217080

บิตทอร์เรนต์เป็นโพรโทคอลสำหรับแลกเปลี่ยนไฟล์แบบเพียร์ทูเพียร์ที่กำลังได้รับความนิยมอย่างมากในปัจจุบัน ส่งผลให้มีกระแสข้อมูลบิตทอร์เรนต์อยู่ในระบบเครือข่ายค่อนข้างมาก ซึ่งอาจส่งผลกระทบกับการใช้งานแอพลิเคชันอื่นบนระบบเครือข่าย การจะควบคุมการใช้งานบิตทอร์เรนต์ได้จำเป็นต้องมีวิธีการระบุเพียร์ที่มีประสิทธิภาพ ในงานวิจัยนี้นำเสนอการระบุเพียร์ของบิตทอร์เรนต์โดยอาศัยพฤติกรรมของกระแสข้อมูลที่เกิดจากขั้นตอนวิธีการเค้น ซึ่งเป็นขั้นตอนวิธีหลักในการควบคุมการแลกเปลี่ยนข้อมูลระหว่างเพียร์ ทำให้สามารถระบุหาเพียร์ได้แม้ว่าเพียร์จะมีการปรับเปลี่ยนรูปแบบการเชื่อมต่อในระดับโฟลเป็นแบบใดก็ตาม และในขั้นตอนการตรวจสอบได้ใช้ข้อมูลจากส่วนหัวของแพ็กเก็ตถึงระดับชั้นเครือข่าย จึงสามารถตรวจหาเพียร์ที่ทำการเข้ารหัสกระแสข้อมูลได้ มีสถานะที่ต้องจำขณะทำงานน้อยกว่างานวิจัยที่ผ่านมาที่ทำการตรวจสอบในระดับโฟล และไม่มีผลกระทบจากการเปลี่ยนแปลงในระดับชั้นขนส่ง จากผลการทดลองกับชุดข้อมูลควบคุมและชุดข้อมูลปกติพบว่า วิธีการที่นำเสนอสามารถตรวจจับเพียร์ที่มีการรับส่งข้อมูลจำนวนมากได้เป็นอย่างดี และยังสามารถตรวจจับได้อย่างรวดเร็ว ซึ่งจะช่วยให้สามารถควบคุมเพียร์ได้ก่อนที่เพียร์จะส่งข้อมูลได้เป็นจำนวนมาก นอกจากนี้ยังมีอัตราการตรวจจับผิดพลาดน้อย ทำให้ไม่เกิดผลกระทบกับการใช้งานแอพลิเคชันทั่วไป

217080

Bittorrent is currently one of the most popular peer-to-peer file sharing protocols. However, it incurs such excessive amount of traffic that it may adversely affect the performance of legacy internet applications. To limit this adverse impact, an efficient methodology for bittorrent identification may be needed. This work proposes a novel approach to identify bittorrent peers based on behaviors of the choke algorithm (the main algorithm used for controlling data exchanges among bittorrent peers) instead of using the transport-layer information. Therefore, this work can identify even the peers that attempt to avoid being detected by altering their flow connection at the transport layer. Given that this work relies on only the network-layer information, our approach is capable of achieving robustness to changes in the transport layer, maintaining fewer states, and identifying peers that encrypt their traffic. The experimental results on the controlled traffic and normal traffic indicate that this approach can efficiently and quickly identify most of excessive bandwidth-consuming peers. Hence, it is possible to manage, stop, or control bittorrent peers before they can transfer a large amount of data. Furthermore, with our low false-positive rate, the approach will rarely misidentify peers and will unlikely worsen the performance of legacy internet applications if not improving it.