US 20230232230A1

(19) **United States**

(12) **Patent Application Publication** (10) **Pub. No.: US 2023/0232230 A1**

Grutzmacher et al. (43) **Pub. Date: Jul. 20, 2023**

(54) **ZERO TRUST WIRELESS MONITORING - SYSTEM AND METHOD FOR BEHAVIOR BASED MONITORING OF RADIO FREQUENCY ENVIRONMENTS**

(71) Applicant: **802 Secure, Inc.**, Pleasanton, CA (US)

(72) Inventors: **Konrad Grutzmacher**, Berkeley, CA (US); **Clifford Fernandez**, Huntington Beach, CA (US)

(21) Appl. No.: **18/180,055**

(22) Filed: **Mar. 7, 2023**

Related U.S. Application Data

(63) Continuation of application No. 17/961,215, filed on Oct. 6, 2022, which is a continuation of application No. 16/365,393, filed on Mar. 26, 2019, now Pat. No. 11,540,130.

(60) Provisional application No. 62/800,927, filed on Feb. 4, 2019.

Publication Classification

(51) **Int. Cl.**

H04W 12/08	(2021.01)
H04W 12/122	(2021.01)
H04L 9/40	(2022.01)
H04W 24/08	(2009.01)

(52) **U.S. Cl.**

CPC ***H04W 12/08*** (2013.01); ***H04W 12/122*** (2021.01); ***H04L 63/1425*** (2013.01); ***H04W 24/08*** (2013.01)

(57) **ABSTRACT**

A System and Method is provided that enable identifying cyber security attacks using observation and monitoring of end point activity. By following and monitoring the wireless connection related activities of endpoint devices as they cycle through various steps leading to establishing a connection to the secure network, a knowledge base is established in the cloud by analysis of the actions, and communication to build the confidence that the users of the network are where they should be. In one embodiment, no access is provided until a user presents valid credentials. Based on these credentials the network then builds a specific path based on access controls, tunnels or other techniques to control the user's communication and access to specific targets within the network.