



US 20230231873A1

(19) **United States**(12) **Patent Application Publication**  
**St. Pierre**(10) **Pub. No.: US 2023/0231873 A1**(43) **Pub. Date: Jul. 20, 2023**(54) **SLOWING REQUESTS FROM MALICIOUS NETWORK CLIENTS**(71) Applicant: **Arbor Networks, Inc.**, Westford, MA (US)(72) Inventor: **Brian St. Pierre**, Acworth, NH (US)(73) Assignee: **Arbor Networks, Inc.**, Westford, MA (US)(21) Appl. No.: **17/807,627**(22) Filed: **Jun. 17, 2022****Related U.S. Application Data**

(60) Provisional application No. 63/300,884, filed on Jan. 19, 2022.

**Publication Classification**(51) **Int. Cl.**  
**H04L 9/40** (2006.01)  
**H04L 67/145** (2006.01)  
**H04L 61/4511** (2006.01)(52) **U.S. Cl.**CPC ..... **H04L 63/1458** (2013.01); **H04L 63/1416** (2013.01); **H04L 63/1425** (2013.01); **H04L 67/145** (2013.01); **H04L 61/4511** (2022.05)

(57)

**ABSTRACT**

A method and network are provided for monitoring a network during a DDoS attack. The method includes establishing a flow record for flows designated for tarpitting and a state machine, each state of multiple states of the state machine having an associated handler function. The handler function associated with a current state of a state machine associated with a flow is invoked to perform one or more actions associated with the flow or the flow record for applying at least one tarpitting technique of one or more candidate tarpitting techniques associated with the flow record, and return a next state, which is used to update the current state of the state machine. The handler function associated with the current state of the state machine is repeatedly invoked, wherein each invocation of the handler function potentially applies different tarpitting techniques.

