmission, by detecting the frame error in data-link layer. Our previous work MPTCP-RC [36] optimized the MPTCP performance by jointly considering the receiver's intelligence and cross-layer activities.

E. MPTCP PARTIALLY RELIABLE EXTENSION CASES

More recently, many researchers have been devoted to extending MPTCP with partial reliability services. Xu *et al.* [37] initiated a partial reliability extension for MPTCP (known as "initiative PR-MPTCP"), in which both the sender and the receiver can support the partially reliable transmission services for the time-sensitive network applications. Qin *et al.* [38] proposed a message-oriented partial-reliability extension for MPTCP in order to allow the MPTCP sender to abandon the expired message and tell the receiver of the message abandonment decision. Diop *et al.* [39] presented a Quality of Service (QoS)-oriented partial reliability extension for MPTCP. This variant was designed in order to improve user's quality of experience (QoE) for the real-time interactive multimedia applications, by giving up the transmission of expired message in MPTCP multipath transmission. Although the partial reliability extensions have been demonstrated useful for the delay-constrained applications, it is worthy to note that extending MPTCP with partial reliability services is still in controversy because MPTCP is designed in order to provide connection-oriented transport services for the loss-sensitive rather than time-sensitive Internet applications, as discussed in our previous work [4].

F. MPTCP SECURITY CASES

Nowadays, the research focus is shifting toward securing MPTCP multipath communications. Noh *et al.* [40] designed a secure and lightweight subflow establishment mechanism for MPTCP, by utilizing a digital signature strategy to prevent the persistent ADD_ADDR attack. Jadin *et al.* [41] designed a secure MPTCP variant by closely integrating authentication and encryption inside the MPTCP protocol. Nguyen *et al.* [42] investigated the Autonomous System (AS)-level Man-in-the-Middle (MITM) attacks acting at the robustness of MPTCP communications, reported which countries and regions had a high-level of robustness against the MITM attacks by studying the AS level graph, and provided a countermeasure in preventing MPTCP from the AS-level MITM attacks when concurrently using multiple Internet-scale paths for multipath communications. Munir *et al.* [43] first reported the potential security vulnerabilities in MPTCP due to cross-path interactions among MPTCP subflows, caused by two typical attacks: connection hijack attacks and directed traffic diversion attacks, and then proposed the corresponding countermeasure proposal to guarantee MPTCP to be no less secure than TCP under the two typical attacks.

In this paper, we present a new vulnerability measurement method to investigate the robustness of MPTCP under cyber attacks with incomplete network information [44]. To this end, we apply the graph theory to abstract the MPTCP communication system, and then introduce a mixed attack model with incomplete information for MPTCP. To the best of our knowledge, this paper is the first study to investigate the vulnerability and robustness of MPTCP under a cyber attack with incomplete network information. We hope to provide a new thought for the measurement of the MPTCP vulnerability under cyber attacks and attract more researchers to pay attention on this topic, after all, as the simultaneous use of multiple network paths in MPTCP is a benefit, there is certainly an additional vulnerability which comes along with that. It is worth mentioning that in our paper, the mentioned cyber attack can be any one of particular type of attack, such as Flood DOS attacks or man-in-the-middle attacks, which can launch false data injection attacks and thus prevents the usage of a network path in MPTCP (namely, to make the MPTCP transmission experience network failure).

III. METHODOLOGY

In this section, we first map the dynamical MPTCP system onto a directed graph, apply the graph theory to abstract the MPTCP communication system, and then introduce an attack strategy with incomplete information that can be used to investigate the vulnerabilities of MPTCP.

A. MPTCP-GRAPH MAPPING

We focus on a steady-state MPTCP communication system and act with a series of assumptions: (i) there are two multi-homed end-hosts equipped with the same amount of network interfaces, (ii) each network interface has its own unique IP address, (iii) the two end-hosts are communicating with each other using multiple end-to-end independent transmission paths (MPTCP subflow), enabled by MPTCP, (iv) all the transmission paths within the MPTCP connection are available for data transmission, and (v) a cyber attacker can access partial network resources and obtain partial MPTCP paths' QoS-related networking parameters (namely incomplete information of MPTCP). Since MPTCP message exchanging between the two end-hosts (a sender and a receiver) is bidirectional, therefore, the MPTCP multipath communication system can be abstractly represented by a graph G with m nodes and n edges, by using the following equation,

$$G = (V, E), \tag{1}$$

which $V = \{\upsilon_1, \upsilon_2, \cdots, \upsilon_m\}$ is the set of nodes (each node is representative for each network interface in MPTCP multipath communication system), therefore, there is

$$m = |V|; \tag{2}$$

And $E = \{(\upsilon_i, \upsilon_j)\}$ is a set of edges (each edge corresponds to each transmission path in MPTCP communication system), therefore, there is

$$n = |E|; \tag{3}$$

The edge set E represents the set of all transmission paths in the MPTCP multipath communication system, which can be represented by the adjacency matrix Z as follows,

$$Z = \begin{pmatrix} z_{1,1} & \cdots & z_{1,m} \\ \vdots & \ddots & \vdots \\ z_{m,1} & \cdots & z_{m,m} \end{pmatrix}. \tag{4}$$

If there is a transmission path between the nodes υ_i and υ_j, the two nodes are considered to be connected by one edge, and this can be represented by the following expression,

$$z_{i,j} = (\upsilon_i, \upsilon_j) = \begin{cases} 1, & \text{if } \upsilon_i \text{ and } \upsilon_j \text{ is connected with each other;} \\ 0, & \text{otherwise.} \end{cases} \tag{5}$$

In this paper, we only consider a symmetric MPTCP communication system. That is, for each two corresponding nodes υ_i and υ_j, there is one and only one transmission path between them for MPTCP packet exchange. For convenience, the edge set E is hereafter represented to as $E = \{e_1, e_e, \cdots, e_n\}$.

B. ATTACK MODE AND STRATEGY

Today's cyber attacks faced by communication networks can generally be grouped into two typical types: random attacks and selective attacks.

- In a random attack, the attacker "knows nothing" about the MPTCP communication system. In other words, it is a "zero information attack mode". In this attack mode, the attacker can only attack the entire MPTCP communication system in a random way.
- In a selective attack, the attacker "knows everything" about the MPTCP communication system. In other words, it is a "complete information attack mode". In this attack mode, the attacker can select the target paths to attack according to the paths' importance.

In practice, the communication networks would face neither "zero information attack" nor "complete information attack" in most cases, but "incomplete information attack", that is, the attackers can only access partial network resources and obtain partial network information [44]. Therefore, we need to construct an attack mode with incomplete information to evaluate the vulnerability and robustness of MPTCP. To simulate an attack mode with incomplete information, two key factors need to be determined: exposed region and attack strategy.

The exposed region is an optimal attacking region in the MPTCP communication system in which an attacker perfectly knows how important and what information of the transmission paths. Let $\mathbb{R}$ and $\mathbb{N}$ be the set of exposed region and unexposed region, which corresponds to the known transmission paths and the unknown transmission paths within the MPTCP communication system, respectively. Therefore, we have

$$\mathbb{R} \cup \mathbb{N} = E. \tag{6}$$

Obviously, an attacker can work better with a bigger exposed region. We will present the exposed region generating method in more detail in the next subsection (Subsection C).

When the exposed region is determined, the attack strategy plays important role to achieve an optimal attack effect under the incomplete information. In the research field of network robustness, there are many attack strategies proposed, such as random attack, degree-based attack, centrality-based attack, and mixed attack [45]–[49]. Among the many attack strategies, we in this paper adopt the most widely-used "mixed attack strategy" to evaluate the vulnerability and robustness of the MPTCP communication system. In this strategy, the attacker uses "degree-based attack strategy" to launch an attack against the paths within the exposed region $\mathbb{R}$ firstly, then uses "random attack strategy" to launch an attack against the paths within the unexposed region $\mathbb{N}$. The principles of the mixed attack strategy used in this paper are as below:

i) Firstly, all the paths in the exposed region $\mathbb{R}$ are attacked in turn according to their rank of importance. That is, the important paths will be attacked one by one.

ii) After all the paths within the exposed region $\mathbb{R}$ are attacked, the paths within the unexposed region $\mathbb{N}$ are attacked again. For the paths in this region, a random attack strategy is adopted by the attacker to launch attack.

iii) For any path in either the exposed region $\mathbb{R}$ or the unexposed region $\mathbb{N}$, if it is attacked, it may experience timeout events (or path failures) and become unavailable, as a result, it can be deactivated and removed from the MPTCP communication system. The path deactivation rate (denoted as P_d) can be expressed by

$$P_d = \frac{H_d}{n}, \tag{7}$$

which H_d is the number of paths deactivated by the MPTCP sender.

C. EXPOSED REGION GENERATING

The generating of exposed region $\mathbb{R}$ depends on how and to what extent an attacker already understands the network information of MPTCP communication system. Under the incomplete information condition, the more information the attacker obtained, the bigger value of $\mathbb{R}$ will be. To determine the exposed region, the breadth parameter (denoted as ξ) and the precision parameter (denoted as ℓ) of $\mathbb{R}$ should be first defined,

- The breadth parameter ξ ($\xi \in [0, 1]$) represents the proportion of the number of paths in an exposed region to the number of all paths in the MPTCP communication system. Because that $(\xi * n)$ corresponds to the size of the exposed region $\mathbb{R}$, therefore, the value of ξ gets larger, the value of $\mathbb{R}$ becomes larger.
- The precision parameter $\ell\,(\ell \in [0, \infty])$ reflects the precision of the important paths within the MPTCP communication system included into the exposed region.

Based on both ξ and ℓ, the calculation of $\mathbb{R}$ can be transformed to a path sampling problem with unequal probabilities. Since the importance of an MPTCP path is related to the attacker's purpose of attacking the MPTCP communication system, therefore, in this paper, the more important the path within the MPTCP communication system is, the higher the probability of sampling. In MPTCP communication system, a path with a higher performance (such as, a higher bandwidth, a lower delay, and so on) generally means it has relatively more importance. In this paper, we adopt the most widely-used available bandwidth to reflect the importance of each MPTCP path. The available bandwidth estimation for each path within the MPTCP connection can by expressed by using the following equation [50],

$$\mathbb{C}_{e_i} = \frac{Size_{packet}}{RTT_{e_i}}, \tag{8}$$

which $Size_{packet}$ is the packet size of each any MPTCP packet sent through path e_i. $\mathbb{C}_{e_i}$ and RTT_{e_i} are the estimated available bandwidth and round-trip time of the path e_i, respectively.

To calculate the sampling probability for each MPTCP path, we should sort all the paths within the MPTCP communication system in descending order according to their own available bandwidth ($\mathbb{C}$). Let κ_i ($\kappa_i \in \{1, 2, \cdots, n\}$) be the order of path e_i, and $\psi_i = \kappa_i^{-\ell}$ be an auxiliary variable of path e_i, then the sampling probability, sP_i, can be defined as:

$$sP_i = \psi_i \times \frac{1}{\sum_{j=1}^{|n|} \psi_j} = \kappa_i^{-\ell} \times \frac{1}{\sum_{j=1}^{|n|} \kappa_j^{-\ell}} \tag{9}$$

Through the above equation, we can see that a MPTCP path with a larger value of $\mathbb{C}_{e_i}$ can be ranked a higher order and have a larger sampling probability, in other words, it can be more prone to be attacked. Based on per-path's sampling probability, we can extract $N = (\xi * n)$ paths from E to generate an exposed region $\mathbb{R}$ and then use it to simulate an attack with incomplete information for the vulnerability evaluation of MPTCP.

IV. MEASUREMENT

A. SIMULATION TOPOLOGY

The performance evaluation of MPTCP under cyber attacks with incomplete information was carried out on NS-2 (Network Simulator 2 version 2.35) [51] in which the MPTCP patch [52] has already been embedded. The simulations considered an MPTCP-based heterogeneous communication system illustrated in Figure 3. The two MPTCP endhosts are connecting with each other through six asymmetric network paths (denoted as $\#1, \#2, \cdots, \#6$, respectively). The total simulation time is set to 60 seconds.

1) MPTCP PATH SETTINGS

All the six MPTCP paths are set with the same bandwidth (10 Mbps) but with different propagation delays in order to simulate a heterogeneous network condition. To this end, the propagation delay ranges of these paths are set with 10-20 milliseconds, 20-30 milliseconds, 30-40 milliseconds, 40-50 milliseconds, 50-60 milliseconds, and 60-70 milliseconds, respectively. The simulation parameters illustrated in Table 1 are utilized for configuring the six network paths. The other simulation parameters of the MPTCP protocol utilize the predefined values of the NS-2 MPTCP module.

2) PACKET LOSS MODEL

In the simulation, all the network access parts of the six paths are attached to two loss models, which are the uniform packet loss model and the 2-state Markov loss model (known as *Gilbert loss model*, it is a 2-state Markov chain-based framework widely used to predict infrequent continuous packet loss), in order to simulate the uniformly distributed packet drops caused by network congestion and the infrequent continuous packet drops caused by the wireless problems, respectively [4].

3) CYBER ATTACK SIMULATION

Moreover, considering the fact that an attacker in general attempts to disperse massive attack traffic to crash a target network [53], therefore, we simulate a path under attacking by removing the path from the multipath transmission. Any of the six paths can become the attack target and experience an attack. Taking a path $\#x$ $(1 \leq x \leq 6)$ for example, if it suffers from an attack, it will become unavailable and be removed from the MPTCP communication system. How many or exactly which paths under attacking are decided by the breadth parameter ξ and the precision parameter ℓ, in order to simulate the cyber attacks with incomplete infor-

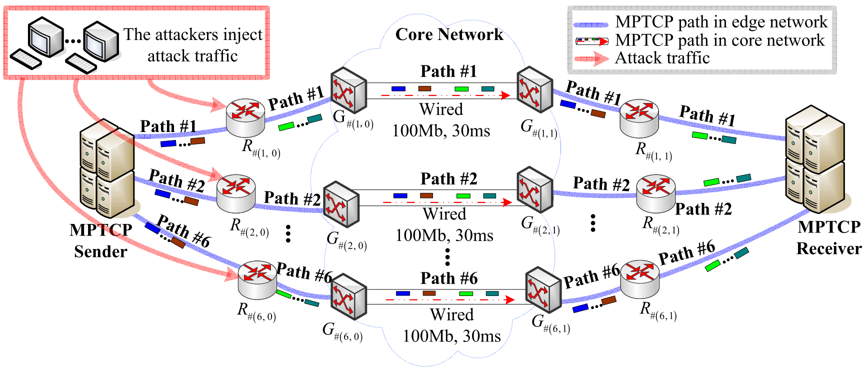


FIGURE 3. Simulation topology.

TABLE 1. Network parameters used for configuring the MPTCP paths.

Network Parameters	Path #1	Path #2	Path #3	Path #4	Path #5	Path #6
Edge network bandwidth	10Mbps	10Mbps	10Mbps	10Mbps	10Mbps	10Mbps
Edge network delay	10-20ms	20-30ms	30-40ms	40-50ms	50-60ms	60-70ms
Edge network queue type	Droptail	Droptail	Droptail	Droptail	Droptail	Droptail
Core network bandwidth	10Mbps	10Mbps	10Mbps	10Mbps	10Mbps	10Mbps
Core network delay	30ms	30ms	30ms	30ms	30ms	30ms
Uniform loss rate	1%	1%	1%	1%	1%	1%
Markov loss rate	1%	1%	1%	1%	1%	1%

mation. All the attack actions begin at the 5.0^{th} second of simulation time, that is, a path can experience path removal after 5 seconds of simulation time if it is marked as "attack target" state.

B. SIMULATION RESULTS

In this section, in order to investigate the impact of cyber attacks, we evaluate the performance robustness of MPTCP under the conditions of no attack and cyber attacks, respectively. Furthermore, we apply cyber attacks with different precision parameters, breadth parameters and attack strategies to measure the presence of cyber attack with incomplete information affecting the robustness of MPTCP. We adopt the packet sending times and throughput to reflect the performance robustness of MPTCP since the two metrics are widely used to portray the characteristics of multipath transport protocols [54], [55].

1) THE EFFECT OF THE PRECISION PARAMETER ℓ ON MPTCP

In order to study the effect of the precision parameter ℓ on the performance robustness of MPTCP, we conduct three different test cases: MPTCP without any attacks, MPTCP under random attacks, and MPTCP under selective attacks. Figures 4 and 5 present the performance robustness comparison of MPTCP in terms of packet sending times (aka sending DSN (Data Sequence Number)) and throughput under the three different test cases, respectively. In order to better illustrate the effect of the precision parameter ℓ on the performance robustness of MPTCP, we assume that the breadth parameter ξ is a constant with a value of $\frac{1}{6}$, which means, there is only one path within the MPTCP connection to be attacked by either random attacks or selective attacks.

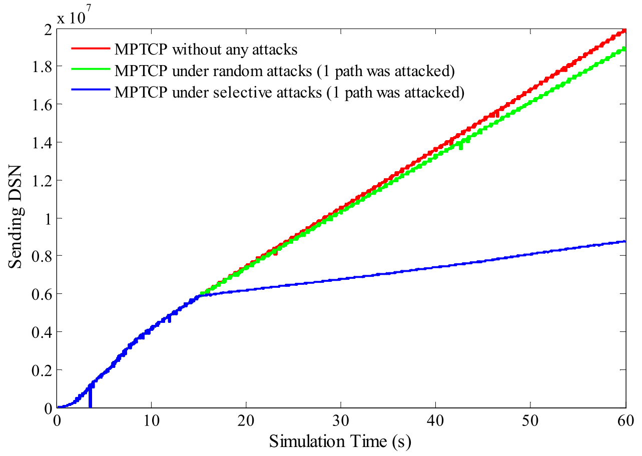


FIGURE 4. The performance robustness comparison of MPTCP in terms of packet sending times under three different test conditions: without any attacks, and under attacks with precision breadth parameters.

When comparing the results of the three test cases, we can note that: (i) the "MPTCP without any attacks" case can achieve the highest performance in terms of both the packet sending times and the throughput, by simultaneously making use of all the paths for the transmission of MPTCP packets; (ii) in both the "MPTCP under random attacks" case and the "MPTCP under selective attacks" case, the performance robustness of MPTCP can be degraded with the presence of either random attacks or selective attacks, because that any one of the paths under attacks can cause the transmission interruptions in other paths; and (iii) the "MPTCP under

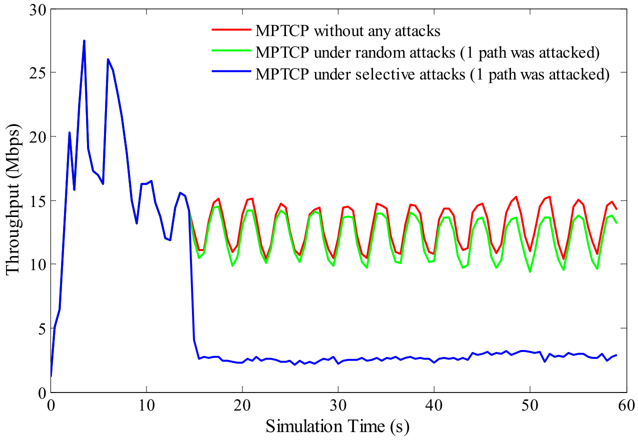


FIGURE 5. The performance robustness comparison of MPTCP in terms of throughput under three different test conditions: without any attacks, and under attacks with precision breadth parameters.

selective attacks'' case performs worse than the ``MPTCP under random attacks'' case in terms of packet sending times and throughput. This is because in the random attack mode, any path including an under-performing path which has the lowest importance in multipath transmission may become the attack target. While in the selective attack mode, the target path that performs the best and has the highest importance in the MPTCP communication system can be accurately attacked and become unavailable for data transmission.

The above results reveal that: (i) the presences of cyber attacks can affect the performance robustness of MPTCP in terms of either packet sending times or throughput; (ii) the selective attack can cause a greater impact on the performance robustness of MPTCP. Thereby, we can conclude that the precision parameter has an important role to play in the effectiveness of a cyber attack and thereby has significant impact (side-effect) on the performance robustness of MPTCP.

2) THE EFFECT OF THE BREADTH PARAMETER ξ ON MPTCP

To analyze the effect of the breadth parameter ξ on the performance robustness of MPTCP, we conduct six different test cases, which are MPTCP without any attacks, MPTCP under selective attacks with 1 target path, MPTCP under selective attacks with 2 target paths, MPTCP under random attacks with 3 target paths, MPTCP under selective attacks with 4 target paths, and MPTCP under selective attacks with 5 target paths. In order to better illustrate the effect of the breath parameter ξ on the performance robustness of MPTCP, we assume that the precision parameter ℓ is fixed, which means under the condition of attacks with incomplete information, the attacker fully knows partial paths' importance degree of the MPTCP communication system.

Figures 6 and 7 portray the performance robustness comparison of MPTCP in terms of packet sending times and throughput under the six test cases, respectively. When comparing the results of the six test cases, we can note that the

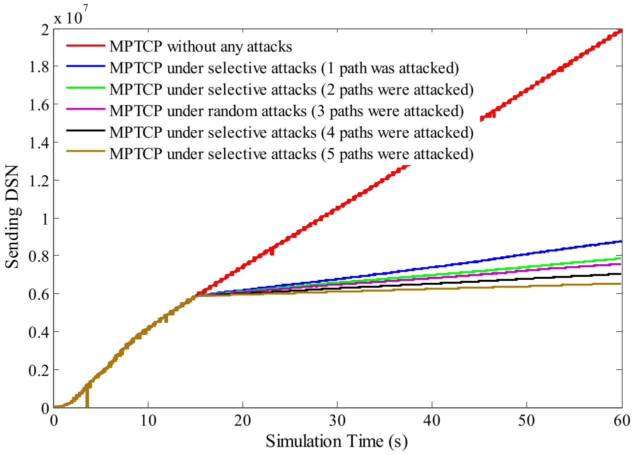


FIGURE 6. The performance robustness comparison of MPTCP in terms of packet sending times under six different test conditions: without any attacks, and under attacks with different breadth parameters.

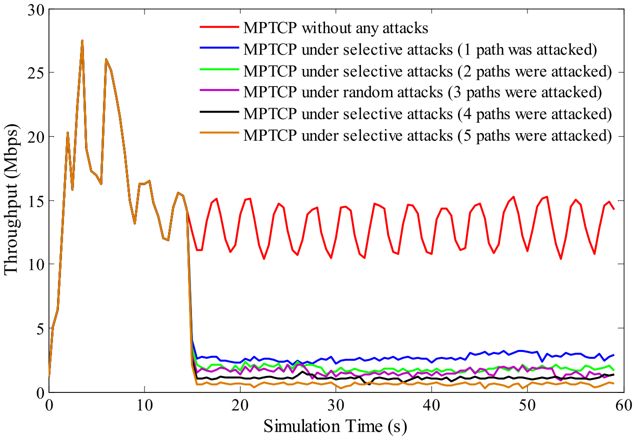


FIGURE 7. The performance robustness comparison of MPTCP in terms of throughput under six different test conditions: without any attacks, and under attacks with different breadth parameters.

performance robustness of MPTCP in any given case can decrease sharply at the start of attacks. In addition, we can also note that under the conditions of attacks, the ``MPTCP under selective attacks with 1 target path'' case performs the best performance, and the ``MPTCP under selective attacks with 5 target paths'' case performs the worst performance in terms of both the packet sending times and the throughput of MPTCP. This means, cyber attacks with different values of breadth parameters can cause variable levels of destruction on the performance robustness of MPTCP, and more precisely, the performance robustness of MPTCP can decrease as the breadth parameter ξ (namely the exposed region $\mathbb{R}$) increases. Thereby, we can conclude that like the precision parameter, the breadth parameter also has an important role to play in the influence of cyber attacks on the performance robustness of MPTCP.

3) THE EFFECTS OF A MIXED ATTACK ON MPTCP WITH A GIVEN EXPOSED REGION $\mathbb{R}$

We conduct a test scenario to investigate the performance robustness of MPTCP under attacks with a proper exposed region ℝ and a mixed attack strategy. In this test scenario, it is assumed that the attacker "knows" the importance degree of four paths, and "does not know" the information of the other two paths (that is, the exposed region ℝ is already given). Based on the given ℝ, we implement a mixed attack strategy with the following principles to attack the MPTCP communication system: (i) firstly, the attacker attacks the MPTCP paths in the exposed region ℝ in turn according to the importance degree of these paths (from the path with the highest importance degree to the one with the lowest importance degree, using the selective attack mode); (ii) after all MPTCP paths exposed region ℝ are attacked and become unavailable, the MPTCP paths in the unexposed region ℕ are attacked and removed in a random way (using the random attack mode).

Figures 8 and 9 show the performance robustness comparison of MPTCP in terms of packet sending times and throughput under attacks with the given ℝ and the mixed attack strategy. From the two result figures, we can note that both the packet sending times and the throughput of MPTCP are going to fall off a cliff and then decrease to zero sharply as all the six MPTCP paths are attacked one after another under the attacks with the mixed attack strategy. This is because that as all the paths within the MPTCP communication system become unavailable and quit from the multipath transmission one-by-one, the structural robustness of the MPTCP communication system suffers from the total interruption of paths, and this causes serious damage to the performance robustness of the MPTCP communication system. Therefore, we can conclude that a cyber attack, even with incomplete information, can lead to a significant deterioration of performance robustness of MPTCP, through a proper attack strategy. In other words, the MPTCP communication systems are vulnerable to a cyber attack; even the attack can only obtain incomplete network information.

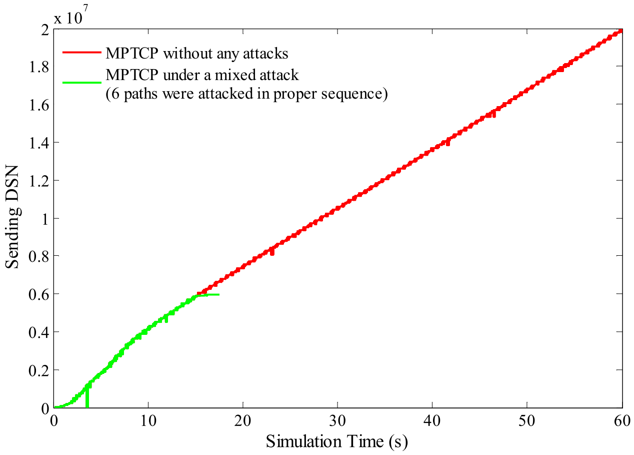


FIGURE 8. The performance robustness comparison of MPTCP in terms of packet sending times under two test conditions: without any attacks, and under a mixed attack in which 6 paths were attacked in proper sequence.

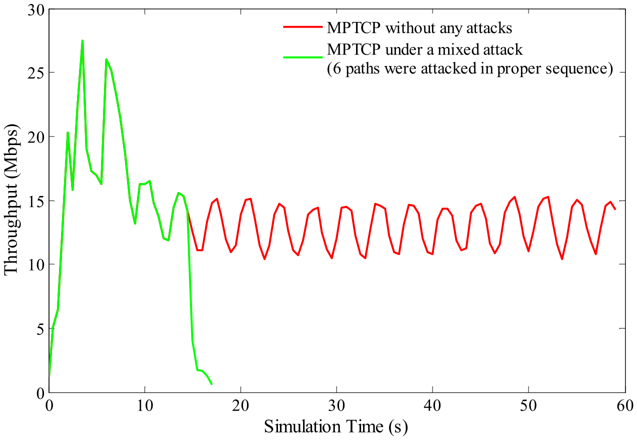


FIGURE 9. The performance robustness comparison of MPTCP in terms of throughput under two test conditions: without any attacks, and under a mixed attack in which 6 paths were attacked in proper sequence.

V. DISCUSSION

The objective of this paper is to introduce a cyber attack mode with incomplete information to MPTCP and provide a simulated study to show how robust the MPTCP is to the presence of cyber attacks with incomplete information. From the simulation results, we can note that the behaviors of cyber attacks can present an obvious impact on the robustness of MPTCP, and the impact degree depends on the precision parameters, breadth parameters and attack strategies of cyber attacks. We here discuss the limitations of our paper and highlight some interesting problems. We hope to attract more researchers to notice this topic and drive this research filed forward.

- In order to investigate the vulnerability and robustness of MPTCP, we simply consider that any one of the MPTCP paths can experience network failure when it suffers from cyber attacks, motivated by the reason that in a computer network, attackers usually exploit network vulnerabilities to disable a target network [56]. Recently, many network security studies [57]–[60] have showed complex behaviors of cyber attacks that are necessary for realistic testing environments. The authors encourage more researchers to consider the cyber attack traffic with the real-world characteristics to investigate the vulnerability and robustness of MPTCP.
- It should be noted that there is no exact rule for measuring the robustness of MPTCP. We thus in this paper adopted the throughput and packet sending times as the metrics to analyze the performance robustness of MPTCP under cyber attacks. We argue that designing a rich set of metrics appropriated for MPTCP robust measurement is an interesting topic worth further study.

VI. CONCLUSION AND FUTURE WORK

With the promising feature of simultaneous transmission of data through multiple TCP connections, MPTCP is being considered as the transport technique of the popular choice for the modern multi-homed mobile devices, however, its multipathing paradigm may be likely to pose a risk of MPTCP being much more susceptible to cyber attacks, especially when the unlicensed wireless local area networks is used in multipath transmissions. Meanwhile, taking into account the fact that most cyber attacks normally would not have complete knowledge on the dynamic MPTCP communication systems, in this paper, we introduced an attack model with incomplete information to investigate the vulnerability and robustness of MPTCP, by using graph-theoretic and mathematical models to abstract and characterize the cyber attacks and the MPTCP communication system, respectively. By simulations, we explored how robust the MPTCP was to the presence of cyber attacks with incomplete information, and what was the performance penalty of MPTCP when the paths suffer from cyber attacks.

Our future work will apply the smart collaborative theory to MPTCP to build a "smart collaborative MPTCP" mode, in which all the network elements (i.e., transmission nodes and protocol stacks) can work in full cooperation, by inter-node collaborations and cross-layer activities, to possibly enhance the robustness of MPTCP under cyber attacks. It is worth noting that build a "smart collaborative MPTCP" is actually a significant challenge because of the diversity of network nodes, we will consider applying the promising Software Defined Network (SDN) technology to counteract the diversity of network nodes.

REFERENCES

[1] M. R. Palash and K. Chen, "MPWiFi: Synergizing MPTCP based simultaneous multipath access and WiFi network performance," *IEEE Trans. Mobile Comput.*, vol. 19, no. 1, pp. 142–158, Jan. 2020.

[2] F. Song, Z. Ai, Y. Zhou, I. You, K.-K.-R. Choo, and H. Zhang, "Smart collaborative automation for receive buffer control in multipath industrial networks," *IEEE Trans. Ind. Informat.*, vol. 16, no. 2, pp. 1385–1394, Feb. 2020.

[3] J. Wu, R. Tan, and M. Wang, "Energy-efficient multipath TCP for quality-guaranteed video over heterogeneous wireless networks," *IEEE Trans. Multimedia*, vol. 21, no. 6, pp. 1593–1608, Jun. 2019.

[4] Y. Cao, L. Zeng, Q. Liu, G. Lei, M. Huang, and H. Wang, "Receiver-assisted partial-reliable multimedia multipathing over multi-homed wireless networks," *IEEE Access*, vol. 7, pp. 177675–177689, 2019.

[5] A. Ford, C. Raiciu, M. Handley, and O. Bonaventure, *TCP Extensions for Multipath Operation With Multiple Addresses*, document IETF RFC 6824, Jan. 2013.

[6] P. Ignaciuk and M. Morawski, "Discrete-time sliding-mode controllers for MPTCP networks," *IEEE Trans. Syst., Man, Cybern. Syst.*, early access, Jan. 1, 2020.

[7] H. Sinky, B. Hamdaoui, and M. Guizani, "Seamless handoffs in wireless HetNets: Transport-layer challenges and multi-path TCP solutions with cross-layer awareness," *IEEE Netw.*, vol. 33, no. 2, pp. 195–201, Mar. 2019.

[8] S. Saha, S. Aggarwal, R. Pathak, D. Koutsonikolas, and J. Widmer, "AMuSe: An agile multipath-TCP scheduler for dual-band 802.11ad/ac wireless LANs," in *Proc. ACM MobiCom*, 2019, pp. 1–6.

[9] B. Y. L. Kimura, D. C. S. F. Lima, L. A. Villas, and A. A. F. Loureiro, "Interpath contention in MultiPath TCP disjoint paths," *IEEE/ACM Trans. Netw.*, vol. 27, no. 4, pp. 1387–1400, Aug. 2019.

[10] 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.

[11] F. Song, Y.-T. Zhou, Y. Wang, T.-M. Zhao, I. You, and H.-K. Zhang, "Smart collaborative distribution for privacy enhancement in moving target defense," *Inf. Sci.*, vol. 479, pp. 593–606, Apr. 2019.

[12] C. Paasch and O. Bonaventure, *Securing the Multipath TCP Handshake With External Keys*, document draft-paasch-mptcp-ssl-00, IETF, 2012. [Online]. Available: https://tools.ietf.org/id/draft-paasch-mptcp-ssl-00.html

[13] B.-H. Oh and J. Lee, "Feedback-based path failure detection and buffer blocking protection for MPTCP," *IEEE/ACM Trans. Netw.*, vol. 24, no. 6, pp. 3450–3461, Dec. 2016.

[14] Y. Cao, M. Collotta, S. Xu, L. Huang, X. Tao, and Z. Zhou, "Towards adaptive multipath managing: A lightweight path management mechanism to aid multi-homed mobile computing devices," *Appl. Sci.*, vol. 10, no. 1, pp. 1–18, 2020.

[15] B. Y. L. Kimura, D. C. S. F. Lima, and A. A. F. Loureiro, "Packet scheduling in multipath TCP: Fundamentals, lessons, and opportunities," *IEEE Syst. J.*, early access, Jan. 27, 2020, doi: 10.1109/JSYST.2020.2965471.

[16] K. Xue, J. Han, D. Ni, W. Wei, Y. Cai, Q. Xu, and P. Hong, "DPSAF: Forward prediction based dynamic packet scheduling and adjusting with feedback for multipath TCP in lossy heterogeneous networks," *IEEE Trans. Veh. Technol.*, vol. 67, no. 2, pp. 1521–1534, Feb. 2018.

[17] B. Y. L. Kimura, D. C. S. F. Lima, and A. A. F. Loureiro, "Alternative scheduling decisions for multipath TCP," *IEEE Commun. Lett.*, vol. 21, no. 11, pp. 2412–2415, Nov. 2017.

[18] E. Dong, M. Xu, X. Fu, and Y. Cao, "LAMPS: A loss aware scheduler for multipath TCP over highly lossy networks," in *Proc. IEEE LCN*, Oct. 2017, pp. 1–9.

[19] T.-A. Le and L. X. Bui, "Forward delay-based packet scheduling algorithm for multipath TCP," *Mobile Netw. Appl.*, vol. 23, no. 1, pp. 4–12, Feb. 2018.

[20] W. Wei, K. Xue, J. Han, D. S. L. Wei, and P. Hong, "Shared bottleneck-based congestion control and packet scheduling for multipath TCP," *IEEE/ACM Trans. Netw.*, vol. 28, no. 2, pp. 653–666, Apr. 2020.

[21] R. Lubben and J. Morgenroth, "An odd couple: loss-based congestion control and minimum RTT scheduling in MPTCP," in *Proc. IEEE LCN*, Oct. 2019, pp. 1–8.

[22] S. Ferlin, O. Alay, T. Dreibholz, D. A. Hayes, and M. Welzl, "Revisiting congestion control for multipath TCP with shared bottleneck detection," in *Proc. IEEE INFOCOM*, Apr. 2016, pp. 1–9.

[23] Y. Thomas, M. Karaliopoulos, G. Xylomenos, and G. C. Polyzos, "Low latency friendliness for multipath TCP," *IEEE/ACM Trans. Netw.*, vol. 28, no. 1, pp. 248–261, Feb. 2020.

[24] J. Zhao, C. Xu, J. Guan, and H. Zhang, "A fluid model of multipath TCP algorithm: Fairness design with congestion balancing," in *Proc. IEEE ICC*, Jun. 2015, pp. 6965–6970.

[25] J. Zhao, J. Liu, H. Wang, C. Xu, W. Gong, and C. Xu, "Measurement, analysis, and enhancement of multipath TCP energy efficiency for datacenters," *IEEE/ACM Trans. Netw.*, vol. 28, no. 1, pp. 57–70, Feb. 2020.

[26] J. Zhao, J. Liu, H. Wang, and C. Xu, "Multipath TCP for datacenters: From energy efficiency perspective," in *Proc. IEEE INFOCOM*, May 2017, pp. 1–9.

[27] J. Wu, B. Cheng, M. Wang, and J. Chen, "Quality-aware energy optimization in wireless video communication with multipath TCP," *IEEE/ACM Trans. Netw.*, vol. 25, no. 5, pp. 2701–2718, Oct. 2017.

[28] W. Wang, X. Wang, and D. Wang, "Energy efficient congestion control for multipath TCP in heterogeneous networks," *IEEE Access*, vol. 6, pp. 2889–2898, 2018.

[29] F. Kaup, M. Wichtlhuber, S. Rado, and D. Hausheer, "Can multipath TCP save energy? A measuring and modeling study of MPTCP energy consumption," in *Proc. IEEE LCN*, Oct. 2015, pp. 442–445.

[30] Y. Cao, S. Chen, Q. Liu, Y. Zuo, H. Wang, and M. Huang, "QoE-driven energy-aware multipath content delivery approach for MPT CP-based mobile phones," *China Commun.*, vol. 14, no. 2, pp. 90–103, Feb. 2017.

[31] C. Xu, P. Wang, C. Xiong, X. Wei, and G.-M. Muntean, "Pipeline network coding-based multipath data transfer in heterogeneous wireless networks," *IEEE Trans. Broadcast.*, vol. 63, no. 2, pp. 376–390, Jun. 2017.

[32] Y. Cui, L. Wang, X. Wang, H. Wang, and Y. Wang, "FMTCP: A fountain code-based multipath transmission control protocol," *IEEE/ACM Trans. Netw.*, vol. 23, no. 2, pp. 465–478, Apr. 2015.

[33] K. Xue, J. Han, H. Zhang, K. Chen, and P. Hong, "Migrating unfairness among subflows in MPTCP with network coding for Wired–Wireless networks," *IEEE Trans. Veh. Technol.*, vol. 66, no. 1, pp. 798–809, Jan. 2017.

[34] Y.-S. Lim, Y.-C. Chen, E. M. Nahum, D. Towsley, and K.-W. Lee, "Cross-layer path management in multi-path transport protocol for mobile devices," in *Proc. IEEE INFOCOM*, Apr. 2014, pp. 1815–1823.

[35] M. Fukuyama, N. Yamai, S. Ohzahata, and N. Kitagawa, "Throughput improvement of MPTCP by selective bicasting with cross-layer control in wireless environment," in *Proc. IEEE COMPSAC*, Jul. 2018, pp. 204–209.

[36] Y. Cao, D. Yu, L. Zeng, Q. Liu, F. Wu, X. Gui, and M. Huang, "Towards efficient parallel multipathing: A receiver-centric cross-layer solution to aid multipath TCP," in *Proc. IEEE ICPADS*, Dec. 2019, pp. 1–8.

[37] C. Xu, H. Huang, H. Zhang, C. Xiong, and L. Zhu, *Multipath Transmission Control Protocol (MPTCP) Partial Reliability Extension*, document draft-xu-mptcp-prmp-04, IETF, 2017. [Online]. Available: https://tools.ietf.org/html/draft-xu-mptcp-prmp-04

[38] J. Qin, C. Xu, H. Huang, L. Zhong, and G.-M. Muntean, "MO-PR: Message-oriented partial-reliability MPTCP for real-time multimedia transmission in wireless networks," in *Proc. IEEE IWCMC*, Jun. 2018, pp. 36–41.

[39] C. Diop, G. Dugué, C. Chassot, and E. Exposito, "QoS-oriented MPTCP extensions for multimedia multi-homed systems," in *Proc. IEEE AINA*, Mar. 2012, pp. 1119–1124.

[40] G. Noh, H. Park, H. Roh, and W. Lee, "Secure and lightweight subflow establishment of multipath-TCP," *IEEE Access*, vol. 7, pp. 177438–177448, 2019.

[41] M. Jadin, G. Tihon, O. Pereira, and O. Bonaventure, "Securing multipath TCP: Design & implementation," in *Proc. IEEE INFOCOM*, May 2017, pp. 1–9.

[42] H. Nguyen, C. Phung, S. Secci, B. Felix, and M. Nogueira, "Can MPTCP secure Internet communications from man-in-the-middle attacks?" in *Proc. 13th Int. Conf. Netw. Service Manage.*, Nov. 2017, pp. 1–7.

[43] A. Munir, Z. Qian, Z. Shafiq, A. Liu, and F. Le, "Multipath TCP traffic diversion attacks and countermeasures," in *Proc. IEEE ICNP*, Oct. 2017, pp. 1–10.

[44] M. A. Rahman and H. Mohsenian-Rad, "False data injection attacks with incomplete information against smart power grids," in *Proc. IEEE GLOBECOM*, Dec. 2012, pp. 1–6.

[45] W. Bi, C. Chen, and K. Zhang, "Optimal strategy of attack-defense interaction over load frequency control considering incomplete information," *IEEE Access*, vol. 7, pp. 75342–75349, 2019.

[46] S.-Y. Tan, J. Wu, L. Lü, M.-J. Li, and X. Lu, "Efficient network disintegration under incomplete information: The comic effect of link prediction," *Sci. Rep.*, vol. 6, no. 1, p. 22916, Mar. 2016.

[47] C. Zhang, M. Zhang, Y. Wang, and S. Wu, "Method to analyse the robustness of aviation communication network based on complex networks," *Syst. Eng. Electron.*, vol. 37, no. 1, pp. 180–184, 2015.

[48] Y. Li and Y. Wang, "False data injection attacks with incomplete network topology information in smart grid," *IEEE Access*, vol. 7, pp. 3656–3664, 2019.

[49] P. Holme, "Efficient local strategies for vaccination and network attack," *Europhys. Lett.*, vol. 68, no. 6, pp. 908–914, Dec. 2004.

[50] S. Mascolo, C. Casetti, M. Gerla, Y. Sanadidi, and R. Wang, "TCP westwood: Bandwidth estimation for enhanced transport over wireless links," in *Proc. ACM SIGMOBILE*, 2001, pp. 287–297.

[51] *USC/ISI and Xerox Parc, NS-2 Documentation and Software, Version 2.35.*, UC Berkeley, Berkeley, CA, USA, LBL.

[52] Google Code Project. *Multipath-TCP: Implement multipath TCP NS-2*. Accessed: Apr. 2020. [Online]. Available: http://code.google.com/p/multipath-tcp/

[53] Check Point Research. *Cyber Attack Trends Analysis Report*. Accessed: Apr. 2020. [Online]. Available: http://snt.hr/boxcontent/CheckPointSecurityReport2019_vol01.pdf

[54] Z.-Y. Ai, Y.-T. Zhou, and F. Song, "A smart collaborative routing protocol for reliable data diffusion in IoT scenarios," *Sensors*, vol. 18, no. 6, p. 1926, Jun. 2018.

[55] C. Xu, T. Liu, J. Guan, H. Zhang, and G.-M. Muntean, "CMT-QA: Quality-aware adaptive concurrent multipath data transfer in heterogeneous wireless networks," *IEEE Trans. Mobile Comput.*, vol. 12, no. 11, pp. 2193–2205, Nov. 2013.

[56] Wikipedia. *Cyberattack*. Accessed: Jun. 2020. [Online]. Available: https://en.wikipedia.org/wiki/Cyberattack

[57] S. J. K. I. Kim Park Lee You and K. Yim, "A brief survey on rootkit techniques in malicious codes," *J. Internet Services Inf. Secur.*, vol. 2, nos. 3–4, pp. 134–147, 2012.

[58] A. Abhishta, W. Heeswijk, M. Junger, L. Nieuwenhuis, and R. Joosten, "Why would we get attacked? An analysis of attacker's aims behind DDoS attacks," *J. Wireless Mobile Netw., Ubiquitous Comput., Dependable Appl.*, vol. 11, no. 2, pp. 3–22, 2020.

[59] H. Kim, "5G core network security issues and attack classification from network protocol perspective," *J. Internet Services Inf. Secur.*, vol. 10, no. 2, pp. 1–15, 2020.

[60] V. Sharma, I. You, F.-Y. Leu, and M. Atiquzzaman, "Secure and efficient protocol for fast handover in 5G mobile xhaul networks," *J. Netw. Comput. Appl.*, vol. 102, pp. 38–57, Jan. 2018.

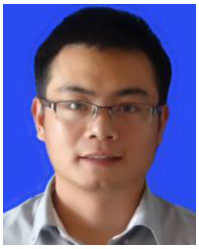
[61] F. Song, M. Zhu, Y. Zhou, I. You, and H. Zhang, "Smart collaborative tracking for ubiquitous power IoT in edge-cloud interplay domain," *IEEE Internet Things J.*, vol. 7, no. 7, pp. 6046–6055, Jul. 2020.

[62] Z. Ai, Y. Liu, L. Chang, F. Lin, and F. Song, "A smart collaborative authentication framework for multi-dimensional fine-grained control," *IEEE Access*, vol. 8, pp. 8101–8113, 2020.

[63] F. Song, Y.-T. Zhou, L. Chang, and H.-K. Zhang, "Modeling space-terrestrial integrated networks with smart collaborative theory," *IEEE Netw.*, vol. 33, no. 1, pp. 51–57, Jan. 2019.

YUANLONG CAO received the B.S. degree in computer science and technology from Nanchang University, China, in 2006, the M.S. degree in software engineering from the Beijing University of Posts and Telecommunications (BUPT), in 2008, and the Ph.D. degree from the Institute of Network Technology, BUPT, in 2014. He was an Intern/Software Engineer with BEA TTC, IBM CDL, and DT Research, Beijing, from 2007 to 2011. He is currently an Associate Professor with the School of Software, Jiangxi Normal University, China. His research interests include multimedia communications and next-generation internet technology. He served as a Technical Reviewer for several journals, including the IEEE Transactions on Industrial Informatics, the IEEE Transactions on Cognitive Communications and Networking, IEEE Access, *Computer Communications*, and *Journal of Network and Computer Applications*.

JING CHEN received the B.S. degree in electronic commerce from the Hubei University of Economics, China, in 2018. She is currently pursuing the M.S. degree in management science and engineering with Jiangxi Normal University under the supervision of Dr. Y. Cao. Her research interests include multimedia networking, internet technology, information management, and information systems.



QINGHUA LIU received the B.S. degree in software engineering and the master's degree in management science and engineering from Jiangxi Normal University (JXNU), China, in 2007 and 2011, respectively. He is currently an Associate Professor with the Software of School, JXNU. His research interests include multimedia networking and next generation internet technology.

GANG LEI is currently an Associate Professor with the School of Software, Jiangxi Normal University, China, where he is also an Associate Director of the Academic Committee. His research interests include internet technology, information management, and information systems.

HAO WANG is currently a Professor with the School of Software, Jiangxi Normal University, China. His major research interests include computer network congestion control and computer network management. He was elected as a University Young and Middle-Aged Academic Leader and a Distinguished Teacher.

ILSUN YOU (Senior Member, IEEE) received the M.S. and Ph.D. degrees in computer science from Dankook University, Seoul, South Korea, in 1997 and 2002, respectively, and the Ph.D. degree from Kyushu University, Japan, in 2012. From 1997 to 2004, he was with Thin Multimedia Inc., Internet Security Company Ltd., and Hanjo Engineering Company Ltd., as a Research Engineer. He is currently a Full Professor with the Department of Information Security Engineering, Soonchunhyang University. He is a Main Organizer of the international conferences and workshops, such as MIST, MobiWorld, MobiSec, and so on. He has published more than 180 articles in these areas. His research interests include 5G/6G security, security for wireless networks and mobile internet, the IoT security, and so on. He is a Fellow of IET. He serves as the EiC for *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA)*. He also serves on the Editorial Board of *Information Sciences (INS)*, *Journal of Network and Computer Applications (JNCA)*, IEEE Access, *Intelligent Automation and Soft Computing (AutoSoft)*, the *International Journal of Ad Hoc and Ubiquitous Computing (IJAHUC)*, *Computing and Informatics (CAI)*, and *Journal of High Speed Networks (JHSN)*.