batman-adv - Bug #242

batadv_neigh_node_release: Double batadv_hardif_neigh_put

03/05/2016 09:43 AM - Sven Eckelmann

Status:	Closed	**Start date:**	03/05/2016
Priority:	Normal	**Due date:**	
Assignee:	Marek Lindner	**% Done:**	0%
Category:		**Estimated time:**	0.00 hour
Target version:	2016.1		

Description

batadv_neigh_node_release (and maybe other places) uses a get + a double put of batadv_hardif_neigh_put without a direct reference in batadv_hardif_neigh_node. So it could be that the reference which is free'd is actually for a different object in memory or maybe was never obtained.

It looks like there should be an explicit reference (pointer) in batadv_hardif_neigh_node to be sure that the correct reference is free'd.

Related issues:

Related to batman-adv - Bug #237: batadv_neigh_node_new: Missing list checks ...	**Closed**	**06/26/2015**

History

#1 - 03/05/2016 09:43 AM - Sven Eckelmann

*- Related to Bug #237: batadv_neigh_node_new: Missing list checks for *list_add* added*

#2 - 03/06/2016 11:08 AM - Sven Eckelmann

Proof-of-concept patches are available in ecsv/no_double_trouble

RFC of the patch was submitted to the mailing list as
https://patchwork.open-mesh.org/project/b.a.t.m.a.n./patch/1457258842-10389-2-git-send-email-sven@narfation.org/

#3 - 03/11/2016 04:47 PM - Sven Eckelmann

- Status changed from New to In Progress

I've posted the cleaned up version of the RFC as patch because there was no objection regarding the idea behind the fix.

- https://patchwork.open-mesh.org/project/b.a.t.m.a.n./patch/1457711046-4603-1-git-send-email-sven@narfation.org/

#4 - 04/21/2016 12:50 PM - Marek Lindner

- Status changed from In Progress to Closed

Sven Eckelmann wrote:

> I've posted the cleaned up version of the RFC as patch because there was no objection regarding the idea behind the fix.
>
> - https://patchwork.open-mesh.org/project/b.a.t.m.a.n./patch/1457711046-4603-1-git-send-email-sven@narfation.org/

Merged! Thanks!

#5 - 02/11/2017 08:39 AM - Sven Eckelmann

- Target version set to 2016.1