



(51) International Patent Classification:
H04L 29/06 (2006.01) *H04W 12/12* (2009.01)

(21) International Application Number:
PCT/MY2014/000134

(22) International Filing Date:
29 May 2014 (29.05.2014)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
PI201313702273 27 November 2013 (27.11.2013) MY

(71) Applicant: MIMOS BERHAD [MY/MY]; Technology
Park Malaysia, 57000 Kuala Lumpur (MY).

(72) Inventors: ABDULLAH, Mohd Ariff; c/o MIMOS Ber-
had, Technology Park Malaysia, 57000 Kuala Lumpur
(MY). MOHD EZANI, Muhammad Faheem; c/o MI-
MOS Berhad, Technology Park Malaysia, 57000 Kuala
Lumpur (MY). HASEEB, Shariq; c/o MIMOS Berhad,
Technology Park Malaysia, 57000 Kuala Lumpur (MY).

(74) Agent: TAY, Wee Chao; c/o Author IP, No. 2-3, Taman
Arosa, Jalan Haji Jaib, 84000 Muar, Johor (MY).

(81) Designated States (*unless otherwise indicated, for every
kind of national protection available*): AE, AG, AL, AM,
AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY,
BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM,
DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT,
HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR,
KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME,
MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ,
OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA,
SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM,
TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM,
ZW.

(84) Designated States (*unless otherwise indicated, for every
kind of regional protection available*): ARIPO (BW, GH,
GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ,
UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ,
TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK,
EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV,
MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM,

[Continued on next page]

(54) Title: METHOD FOR COORDINATING MULTIPLE ATTACKING DEVICES IN A WIRELESS COMMUNICATION NET-
WORK

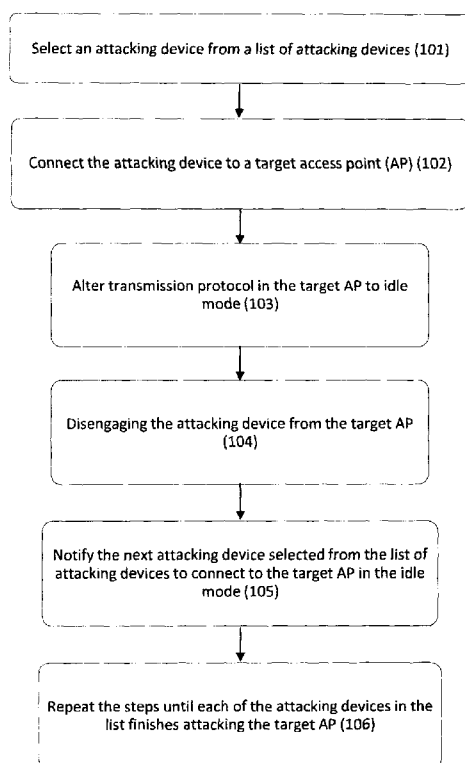


Figure 1

(57) Abstract: The present invention relates to a method for coordinating mul-
tiple attacking devices in a wireless communication network to attack a target ac-
cess point (AP), one at a time without jamming any frequency. The method is
characterized by the steps of: selecting an attacking device from a list of attack-
ing devices (101); connecting the attacking device to the target AP (102); alter-
ing transmission protocol in the target AP to idle mode (103), thereafter disenga-
ging the attacking device from the target AP (104); notifying the next attacking
device selected from the list of attacking devices to connect to the target AP
while the target AP is still in the idle mode (105), and repeating the steps until
each of the attacking devices in the list has its turn attacking the target AP (106).



TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

— *of inventorship (Rule 4.17(iv))*

Declarations under Rule 4.17:

Published:

- *as to the identity of the inventor (Rule 4.17(i))*
- *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))*

— *with international search report (Art. 21(3))*

METHOD FOR COORDINATING MULTIPLE ATTACKING DEVICES IN A WIRELESS COMMUNICATION NETWORK

5 TECHNICAL FIELD OF THE INVENTION

This invention relates to a method for coordinating multiple attacking devices in wireless communication networks.

10 BACKGROUND OF THE INVENTION

Denial-of-service (DoS) attack is a type of attack on a network preventing legitimate users of a service from using that service. The methods of DoS attack include attempts to flood a network thereby preventing legitimate network traffic, attempts to disrupt connections between two machines thereby preventing
15 access to a service, attempts to prevent a particular individual from accessing a service, and attempts to disrupt services to a specific system or person.

Most often, DoS attack is viewed as an attempt to hack information. However, not all hackings are for bad motives. DoS attack may also be used for a purpose
20 of gaining access to information to take down for example pedophile darknets, drug cartels, exposing corporate greed, and uncovering all manner of criminals. Some organizations use DoS attack to check on the vulnerability of their security protocol before implementing preventive measures.

25 In current DoS attack on wireless communication network, the techniques usually involve jamming target device with multiple requests or jamming target frequency with signals. Both of the techniques require a dedicated radio frequency in order for them to be executed. However, recently most of the user's device comes with single radio frequency interface; thus, a more favorable
30 technique is sought instead of using currently available DoS techniques.

There are two suggested options to maintain access while performing attacks to a target device, which are by using multiple devices or using a device designated with multiple radio frequency interfaces.

- 5 Patent registration no. EP 1 433 291 B1 disclosed a method for multi-hop packet transmissions in a wireless network. The disclosed prior art is related to hopping data from device to device before the data reaches its targeted destination, but it is unable to manage a situation if there are multiple devices wanting to access data from one target device.

10

Patent publication no. US 2013/0023201 A1 disclosed a method for radio frequency hopping communications jamming system. By using this method, it may cause an increase in cost and power consumption.

- 15 Patent registration no. EP1 648 115 B1 disclosed a method for improving handover procedure between two WLAN cells based on standard wireless network protocol and working at two different frequencies. Herein, only two WLAN cells are involved, thus may not be able to manage a situation when more than two WLAN cells are involved.

20

All of the above cited documents, when applied, may cause unnecessary jamming to the frequency and thereafter may take longer time for single or multiple devices to gain access to the target device.

- 25 Accordingly, it can be seen in the prior art that there exists a need to provide a method for coordinating multiple attacking devices on wireless communication networks without jamming any frequency.

30 **SUMMARY OF THE INVENTION**

The present invention provides a method for coordinating multiple attacking devices in a wireless communication network to prevent legitimate users from using services of a particular target access point. The method is implemented

without jamming any frequency. In general, the method works by allowing each of the attacking devices to attack the target access point one at a time. The method comprises the steps of: selecting an attacking device from a list of attacking devices; connecting the attacking device to the target access point; 5 altering transmission protocol in the target access point to idle mode, thereafter disengaging the attacking device from the target access point; notifying the next attacking device in the list of attacking devices to connect to the target access point in the idle mode; and repeating the steps until each of the attacking devices in the list has its turn attacking the target access point.

10

BRIEF DESCRIPTION OF THE DRAWINGS

The features of the invention will become more apparent from the following detailed description and the appended claims when read in conjunction with the 15 accompanying drawings of the preferred embodiment of the present invention, in which:

Figure 1 is a flow chart of a method for coordinating multiple attacking devices in a wireless communication;

20

Figure 2 is a flow chart showing steps of the attacking device settings network allocation vector in access point;

Figure 3 is a flow chart showing a method for coordinating multiple attacking 25 devices via client attacking device; and

Figure 4 is a flow chart showing a method for coordinating multiple attacking devices via an attacking coordinator.

30

DETAILED DESCRIPTION OF THE INVENTION

The above mentioned and other features and objects of this invention will become more apparent and better understood by reference to the following

detailed description. It should be understood that the detailed description made known below is not intended to be exhaustive or limit the invention to the precise disclosed form as the invention may assume various alternative forms. On the contrary, the detailed description covers all the relevant modifications and alterations made to the present invention, unless the claims expressly state otherwise. The present invention will now be described with reference to figures 1 - 4.

Referring to figure 1, the present invention relates to a method for coordinating multiple attacking devices in a wireless communication network, the method characterised by the steps of: selecting an attacking device from a list of attacking devices (101); connecting the attacking device to a target access point (AP) (102); altering transmission protocol in the target AP to idle mode (103), thereafter disengaging the attacking device from the target AP (104); notifying the next attacking device selected from the list of attacking devices to connect to the target AP in the idle mode (105); and repeating the steps until each of the attacking devices in the list has its turn attacking the target AP (106). Once all the attacking devices have finished attacking the target AP, the attacking devices disconnect from the target AP and the list of the attacking device is reset (107).

In an embodiment of the present invention, the step of connecting the attacking device to the target AP (102) further comprises the step of configuring the frequency of the attacking device to be identical to the target AP. In other words, if the target AP is on a different frequency compared to the attacking device, the attacking device may configure its frequency to match the frequency of the target AP before attempting to connect to the target AP. In the case where the frequency of the attacking device is already identical to the target AP, the attacking device may continue to connect to the target AP as one of the wireless clients. Upon successfully connecting to the target AP, the attacking device stores the authentication of the frequency for next attacking devices in the list of attacking devices. The authentication of the frequency may be used by the next attacking devices to connect to the target AP without re-configuring the frequency again.

In another embodiment of the present invention, the step of altering transmission protocol in the target AP to idle mode (103) further comprises the step of setting network allocation vector (NAV) (30).

5

In figure 2, an embodiment of the present invention describes the step of the attacking device setting network allocation vector (NAV) (30) which further comprises the steps of: creating bogus request-to-send (RTS) frame with a maximum value in a two-bytes duration field (31); sending the RTS frame to the target AP (32); waiting for a clear-to-send (CTS) frame from the target AP (33),
10 thereafter forcing the target AP into idle mode (33a) throughout the duration field and initiates NAV timer (33b); and disengaging the attacking device from the target AP after receiving CTS frame (104). If the attacking device did not receive the CTS frame, the attacking device will send the RTS frame to the target AP (32)
15 and wait until CTS frame is received.

In the present method, the purpose of sending RTS frame to the target AP is not to request a timeslot for data transmission but to force the target AP into idle state. This is possible, as the attacking device sets the two bytes duration field
20 into maximum value to transmit opportunity (TXOP) in the RTS frame header. Any devices that are within the range of the attacking device will stop transmitting at that frequency to avoid collision. The duration field in the RTS header will be used to initiate NAV timer on all devices within the range of the attacking device. In a preferred embodiment, the duration field for the next
25 attacking device is equal to the duration field of the previous attacking device.

In the CTS frame header, the duration field is based on the duration field of the previous RTS frame. By responding RTS with CTS, the target AP stops transmitting any frame after NAV is initiated and starts preparing to receive the
30 frame from the attacking device. Any devices that are not within the range of the attacking device but still in the range of the target AP will stop trying to transmit at that frequency range. The restrain in transmission may continue until NAV timer expires.

In an embodiment of the present invention, the attacking device disengages from the target AP (104) after receiving the CTS frame to allow the next attacking device to connect to the target AP. During this period, the NAV timer may still be running and no other device will connect to the target AP until the NAV timer is expired.

While the NAV timer is still running, the target AP is still in idle mode waiting to receive the attacking device's frame. On the contrary, the attacking device, which has already disengaged itself from the target AP, is now free to connect to another network or perform other operations during this time. The attacking device may also use this period to serve its own clients, if the attacking device is embodied as an access point.

In the present invention, there are two possible ways of coordinating attacking devices that is by client attacking device or by using an appointed attacking coordinator. The attacking coordinator may be appointed among the attacking devices, as long as all the attacking devices are connected to the same network at the same time.

The client attacking device is referred herein as the attacking device. In a further embodiment of the present invention, and by referring to figure 3, the step of the attacking device notifying the next attacking device to connect to the target AP (105), further comprises the steps of: sharing NAV timer of the attacking device with the next attacking device (201); notifying the next attacking device on the expiration of the NAV timer (202); and connecting the next attacking device to the target AP as the NAV timer expires (203). If there are other attacking devices available in the list of the attacking devices, the steps of sharing NAV timer of the attacking device with the next attacking device (201), notifying the next attacking device on the expiration of the NAV timer (202), and connecting the next attacking device to the target AP as the NAV expires (203) continue until all the attacking devices in the list have finished attacking the target AP. If there are no other attacking devices available, the list of the attacking devices is reset (107).

In an embodiment of the present invention, the multiple attacks are coordinated through a distribution system by an attacking coordinator. By utilising distribution system, the attacking devices will not consume unnecessary bandwidth from the wireless network. In a preferred embodiment of the present invention and by referring to figure 4, the step of notifying the next attacking device to connect to the target AP (105) via attacking coordinator, further comprises the steps of: receiving NAV timer from the attacking device (301); sending the NAV timer to the next attacking device (302); and instructing the next attacking device to attack the target AP as the NAV timer expires (303). If there are other attacking devices in the list of the attacking devices, the attacking coordinator will send the NAV timer to the next attacking device (302) and instructs the next attacking device to attack the target AP as the NAV timer expires (303) until all the attacking devices in the list have finished attacking the target AP. After all the attacking devices in the list have finished attacking the target AP, the list of the attacking device is reset (107).

In another embodiment of the present invention, the attacking devices include devices having identical service set identifier (SSID) as the target AP.

20

In a preferred embodiment, the attacking devices include wireless devices, client devices, and access points.

By periodically forcing the target AP to stay in idle mode, the attacking devices cause the services of the target AP to be unavailable to its clients without having to waste much time on executing each attack. By coordinating multiple attacking devices systematically, each attacking device can further reduce the time it uses for each attack. The embodiments of the present invention may also be used for a single attack.

30

CLAIMS

- 1) A method for coordinating multiple attacking devices in a wireless communication network, the method is characterized by the steps of:
5 selecting an attacking device from a list of attacking devices (101);
connecting the attacking device to a target access point (AP) (102);
altering transmission protocol in the target AP to idle mode (103),
thereafter disengaging the attacking device from the target AP (104);
notifying the next attacking device selected from the list of attacking
10 devices to connect to the target AP in the idle mode (105); and
repeating the steps until each of the attacking devices in the list has its
turn attacking the target AP (106).
- 2) A method according to claim 1, wherein the step of connecting the
15 attacking device to the target AP (102) further comprises the step of
configuring the frequency of the attacking device to be identical to the
frequency of the target AP.
- 3) A method according to claim 1, wherein the step of altering transmission
20 protocol in the target AP to idle mode (103) further comprises the step of
setting network allocation vector (NAV) (30).
- 4) A method according to claim 3, wherein the step of setting network
allocation vector (NAV) (30) further comprises the steps of:
25 creating bogus request-to-send (RTS) frame with a maximum value in a
two-bytes duration field (31);
sending the RTS frame to the target AP (32);
waiting for a clear-to-send (CTS) frame from the target AP (33), thereafter
forcing the target AP into idle mode (33a) and initiate NAV timer (33b);
30 and
disengaging the attacking device from the target AP (104) after receiving
the CTS frame.

- 5) A method according to claim 1, wherein the step of notifying the next attacking device selected from the list of attacking devices to connect to the target AP in the idle mode (105) further comprises the steps of:
sharing a NAV timer of the attacking device with the next attacking device
5 (201);
notifying the next attacking device on the expiration of the NAV timer (202); and
connecting the next attacking device to the target AP as the NAV timer expires (203).
10
- 6) A method according to claim 1, wherein the multiple attacks are coordinated through a distribution system by an attacking coordinator.
- 7) A method according to claim 1 wherein the step of notifying the next
15 attacking device selected from the list of attacking devices to connect to the target AP in the idle mode (105) via an attacking coordinator further comprises the steps of:
receiving a NAV timer from the attacking device (301);
sending the NAV timer to the next attacking device (302); and
20 instructing the next attacking device to attack the target AP as the NAV timer expires (303).
- 8) A method according to claim 1, wherein the attacking devices include
25 devices having identical service set identifier (SSID) as the target AP.

1/4

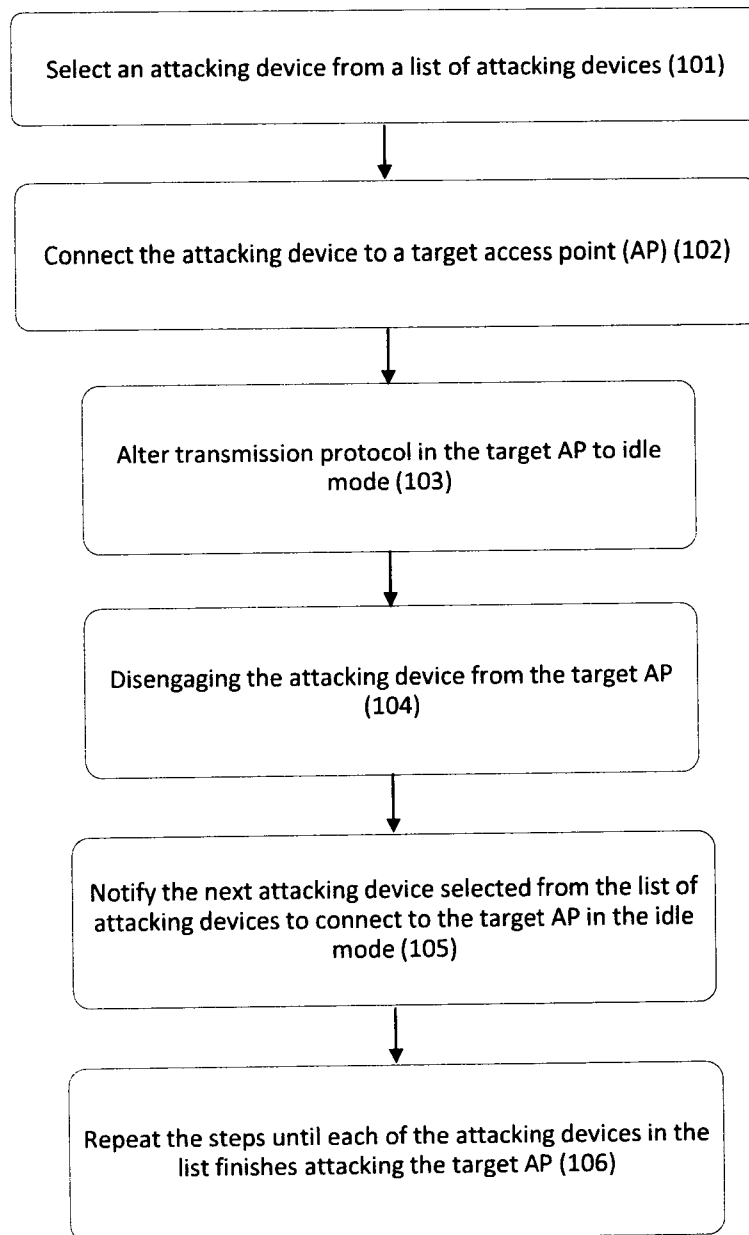


Figure 1

2/4

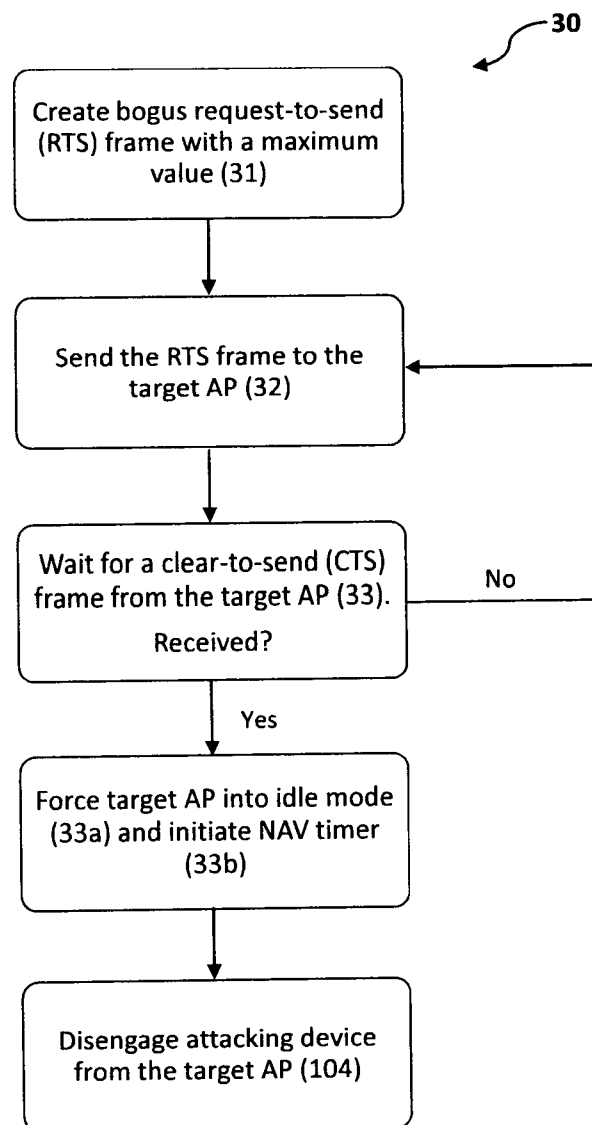


Figure 2

3/4

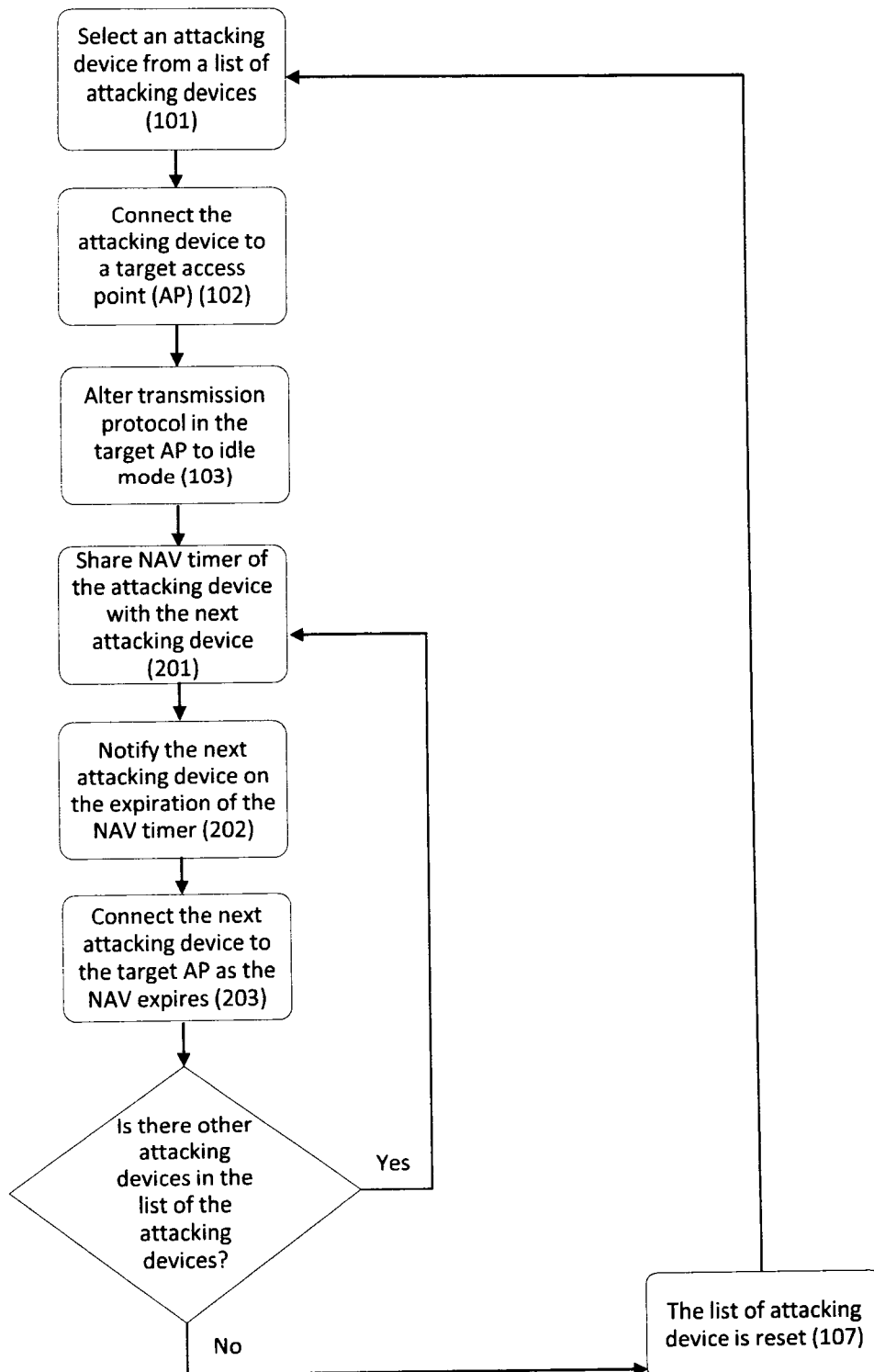


Figure 3

4/4

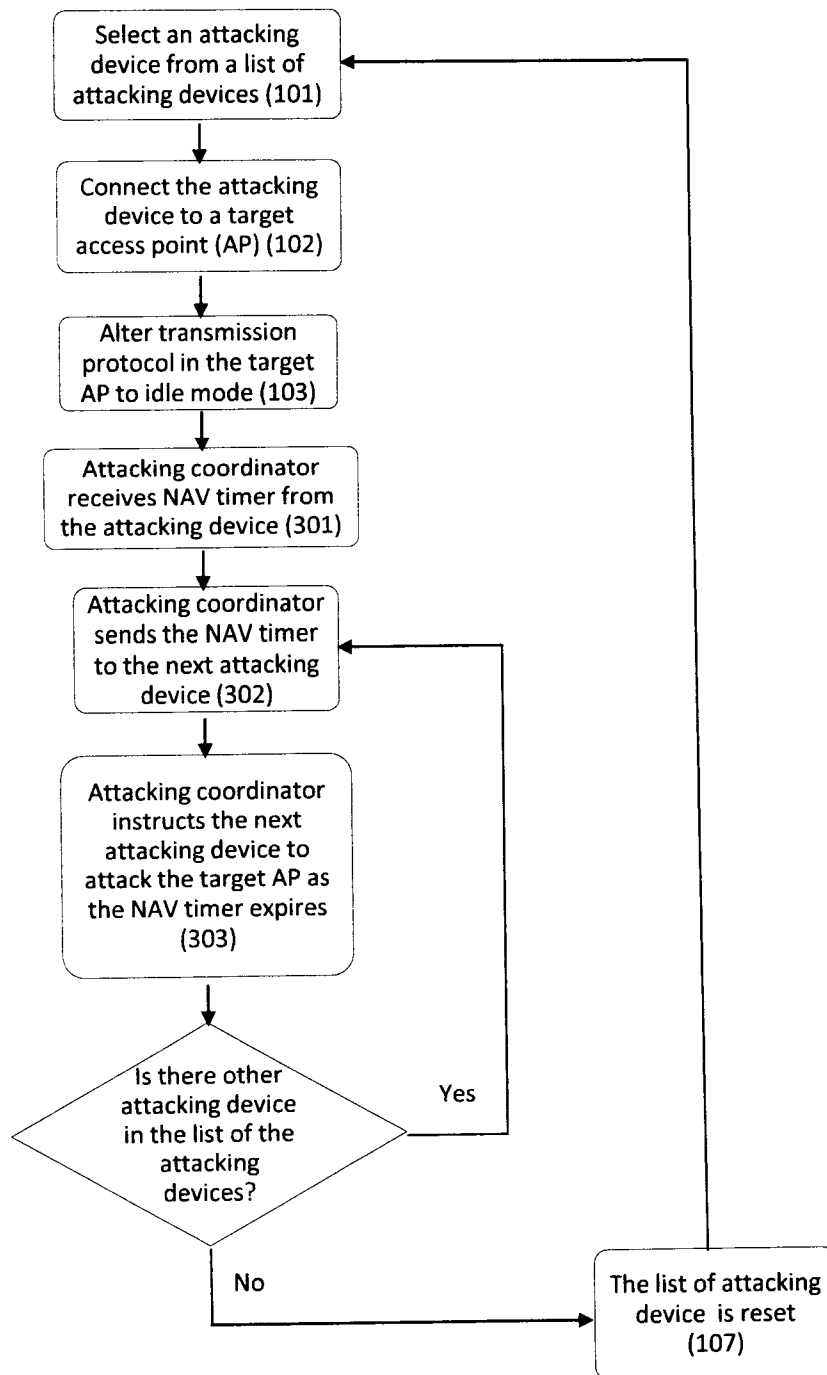


Figure 4

INTERNATIONAL SEARCH REPORT

International application No
PCT/MY2014/000134

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L29/06 H04W12/12
ADD.

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04L H04W

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EPO-Internal, INSPEC, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 1 708 538 A1 (LUCENT TECHNOLOGIES INC [US]) 4 October 2006 (2006-10-04)	1-4,6,8
A	abstract paragraphs [0003], [0006], [0007], [0010], [0014] - [0019] -----	5,7
A	US 2012/180126 A1 (LIU LEI [US] ET AL) 12 July 2012 (2012-07-12) abstract paragraph [0095] -----	1-8
A	US 7 389 354 B1 (SITARAMAN ARAVIND [IN] ET AL) 17 June 2008 (2008-06-17) abstract column 3, line 53 - line 65 -----	1-8



Further documents are listed in the continuation of Box C.



See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search

18 November 2014

Date of mailing of the international search report

25/11/2014

Name and mailing address of the ISA/

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040,
Fax: (+31-70) 340-3016

Authorized officer

San Millán Maeso, J

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/MY2014/000134

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 1708538	A1	04-10-2006	CN 1842087 A 04-10-2006
			DE 602006000127 T2 03-07-2008
			EP 1708538 A1 04-10-2006
			JP 4891641 B2 07-03-2012
			JP 2006295920 A 26-10-2006
			KR 20060105590 A 11-10-2006
			US 2006229022 A1 12-10-2006
US 2012180126	A1	12-07-2012	NONE
US 7389354	B1	17-06-2008	NONE