3.1. Statistical methods 9 h58 Statistical properties of normal and attack patterns can be exploited for detection of DDoS attacks. Generally a statistical model for normal traffic is fitt^^lcPihen a statistical infdrt!Mci^%&st is applied to d^@fitygfy|e if a new instance, ^elor®?j|g this model. Instances that do not the legxnt^m^	3.1 Các phương pháp thống kê Tính chất thống kê của các mô hình bình thường và mô hình tấn công (kiểu tấn công) có thể được khai thác để phát hiện các cuộc tấn công DDoS. Nói chung, mô hình thống kê đối với lưu lượng mạng thông thường được khớp và sau đó chúng ta áp dụng phép suy luận thống kê để xác định xem

based on the applied test statistics, are classified as anomalies. Chen et al. [19] develop a distributed change point (DCP) detection architecture using change aggregation trees (CATs). The non-p^M18tPfc approach was adafrtftdi Igh I describe the distribution of pre-change or post-change network traffic. When a DDoS flooding attack is being lauMifiM^^he cumuleJtf^fe' deviation is noticeably higher than random fluctuations. The CAT mechanism is designed to work at the router level to detect abrupt changes in traffic flows. The domain server uses the traffic change patterns detected at attack-transit routers to construct the CATs, which represent the attack flow pattern. A very well-known DDoS defense scheme called D-WARD is presented in [20]. D-WARD identifies an attack based on continuous monitoring of bidirectional traffic flows between the network and the rest of the Internet and by periodic deviation analysis with the normal flow patterns. Mismatched flows are rate limited in proportion to their aggressiveness. D- WARD not only offers a good detection rate but also reduces DDoS attack traffic significantly. It uses a predefined model for normal traffic to detect anomalies	trường hợp mới này có thuộc mô hình này hay không. Chen và các cộng sự [19] đã xây dựng kiến trúc phát hiện điểm thay đổi phân tán (DCP) dùng các cây thay đổi kết tập (các CAT). Phương pháp phi tham số được hiệu chỉnh để mô tả lưu lượng mạng trước và sau khi thay đổi. Khi một cuộc tấn công gây tắt nghẽn DdoS (tấn công từ chối dịch vụ) bắt đầu, độ lệch tích lũy cao hơn rất nhiều so với những dao động ngẫu nhiên. Cơ chế CAT được thiết kế để làm việc ở mức bộ định tuyến để phát hiện những thay đổi đột ngột trong lưu lượng mạng. Máy chủ tên miền sự dụng các kiểu thay đổi lưu lượng mạng được phát hiện ở các bộ định tuyến tấn công-chuyển tiếp để xây dựng các CAT, CAT biểu diễn kiểu lưu lượng mạng tấn công. Cơ chế bảo vệ phổ biến DdoS có tên là D-WARD được trình bày trong tài liệu tham khảo [20]. D-WARD xác định một cuộc tấn công dựa trên việc giám sát liên tục lưu lượng mạng hai chiều giữa mạng và phần còn lại của Internet và thông qua phân tích độ lệch tuần hoàn so với các kiểu lưu lượng mạng thông thường. Các lưu lượng mạng bất thường sẽ bị giới hạn tốc độ tùy thuộc vào mức độ mạng yếu của chúng. D-WARD không chỉ có tỷ lệ phát hiện cao mà còn giảm đáng kể lưu lượng mạng tấn công DdoS. Nó dùng mô hình định trước về lưu lượng mạng thông

	thường để phát hiện các bất thường.
FIGURE 9. Classification of DDoS attack detection methods	HÌNH 9. Phân loại các phương pháp phát hiện tấn công DdoS
in the two-way traffic statistics for each peer. If it identifies a DDoS attack, it imposes a rate limit on the suspicious outgoing flow for the peer. Next, D-WARD observes the traffic for either confirmation of the attack or refutation. If confirmed, D-WARD further controls the rate limit. However, if refuted, it gradually allows increased traffic rate. Saifullah [21] proposes a defense mechanism based on a distributed algorithm that performs weight-fair throttling at upstream routers. The throttling is weight-fair because the traffic destined for the server is controlled (increased or decreased) by leaky buckets at the routers based on the number of users connected, directly or through other routers, to each router. In the beginning of the algorithm, the survival capacity is underestimated by the routers so as to protect the server from any sudden initial attack. The rate is updated (increased or decreased), based on the server's feedback sent to its child routers and eventually propagated downward to all routers, in the subsequent rounds of the algorithm with a view to converging the total server load to the tolerable capacity range.	trong thống kê lưu lượng hai đường cho mỗi peer (bạn cùng cấp, người dùng cùng cấp). Nếu nó xác định được một cuộc tấn công DdoS, nó sẽ áp đặt giới hạn tốc độ trên lưu lượng ra đáng ngờ của peer. Tiếp theo, D-WARD quan sát lưu lượng để xác nhận tấn công hoặc bác bỏ. Nếu bác bỏ, nó cho phép tốc độ lưu lượng dần dần tăng lên. Saifullah [21] đã đưa ra một cơ chế bảo vệ dựa trên thuật toán phân tán thực hiện điều chỉnh cân bằng trọng số ở các bộ định tuyến ngược dòng. Quá trình điều chỉnh có tính cân bằng trọng số bởi vì lưu lượng danh cho máy chủ được điều khiển (tăng hoặc giảm) bằng giải thuật thùng rò tại các bộ định tuyến dự trên số lượng người dùng được kết nối, trực tiếp hoặc thông qua các bộ định tuyến khác đến mỗi bộ định tuyến. Trong phần bắt đầu của thuật toán, khả năng sống còn được đánh giá sơ bộ (thấp hơn thực tế) để bảo vệ server khỏi bất kỳ cuộc tấn công bất thình lình nào. Tốc độ được cập nhật (tăng hoặc giảm), dựa trên thông tin phản hồi của server gửi đến các bộ định tuyến con của nó và cuối cùng truyền xuống tất cả các bộ định tuyến, trong các vòng tiếp theo của thuật toán nhằm hội tụ tổng tải máy chủ thành khoảng dung lượng chấp nhận được.

Chen [22] presents a new detection method for DDoS attack traffic based on the two-sample i-test. It first obtains statistics for normal SYN arrival rate (SAR) and confirms that it follows the normal distribution. The method identifies an attack by computing (a) the difference between incoming SAR and normal SAR, and (b) the difference between the number of SYN and ACK packets. Unlike most previous DDoS defense schemes that only deal with either flooding or meek attack, the proposal uses two statistical tests to identify malicious traffic. It first compares the differences between the overall means of the incoming traffic arrival rate and the normal traffic arrival rate by the two- sample t-test If the difference is significant, it concludes that the traffic may include flooding attack packets. However, the low-rate attack traffic may pass the arrival rate test and make the backlog queue full. The approach then compares the two groups that contain different numbers of SYN and ACK packets by the two-sample t-test If there is a significant difference, it recognizes that the attack traffic is mixed into the current traffic. Zhang et aL [23] propose a prediction method for the available service rate of a protected server by applying the Auto Regressive Integrated	Chen [22] đưa ra phương pháp phát hiện lưu lượng tấn công DdoS dựa trên phép kiểm định I hai mẫu. Trước hết, nó ghi nhận số liệu thông kê tốc độ đến SYN thông thường (SAR) và xác nhận rằng nó tuân theo phân bố thông thường. Phương pháp này xác định tấn công thông qua tính toán (a) sự chênh lệch giữa SAR đến và SAR thông thường, và (b) sự chênh lệch giữa số gói tin SYN và ACK. Không giống như đa số cơ chế bảo vệ DdoS trước đây chỉ xét tấn công tắt nghẽn hoặc tấn công ôn hòa, người ta đề xuất dùng hai phép kiểm định thống kê để xác định lưu lượng nguy hiểm. Trước hết, nó so sánh độ chênh lệch giữa các trung bình tổng thể của tốc độ đến của lưu lượng mạng đến và tốc độ đến của lưu lượng bình thường thông qua kiểm định t hai mẫu. Nếu độ chênh lệch lớn, nó kết luận rằng lưu lượng có thể chưa những gói tin tấn công tắt nghẽn. Tuy nhiên, lưu lượng tấn công tốc độ thấp có thể vượt qua được phép kiểm tra tốc độ đến và làm cho xếp hàng backlog đầy. Sau đó, phương pháp này so sánh hai nhóm chứa số lượng gói tin SYN và ACK khác nhau thông qua kiểm định t hai mẫu. Nếu có sự khác biệt lớn, nó ghi nhận rằng lưu lượng tấn công đã thâm nhập vào lưu lượng hiện tại. Zhang và các cộng sự [23] đề xuất phương pháp tiên đoán tốc độ dịch vụ hiện tại của server được bảo vệ bằng

Moving Average (ARIMA) model. They use available service rates to qualify the server's availability to detect DDoS attacks. Their prediction method divides server resources into CPU time, memory utilization and networking buffer. Rased on the prediction, they use abnormal detection technology to analyze the consumption of server resources to predict whether the server is under DDoS attack.	cách áp dụng mô hình Trung Bình Trượt Kết Hợp Tự Hồi Quy (ARIMA). Họ sử dụng tốc độ dịch vụ sẵn có để đánh giá tính khả dụng của server để phát hiện các cuộc tấn công DdoS. Phương pháp phát hiện của họ chia các tài nguyên server thành thời gian CPU, khả năng sử dụng bộ nhớ và bộ đệm mạng. Căn cứ vào dự đoán, họ dùng công nghệ phát hiện bất thường để phân tích mức tiêu thụ tài nguyên server và thông qua đó dự đoán sever có đang bị tấn công DdoS hay không.
Akella et al. [24] explore key challenges in helping an ISP network detect attacks on itself or attacks on external sites which use the ISP network. They propose a detection mechanism where each router detects traffic anomalies using profiles of normal traffic constructed using stream sampling algorithms. Initial results show that it is possible to: (1) profile normal traffic reasonably accurately, (2) identify anomalies with low false positive and false negative rates (locally, at the router), and (3) be cost effective in terms of memory consumption and per packet computation. In addition, ISP routers exchange information with each other to increase confidence in their detection decisions. A router gathers responses from all other routers regarding suspicions and based	Akella và các cộng sự [24] đã nghiên cứu những thách thức quan trọng nhằm giúp một mạng ISP phát hiện những cuộc tấn công trên chính nó hoặc những cuộc tấn công ở các vị trí bên ngoài đang dùng mạng ISP. Họ đề xuất cơ chế phát hiện trong đó mỗi bộ định tuyến phát hiện những bất thường về lưu lượng mạng thông qua các profile (biên dạng, kiểu) sử dụng thuật toán lấy mẫu luồng. Các kết quả ban đầu cho thấy rằng chúng ta có thể: (1) profile (biên dạng) lưu lượng mạng thông thường có độ chính xác vừa phải, (2) xác định những bất thường với tỷ lệ dương tính và âm tính thấp (cực bộ, tại bộ định tuyến) và (3) tính hiệu quả về giá thành xét theo mức độ tiêu thụ bộ nhớ và theo mức độ tính toán trên gói tin. Thêm vào đó, các bộ định tuyến ISP trao đổi thông tin với nhau để tăng độ

on them decides whether a traffic aggregate is an attack or is normal. The initial results show that individual router profiles capture key characteristics of the traffic effectively and identify anomalies with low false positive and false negative rates. Peng et al. [25] describe a novel approach to detect bandwidth attacks by monitoring the arrival rate of new source IP addresses. The detection scheme is based on an advanced non-parametric change detection scheme, CUSUM.	tin cậy trong các quyết định phát hiện. Một bộ định tuyến thu thập các đáp ứng từ tất cả các bộ định tuyến khác về những nghi ngờ và dựa trên đó quyết định xem tập hợp lưu lượng là một cuộc tấn công hay bình thường. Kết quả ban đầu cho thấy rằng từng profile định tuyến riêng biệt ghi nhận các đặc trưng quan trọng của lưu lượng mạng một cách có hiệu quả và xác định những bất thường với tỷ lệ dương tính và âm tính giả thấp. Peng và các cộng sự [25] mô tổ một phương pháp mới để phát hiện các cuộc tấn công băng thông qua giám sát tốc độ đến của các địa chỉ IP của nguồn mới. Phương pháp phát hiện này dựa trên phương pháp phát hiện thay đổi phi tham số nâng cao, CUSUM.
Cheng et al. [26] propose the IP Flow Feature Value (FFV) algorithm based on the essential features of DDoS attacks, such as abrupt traffic change, flow dissymmetry, distributed source IP addresses and concentrated target IP addresses. Using a Unear prediction technique, a simple and efficient ARM A prediction model is established for normal network flow. Then a DDoS attack detection scheme based on anomaly detection techniques and linear prediction model (DDAP) is used. Udhayan and Hamsapriya [27] present a Statistical Segregation Method (SSM), which samples the flow in consecutive intervals	Cheng và các cộng sự [26] đề xuất giá trị đặc trưng lưu lượng IP (FFV) dựa trên các đặc trưng cở bản của các cuộc tấn công DdoS, chẳng hạn như những thay đổi lưu lượng mạng đột xuất, sự bất đối xứng lưu lượng mạng, các địa chỉ IP nguồn phân tán và các địa chỉ IP mục tiêu tập trung. Dùng kỹ thuật tiên đoán Unear, các nhà nghiên cứu đã xây dựng được một mô hình tiên đoán ARM hiệu quả cho lưu lượng mạng thông thường. Sau đó dùng phương pháp phát hiện tấn công DdoS dựa trên các kỹ thuật phát hiện bất thường và mô hình phát hiện tuyến tính (DDAP). Udhayan và

and compares the samples against the attack state condition and sorts them with the mean as the parameter. Then correlation analysis is performed to segregate attack flows from legitimate flows. The authors compare SSM against various other methods and identify a blend of segregation methods for alleviating false detections.	Hamsapriya [27] đưa ra phương pháp chia tách thống kê (SSM), phương pháp này lấy mẫu các luồng trong những khoảng thời gian liên tiếp và so sánh các mẫu theo điều kiện trạng thái tấn công và phân loại chúng thông qua mean (giá trị trung bình) như một tham số. Sau đó, phân tích tương quan được tiến hành để tách các luồng tấn công ra khỏi các luồng hợp pháp. Các tác giả so sánh SSM theo các phương pháp khác nhau và xác định sự pha trộn giữa các phương pháp phân tích để làm giảm các phát hiện không chính xác.
In [28], the authors introduce a generic DoS detection scheme based on maximum likelihood criterion with random neural networks (RNN). The method initially selects a set of traffic features in offline mode to obtain pdf estimates and to evaluate the likelihood ratios. During decision making, it measures the features of incoming traffic and attempts to decide according to each feature. Finally, it obtains an overall decision using both feed-forward and recurrent architectures of the RNN. A brief summary of these methods is given in Table 1	Trong [28], các tác giả đã đưa vào một chương trình phát hiện tấn công từ chối dịch vụ tổng quát dựa trên tiêu chuẩn khả năng cực đại với các mạng nơ-ron ngẫu nhiên (RNN). Ban đầu, phương pháo chọn một tập hợp các đặc trưng lưu lượng trong chế độ offline để thu được các ước lượng pdf và đánh giá tỷ số khả năng (tỷ số khả dĩ). Trong suốt quá trình thực hiện quyết định, nó đo các đặc trưng của lưu lượng đến và cố gắng quyết định theo mỗi đặc trưng. Cuối cùng, nó thu được quyết định tổng thể dùng các kến trúc truyền thẳng và các kiến trúc hồi quy của RNN. Bảng 1 tóm tắt những phương pháp này.