



US 20240214375A1

(19) **United States**

(12) **Patent Application Publication**
Wyseur

(10) **Pub. No.: US 2024/0214375 A1**

(43) **Pub. Date: Jun. 27, 2024**

(54) **SENDING AND RECEIVING MESSAGES**

Publication Classification

(71) Applicant: **NAGRAVISION SARL**,
CHESEAUX-SUR-LAUSANNE (CH)

(51) **Int. Cl.**
H04L 9/40 (2006.01)
H04L 9/32 (2006.01)

(72) Inventor: **Brecht Wyseur**,
CHESEAUX-SUR-LAUSANNE (CH)

(52) **U.S. Cl.**
CPC **H04L 63/083** (2013.01); **H04L 9/3242**
(2013.01); **H04L 2209/043** (2013.01)

(73) Assignee: **NAGRAVISION SARL**,
CHESEAUX-SUR-LAUSANNE (CH)

(57) **ABSTRACT**

(21) Appl. No.: **18/438,741**

The present disclosure relates to the exchange of information between a message sending device and a message receiving device with message authentication and proposes to reduce the time required for message authentication by pre-computing a message tag, such as a MAC, and subsequently replacing the computation of the MAC when the tag is to be validated (or indeed also on sending) by a table look-up. The approach requires a set of messages and works particularly well for small sets of messages, for example as small as two or three messages, or less than five or ten messages. The approach finds particular application in control networks where control decisions have to be taken quickly and securely, for example in the control of a vehicle, for example an autonomous vehicle, or the control of a smart electricity grid.

(22) Filed: **Feb. 12, 2024**

Related U.S. Application Data

(63) Continuation of application No. 17/270,556, filed on Feb. 23, 2021, now Pat. No. 11,936,643, filed as application No. PCT/EP2019/071784 on Aug. 14, 2019.

Foreign Application Priority Data

(30) Aug. 24, 2018 (EP) 18190859.1

