US010142426B2

(12) **United States Patent**
Zlatokrilov

(10) **Patent No.: US 10,142,426 B2**
(45) **Date of Patent: Nov. 27, 2018**

(54) **SYSTEM AND METHOD FOR IDENTIFYING COMMUNICATION SESSION PARTICIPANTS BASED ON TRAFFIC PATTERNS**

(71) Applicant: **VERINT SYSTEMS LTD.**, Herzliya Pituach (IL)

(72) Inventor: **Haim Zlatokrilov**, Tel Aviv (IL)

(73) Assignee: **VERINT SYSTEMS LTD.**, Herzliya, Pituach (IL)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 261 days.

(21) Appl. No.: **15/084,408**

(22) Filed: **Mar. 29, 2016**

(65) **Prior Publication Data**

US 2016/0285978 A1 Sep. 29, 2016

(30) **Foreign Application Priority Data**

Mar. 29, 2015 (IL) 238001

(51) **Int. Cl.**
H04L 29/08 (2006.01)
H04L 12/851 (2013.01)
H04L 12/859 (2013.01)

(52) **U.S. Cl.**
CPC ***H04L 67/146*** (2013.01); ***H04L 47/2475*** (2013.01); ***H04L 47/2483*** (2013.01)

(58) **Field of Classification Search**
CPC H04L 47/2475; H04L 47/2483; H04L 67/146
USPC 709/224
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,689,442 A 11/1997 Swanson et al.
6,404,857 B1 6/2002 Blair et al.
6,718,023 B1 4/2004 Zolotov
6,741,992 B1 5/2004 McFadden
(Continued)

FOREIGN PATENT DOCUMENTS

WO 2012/075347 6/2012

OTHER PUBLICATIONS

Aho, Alfred V., et al., "Efficient String Matching: An Aid to Bibliographic Search," Communication of the ACM, Jun. 1975, vol. 18, No. 6, pp. 333-340.
(Continued)

Primary Examiner — Michael C Lai
(74) *Attorney, Agent, or Firm* — Meunier Carlin & Curfman

(57) **ABSTRACT**

A monitoring system monitors traffic flows that are exchanged over a communication network. The system characterizes the flows in terms of their temporal traffic features, and uses this characterization to identify communication devices that participate in the same communication session. By identifying the communication devices that serve as endpoints in the same session, the system establishes correlations between the users of these communication devices. The monitoring system characterizes the flows using traffic features such as flow start time, flow end time, inter-burst time and burst size, and/or statistical properties of such features. The system typically generates compressed-form representations ("signatures") for the traffic flows based on the temporal traffic features, and finds matching flows by finding similarities between signatures.

16 Claims, 2 Drawing Sheets