

Errata

Publication I

Authors' organizational affiliation marked with dagger-symbol (†) should have been Department of Computer Science *and Engineering* instead of Department of Computer Science.

Page 5, last paragraph of section 3. The value of Δ_1 should be 200 ms and Δ_2 500 ms. Variable Δ_3 does not exist in the protocol or the prototype.

Citation [28] in the publication has incorrect publication year and venue. See the citation [87] in this dissertation for the correct information.

Publication III

The first column of Table 1 was not printed correctly. The table should look as shown below.

Table 1: List of attacks analyzed in this paper

	Flow-table modification				Control-channel hijacking			
	No TLS	Controller authentication	Mutual authentication	Out-of-band control channel	No TLS	Controller authentication	Mutual authentication	Out-of-band control channel
Eavesdrop control data with packet duplication	✓	✓	✓	✓	✓	✓	✓	✓
MitM attack by diverting traffic	✓	✓	✓	✓	✓	✓	✓	✓
Spoof the state of the compromised switch e.g. to avoid attack detection					✓	✓	✓	✓
Eavesdrop control traffic of the compromised switch					✓	✓	✓	✓
Eavesdrop downstream switches' control traffic	✓				✓			
Spoof downstream switches' state	✓				✓			
Topology spoofing: add bogus switches to the network	✓	✓		? ¹	✓	✓		? ¹
Empty downstream switches' flowtables (DoS)	✓				✓			

¹Depends on the control-network implementation. This and many further attacks against uncompromised switches may be possible if the control network does not provide adequate isolation between switches.