

CESNET Technical Report 021/2008

eduroam authentication over jammed network

JAN TOMÁŠEK, MILAN SOVA

Abstract

Current *eduroam* can use several different transport mechanisms to carry messages of different EAP authentication mechanisms. Any particular combination is susceptible to disruption of the transport network at some level. This paper compares the resistance of some of the commonly used configurations to network disruptions.

Keywords: RADIUS, EAP, PEAP, *eduroam*

1 *eduroam* authentication methods

*eduroam*¹ is a wireless roaming network where the user's authentication is provided by his home institution. In the current implementation, this is achieved by proxying RADIUS packets from the access point in the visited network to the RADIUS server at the home institution. The "classic" UDP-based RADIUS transport is susceptible to network disruptions between the visited and home networks.

RadSec ("RADIUS over TLS", see [1]) has been tested recently. Using TCP for transport, RadSec's response to packet loss is different to plain RADIUS.

The most common authentication mechanisms used in *eduroam* are PEAP-MS-CHAPv2, EAP-TTLS and EAP-TLS. The first two are password-based, the last one uses X.509 certificates to authenticate clients (servers are authenticated by X.509 certificates in all three cases). As the protocol exchange in PEAP-MSCHAPv2 and EAP-TTLS are almost identical we have chosen to consider only the former for the sake of simplicity. PEAP-MSCHAPv2 requires the exchange of 11 RADIUS Request-Response packets.

EAP-TLS requires 6 Request-Response exchanges. In addition to that, in contrast to the password-based authentication methods, EAP-TLS does not in principle require contacting the authentication server within the user's home institution - a client certificate can be equally easily verified by a service in the visited institution. This configuration obviously eliminates any effect of the quality of the link between the visited and home institution and can be considered as the reference for the other methods.

2 Measuring setup

We have used the following infrastructure to measure the influence of network quality on the user experience during authentication:

server1 - RADIUS server

Fujitsu-Siemens RX100, 1x Intel Pentium D @ 2.80GHz, 3GB RAM, 1Gbps Ethernet

¹ <http://www.eduroam.org/>

Debian GNU/Linux Etch, Radiator 4.2 + patch 1.904

server2 - RADIUS server

Supermicro, 2x Intel Pentium 4 @ 3.20GHz, 2GB RAM, 1Gbps Ethernet
Debian GNU/Linux Etch, Radiator 4.2 + patch 1.904

server3 - RADIUS server

DELL PE1750, 2x Intel Xeon @ 3.06GHz, 2GB RAM, 1Gbps Ethernet
Debian GNU/Linux Etch, Radiator 4.2 + patch 1.904

server4 - RADIUS server

DELL PE2950, 2x Intel Xeon X5355 @ 2.66GHz, 16GB RAM, 1Gbps Ethernet
Debian GNU/Linux Etch, Radiator 4.2 + patch 1.904

jammer - a router with defined packet loss

VIA Nehemiah @ 1GHz, 512 MB RAM, 100Mbps Ethernet
Slackware Linux 10.0.0, NIST Net 2.0.12b²

We connected the servers a private network (see Figure 1 and Figure 2). The client (*eapol_test* from the *wpa_supplicant* package) is connected directly to the “visited” RADIUS server via ethernet (no access point involved). The tests over WiFi provided a dispersion so high to be useful (some values are provided in).

3 The effect of multiple RADIUS proxies

The first measurement served for calibrating the whole infrastructure. The systems were inter-connected as in Figure 1. We have tested both authentication methods (EAP-TLS, PEAP-MSCHAPv2) over both transports (RADIUS, RadSec).

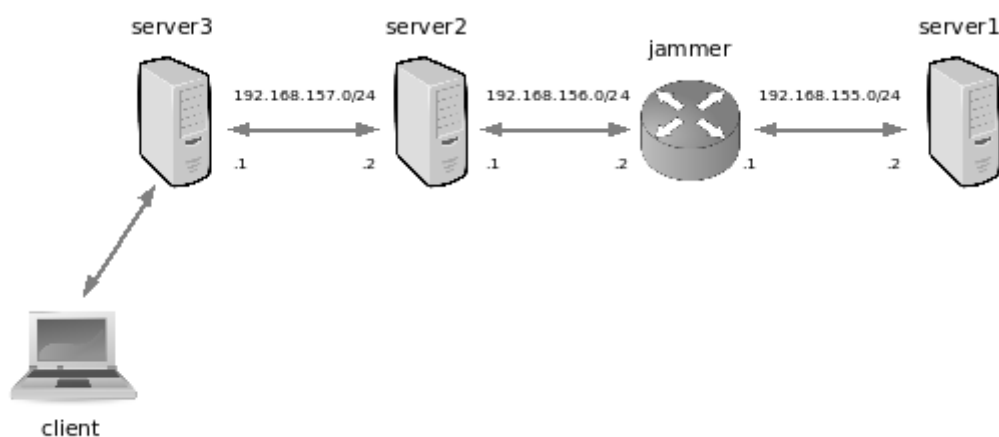


Figure 1. Multiple RADIUS proxies

The delay caused by connecting individual RADIUS servers is recorded in Table 1 for EAP-TLS and in Table 2 for PEAP-MSCHAPv2. For this measurement, the NIST Net router was configured to induce no packet loss.

² <http://snad.ncsl.nist.gov/nistnet/>

Table 1. The delay caused by RADIUS servers using EAP-TLS

Transport	Servers	Success [%]	Mean [s]	Median [s]	Std. dev. [s]	Min [s]	Max [s]
UDP	1	100	0.06	0.06	0.01	0.05	0.12
UDP	1,2	100	0.11	0.11	0.01	0.11	0.18
UDP	1,2,3	100	0.16	0.16	0.01	0.15	0.23
RadSec	1,2	100	0.11	0.11	0.01	0.11	0.19
RadSec	1,2,3	100	0.16	0.16	0.00	0.15	0.22

Table 2. The delay caused by RADIUS servers using PEAP-MSCHAPv2

Transport	Servers	Success [%]	Mean [s]	Median [s]	Std. dev. [s]	Min [s]	Max [s]
UDP	1	100	0.09	0.09	0.01	0.09	0.25
UDP	1,2	100	0.18	0.18	0.02	0.17	0.42
UDP	1,2,3	100	0.26	0.26	0.01	0.25	0.44
RadSec	1,2	100	0.18	0.18	0.01	0.17	0.28
RadSec	1,2,3	100	0.26	0.26	0.01	0.25	0.34

The results show that one RADIUS server adds 0.05 seconds to the overall delay for EAP-TLS and 0.08 seconds for PEAP-MSCHAPv2. The difference is caused by the fact that EAP-TLS requires 6 Request-Response exchanges while PEAP-MSCHAPv2 needs 11 of them.

Note that NIST Net router does not add to the delay.

4 The effect of wireless connection

The tables in this section describe mainly the influence of a wireless channel to the precision of the measurement.

Table 3. The delay caused by RADIUS servers using WiFi 802.11b (2.4GHz) and EAP-TLS

Transport	Servers	Success [%]	Mean [s]	Median [s]	Std. dev. [s]	Min [s]	Max [s]
UDP	1	100	3.42	3.14	0.85	0.30	6.17
UDP	1,2	100	4.22	3.25	5.13	0.30	75.42
UDP	1,2,3	98	4.62	3.26	6.19	0.41	70.43

Table 4. The delay caused by RADIUS servers using WiFi 802.11a (5GHz) and EAP-TLS

Transport	Servers	Success [%]	Mean [s]	Median [s]	Std. dev. [s]	Min [s]	Max [s]
UDP	1	100	4.81	4.61	2.16	4.50	41.87
UDP	1,2	99	4.98	4.62	3.04	4.51	41.84
UDP	1,2,3	100	4.92	4.71	2.16	4.61	41.85

Note the high variance of the time needed to authenticate. This precludes using the wireless channel for measuring the robustness of different authentication methods with respect to the transport channel quality.

5 The effect of packet loss

To find out the influence of the packet loss has on the *eduroam* authentication process, we have set up the systems according to Figure 2. The client used an usual *wpa_supplicant*'s strategy of re-sending requests until either the connection is established or the authentication timer (120 seconds in our case) expires.

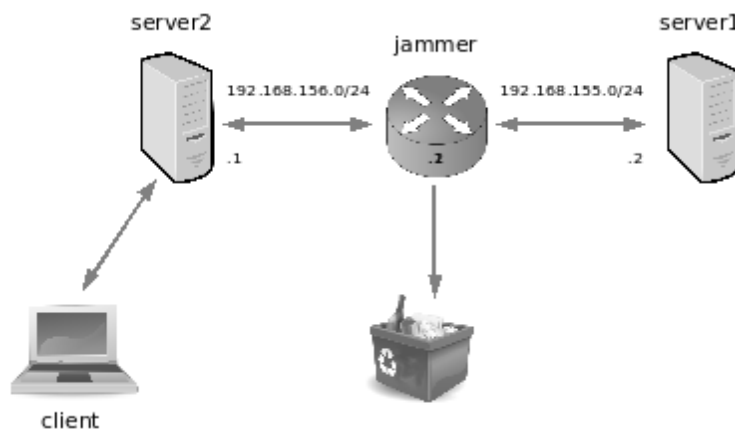


Figure 2. Controlling packet loss

We have tested the responsiveness of individual authentication mechanisms over different transports in three scenarios:

1. the NIST Net router dropped packets going from the client to the RADIUS server
2. the NIST Net router dropped packets going from the RADIUS server to the client
3. the NIST Net router dropped packets going in both directions

The results are provided in the following sections where

Loss

packet loss

Success

rate of successful authentications

Mean

mean time before successful authentication

Median

median time before successful authentication

Std. dev.

standard deviation of the time before successful authentication

Min

minimal value of the time before successful authentication

Max

maximal value of the time before successful authentication

5.1 Dropping packets from client to server1

For the first set of measurements, the NIST Net router discarded packets originated at *server2* designated to *server1*.

Table 5. EAP-TLS over UDP, packet loss from client to server

Loss	Success [%]	Mean [s]	Median [s]	Std. dev. [s]	Min [s]	Max [s]
1.0	100	0.28	0.11	0.69	0.11	3.12
5.0	100	1.31	0.11	2.96	0.11	24.12
10.0	100	3.27	0.11	6.14	0.11	42.13
20.0	99	6.71	3.11	9.33	0.11	48.15
30.0	96	15.59	9.11	15.18	0.11	90.17
40.0	90	24.34	24.12	19.70	0.11	87.14
50.0	68	35.22	30.13	22.34	0.11	96.14
60.0	49	42.13	45.13	27.08	0.11	114.16
70.0	19	48.39	48.13	24.43	0.11	117.17
80.0	3	75.15	72.15	20.62	33.13	111.16

Table 6. EAP-TLS over RadSec, packet loss from client to server

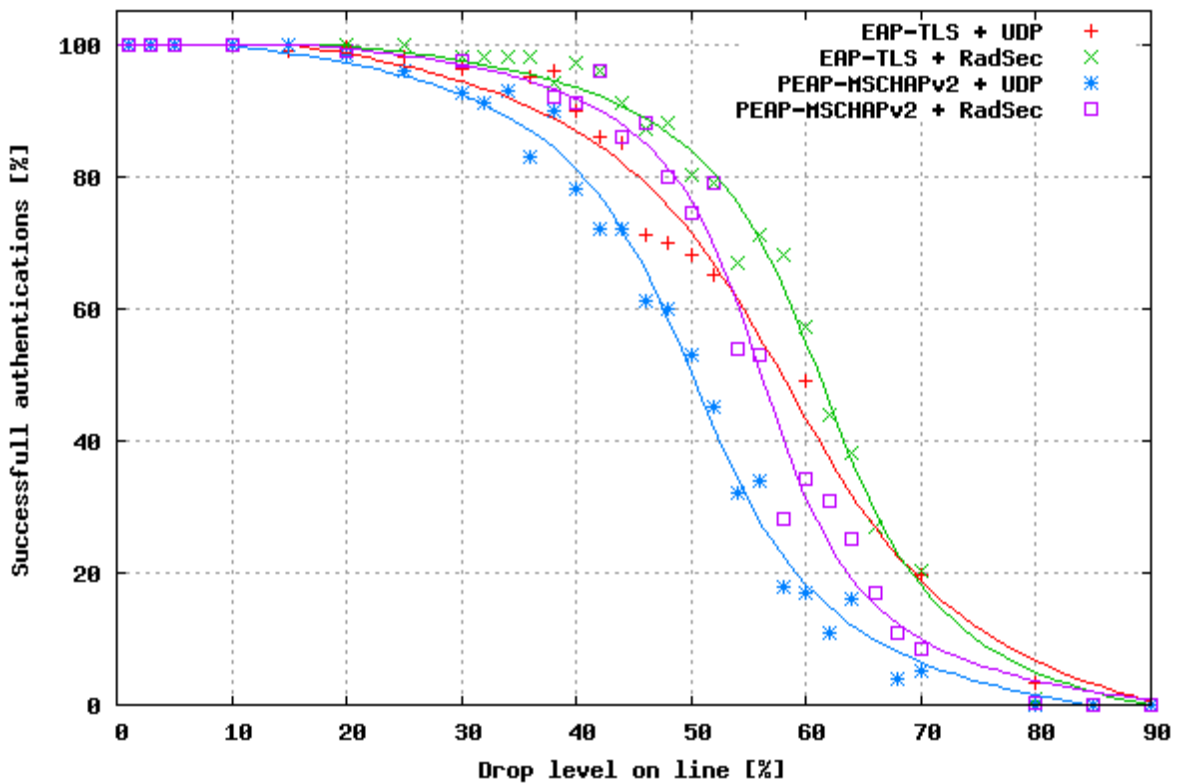
Loss	Success [%]	Mean [s]	Median [s]	Std. dev. [s]	Min [s]	Max [s]
1.0	100	0.13	0.11	0.06	0.11	0.32
5.0	100	0.19	0.11	0.16	0.11	1.56
10.0	100	0.25	0.11	0.21	0.11	1.57
20.0	100	0.54	0.32	0.58	0.11	3.64
30.0	98	0.86	0.53	0.80	0.11	4.48
40.0	97	1.53	0.94	2.66	0.11	22.95
50.0	80	3.91	1.98	7.77	0.11	50.53
60.0	57	5.12	2.51	8.01	0.32	50.13
70.0	20	16.51	7.18	17.24	0.32	51.98
80.0	1	33.01	25.70	nan	24.45	48.87

Table 7. PEAP-MSCHAPv2 over UDP, packet loss from client to server

Loss	Success [%]	Mean [s]	Median [s]	Std. dev. [s]	Min [s]	Max [s]
1.0	100	0.40	0.18	0.82	0.17	6.18
5.0	100	1.97	0.18	3.01	0.17	24.19
10.0	100	6.16	3.18	8.10	0.17	66.20
20.0	98	13.64	6.18	13.20	0.17	69.20
30.0	92	27.16	24.20	20.86	0.17	96.22
40.0	78	40.03	33.20	24.30	0.17	111.24
50.0	53	56.02	54.20	21.88	9.18	108.23
60.0	17	70.74	75.21	28.07	6.17	117.24
70.0	5	87.82	93.21	19.02	51.20	105.22
80.0	0	nan	nan	nan	nan	nan

Table 8. PEAP-MSCHAPv2 over RadSec, packet loss from client to server

Loss	Success [%]	Mean [s]	Median [s]	Std. dev. [s]	Min [s]	Max [s]
1.0	100	0.20	0.18	0.07	0.18	0.60
5.0	100	0.29	0.18	0.16	0.17	1.01
10.0	100	0.45	0.39	0.31	0.18	1.66
20.0	99	0.91	0.80	0.69	0.18	4.75
30.0	97	1.71	1.43	1.67	0.18	22.84
40.0	91	3.08	2.26	4.02	0.18	50.82
50.0	74	5.76	3.74	8.42	0.38	51.55
60.0	34	10.71	5.99	12.14	0.80	54.27
70.0	8	18.51	9.01	18.54	2.06	72.20
80.0	0	nan	nan	nan	nan	nan

**Figure 3.** Dropping packets from client to server

5.2 Dropping packets from server1 to client

In the second set of measurement, the NIST Net router discarded packets originated at *server1* and designated to *server2*.

5.3 Dropping packets in both directions

The packet loss values in tables and graphs in this section were configured for both directions. I. e. the overall packet loss on the link was twice as high as the value listed. For instance, the value 20% means 20% packets lost from client to server plus another 20% lost in the opposite direction.

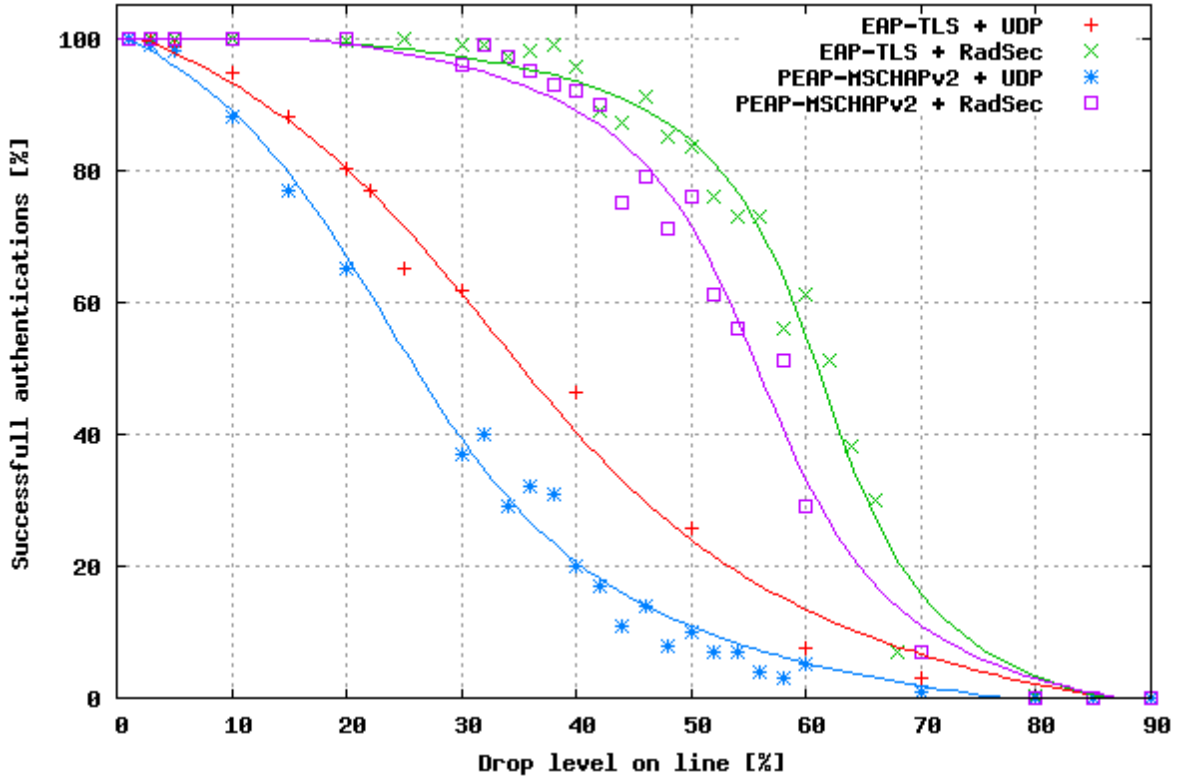


Figure 4. Dropping packets from server1 to client

Table 9. EAP-TLS over UDP, packet loss from server to client

Loss	Success [%]	Mean [s]	Median [s]	Std. dev. [s]	Min [s]	Max [s]
1.0	100	0.23	0.11	0.68	0.11	6.10
5.0	98	1.02	0.11	1.58	0.11	9.12
10.0	94	1.72	0.11	2.78	0.11	27.12
20.0	80	4.44	3.11	6.00	0.11	33.11
30.0	61	6.89	3.11	9.17	0.11	51.12
40.0	46	8.77	6.10	9.44	0.11	57.12
50.0	25	12.77	6.11	12.41	0.11	54.11
60.0	7	13.71	6.11	14.35	0.11	54.11
70.0	3	24.77	27.11	13.26	6.10	51.12
80.0	0	nan	nan	nan	nan	nan

6 Conclusions

The TCP transport is significantly more reliable than UDP and provides authentication success rate over 90% over links with 40% packet loss. With worsening quality of the link the success rate decreases dramatically below 20% at 60% lost packets.

The reliance of UDP transport on the link quality is much more linear, getting below the usability threshold of 50% at around 35% lost packets depending on the length of authentication exchange. The more favorable results for client-to-server jamming are caused by the aggressive packet re-sending strategy of wpa_supplicant compared to the behaviour of Radiator.

Table 10. EAP-TLS over RadSec, packet loss from server to client

Loss	Success [%]	Mean [s]	Median [s]	Std. dev. [s]	Min [s]	Max [s]
1.0	100	0.13	0.11	0.06	0.11	0.33
5.0	100	0.17	0.11	0.13	0.11	0.99
10.0	100	0.27	0.11	0.21	0.11	1.41
20.0	99	0.51	0.33	0.48	0.11	3.78
30.0	99	0.94	0.54	1.00	0.11	7.90
40.0	95	1.65	0.98	3.16	0.11	46.40
50.0	83	3.35	1.83	6.73	0.11	52.59
60.0	61	6.69	3.33	11.00	0.33	50.60
70.0	7	9.52	3.75	15.95	0.32	48.30
80.0	0	nan	nan	nan	nan	nan

Table 11. PEAP-MSCHAPv2 over UDP, packet loss from server to client

Loss	Success [%]	Mean [s]	Median [s]	Std. dev. [s]	Min [s]	Max [s]
1.0	100	0.60	0.18	1.12	0.17	6.17
5.0	98	1.34	0.17	1.90	0.17	6.18
10.0	88	4.67	3.17	4.93	0.17	24.21
20.0	65	9.98	6.17	9.86	0.17	54.18
30.0	37	13.79	9.17	10.41	0.17	36.17
40.0	20	21.77	13.66	15.44	6.16	57.19
50.0	10	28.07	28.68	12.52	12.15	54.18
60.0	5	18.82	12.16	12.09	6.16	36.19
70.0	1	27.20	27.20	nan	27.20	27.20
80.0	0	nan	nan	nan	nan	nan

Table 12. PEAP-MSCHAPv2 over RadSec, packet loss from server to client

Loss	Success [%]	Mean [s]	Median [s]	Std. dev. [s]	Min [s]	Max [s]
1.0	100	0.21	0.18	0.07	0.17	0.39
5.0	100	0.32	0.18	0.18	0.17	1.06
10.0	100	0.43	0.39	0.25	0.17	1.23
20.0	100	0.94	0.81	0.66	0.17	4.20
30.0	96	1.54	1.25	1.07	0.18	5.45
40.0	92	3.32	2.50	3.77	0.59	22.69
50.0	76	5.95	3.89	7.63	0.60	47.95
60.0	29	12.68	6.56	12.90	1.65	51.97
70.0	7	34.52	31.87	20.17	5.31	58.03
80.0	0	nan	nan	nan	nan	nan

The measuring method used was quite simple. In addition to just dropping packets, real networks might misbehave with regards to the size of a packet (e. g. MTU problems) or the influence of other traffic. However, the responsiveness of TCP and UDP transport should be comparable to our results.

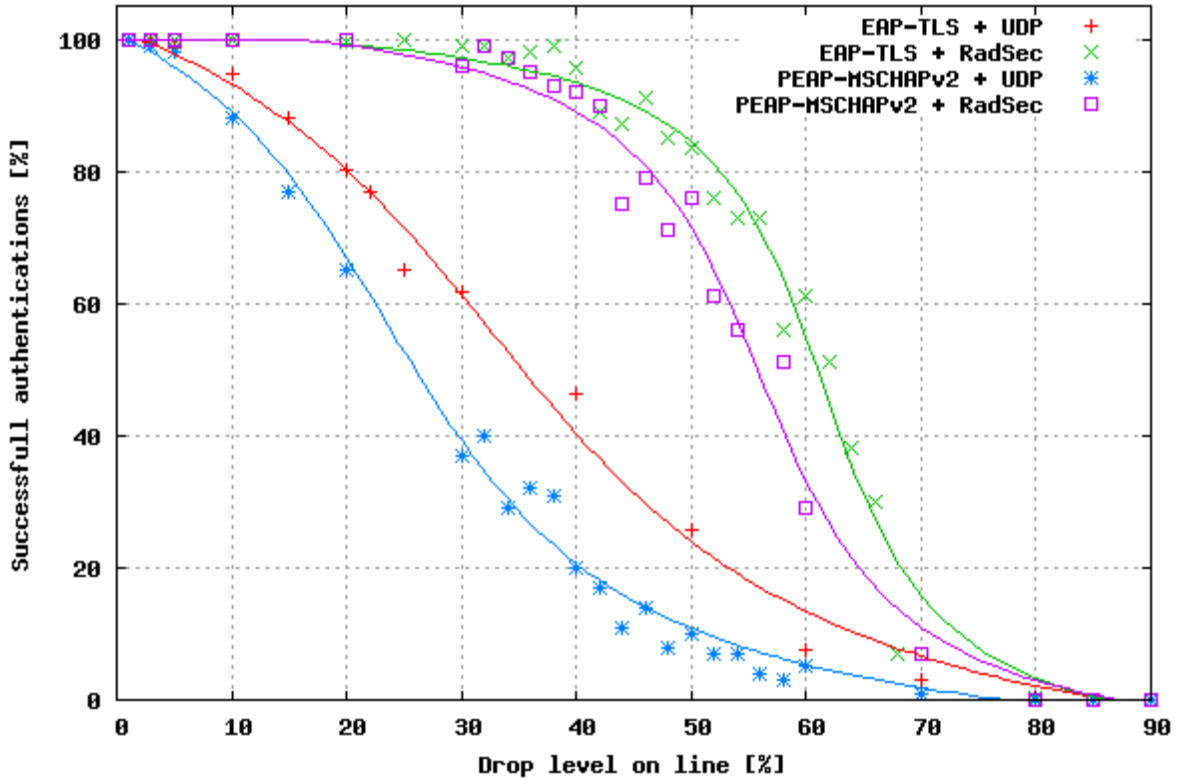


Figure 4. Dropping packets from server1 to client

Table 13. EAP-TLS over UDP, packet loss in both directions

Loss	Success [%]	Mean [s]	Median [s]	Std. dev. [s]	Min [s]	Max [s]
1.0	100	0.47	0.11	1.03	0.11	6.11
3.0	99	1.54	0.11	3.14	0.11	24.13
5.0	97	2.11	0.11	3.53	0.11	24.12
10.0	88	4.53	3.11	6.55	0.11	54.13
15.0	74	9.00	3.12	11.36	0.10	54.13
20.0	63	11.22	6.11	11.25	0.11	51.12
25.0	52	17.33	9.10	15.67	0.10	72.13
30.0	35	20.41	21.12	15.92	0.11	75.14
40.0	14	32.30	30.12	25.40	3.10	114.15
50.0	3	46.33	46.62	25.83	9.11	96.15

Table 14. EAP-TLS over RadSec, packet loss in both directions

Loss	Success [%]	Mean [s]	Median [s]	Std. dev. [s]	Min [s]	Max [s]
1.0	100	0.14	0.11	0.09	0.11	0.60
3.0	100	0.18	0.11	0.13	0.11	0.79
5.0	100	0.25	0.11	0.19	0.11	1.24
10.0	100	0.47	0.34	0.41	0.11	2.99
15.0	100	0.85	0.64	0.74	0.10	4.66
20.0	98	1.58	1.18	1.41	0.11	8.17
25.0	87	3.15	1.86	6.19	0.10	53.03
30.0	0	nan	nan	nan	nan	nan
40.0	0	nan	nan	nan	nan	nan
50.0	0	nan	nan	nan	nan	nan

Table 15. PEAP-MSCHAPv2 over UDP, packet loss in both directions

Loss	Success [%]	Mean [s]	Median [s]	Std. dev. [s]	Min [s]	Max [s]
1.0	99	1.04	0.18	1.94	0.17	21.20
3.0	98	2.30	0.18	3.83	0.17	24.19
5.0	93	4.27	3.17	5.44	0.17	30.19
10.0	80	7.32	6.17	7.64	0.17	42.19
15.0	61	14.83	9.17	12.81	0.17	51.18
20.0	37	21.75	15.19	17.62	0.17	78.21
25.0	26	27.53	27.18	21.19	0.17	78.20
30.0	12	40.29	39.17	25.20	6.16	96.22
40.0	1	64.39	63.18	nan	36.17	90.20
50.0	0	nan	nan	nan	nan	nan

Table 16. PEAP-MSCHAPv2 over RadSec, packet loss in both directions

Loss	Success [%]	Mean [s]	Median [s]	Std. dev. [s]	Min [s]	Max [s]
1.0	100	0.22	0.18	0.09	0.18	0.80
3.0	100	0.34	0.38	0.19	0.18	1.11
5.0	100	0.49	0.40	0.32	0.18	2.38
10.0	100	0.82	0.63	0.60	0.18	3.94
15.0	98	1.61	1.08	3.04	0.18	30.16
20.0	94	3.28	2.55	3.08	0.18	25.37
25.0	56	5.90	3.50	7.55	0.19	47.44
30.0	13	14.60	6.31	23.33	0.95	100.74
40.0	0	nan	nan	nan	nan	nan
50.0	0	nan	nan	nan	nan	nan

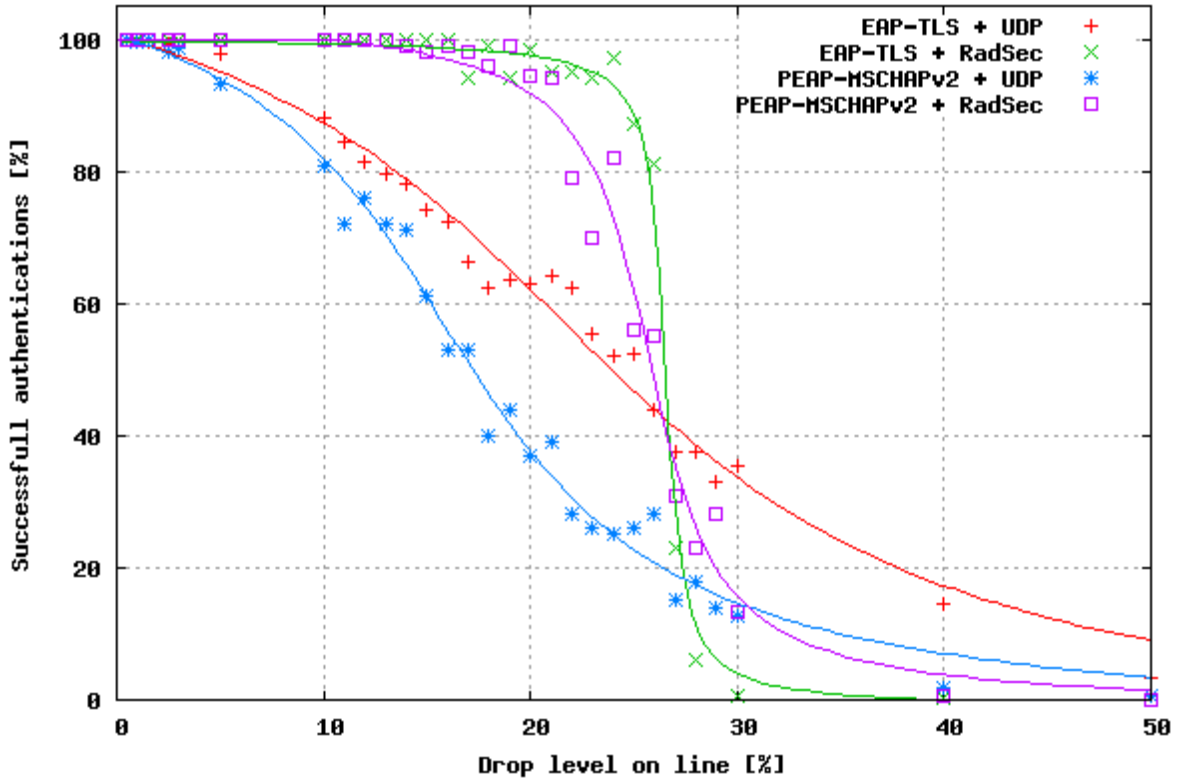


Figure 5. Dropping packets in both directions

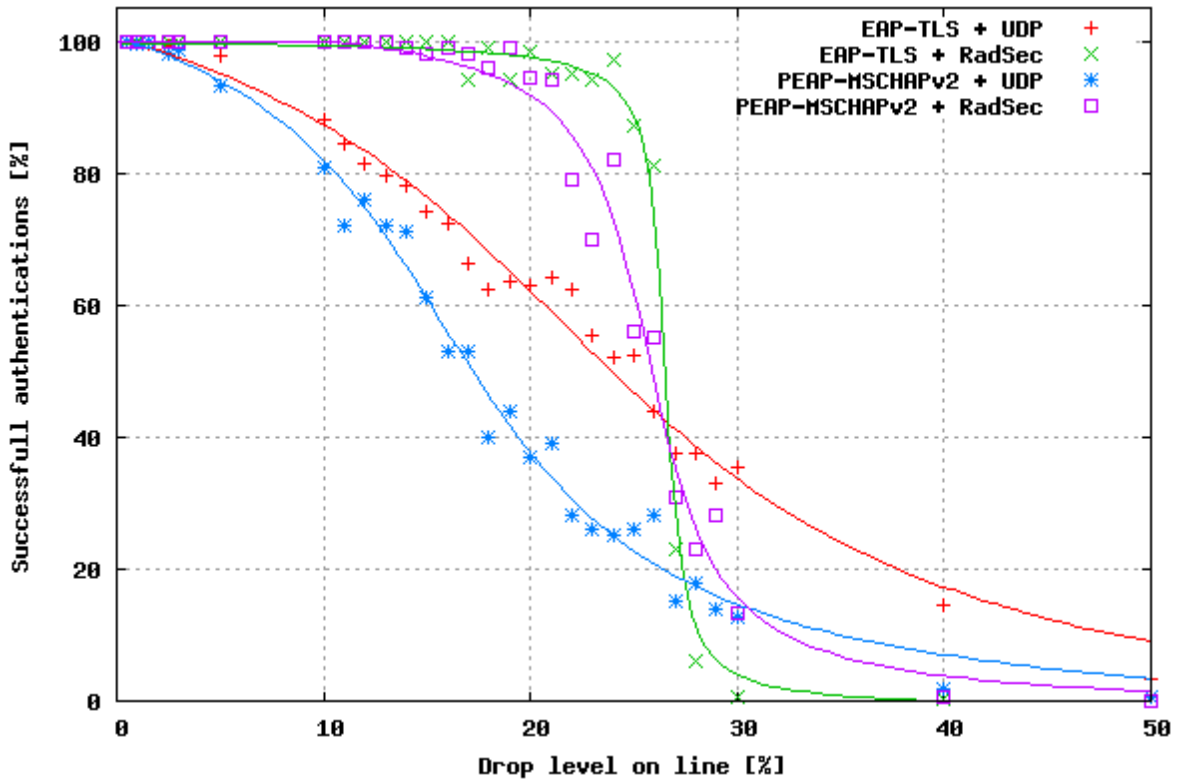


Figure 5. Dropping packets in both directions

References

- [1] WINTER, S.; VENAAS, S.; WIERENGA, K. *TLS encryption for RADIUS over TCP (RadSec)*. draft-ietf-radext-radsec-02³, IETF, 2008.

³ <http://tools.ietf.org/html/draft-ietf-radext-radsec-02>