False Detection Problem

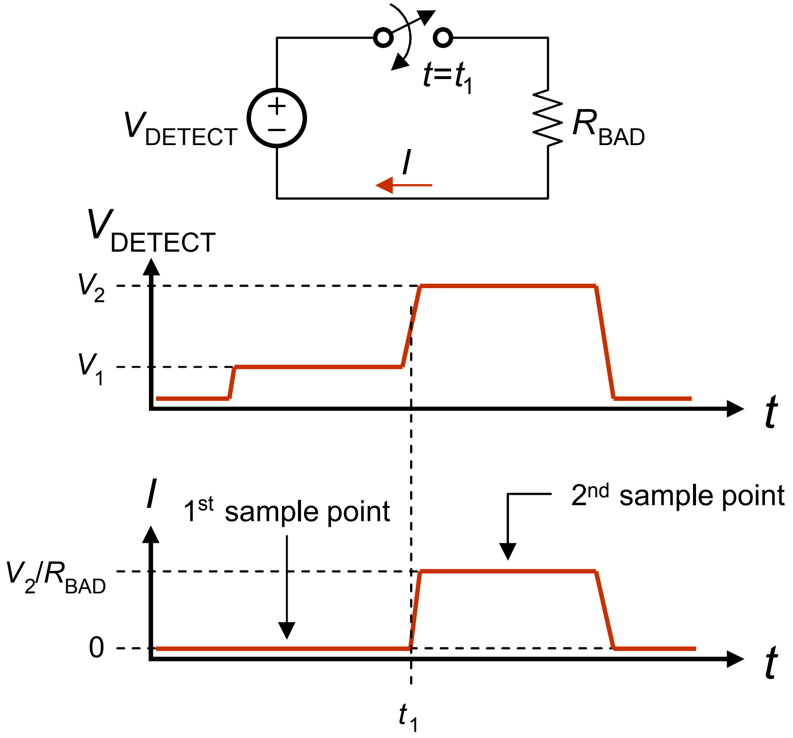
Steve Robbins

Overview

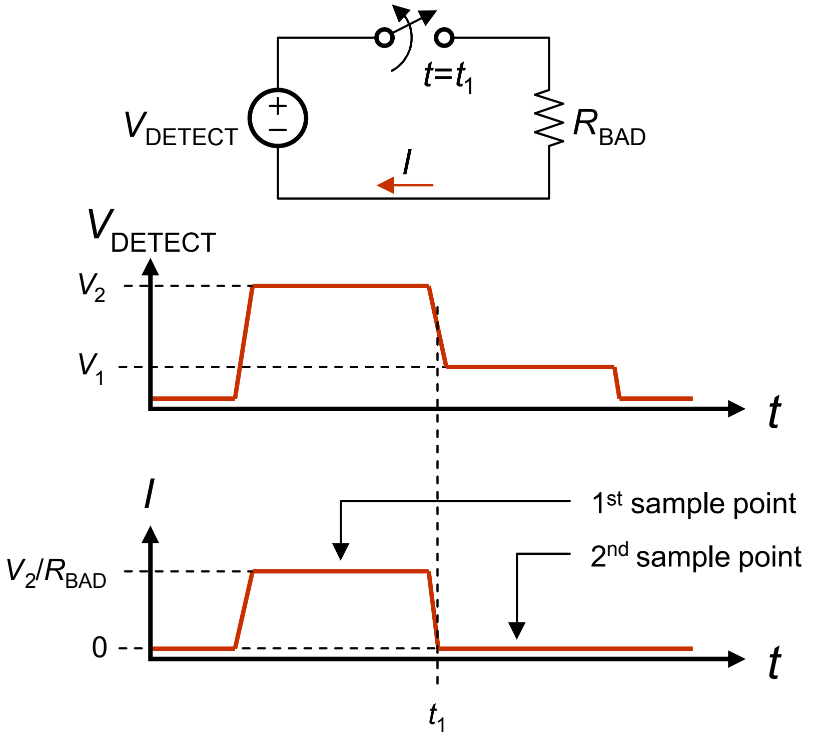
- There is a flaw in the detection protocol defined in 802.3af. A PSE should never turn on power to a PD if R_{SIG} is outside the R_{GOOD} range. *But it can happen*.
- A network device with an invalid signature (far outside the R_{GOOD} range) can fool the PSE if it's connected (or disconnected) at some instant between the two detection sample points.
- This is not just a theory. This problem has been observed repeatedly during PSE testing.
- The chance of this happening in the field are small, but this loophole should be closed.

Circuit Theory

Case 1: Invalid PD connected in the middle of detection



Case 2: Invalid PD disconnected in the middle of detection



Note: Two other cases are possible, where the open circuit occurs while $V_{DETECT}=V_2$. But these cases produce a negative number for $R_{MEASURED}$. The PSE controller should be designed to ignore negative detection signatures.

Error Analysis

- In both the cases from the previous slide, the PSE sees

$$R_{\mathrm{MEASURED}} = \frac{V_2 - V_1}{V_2/R_{\mathrm{BAD}} - 0} = R_{\mathrm{BAD}}(1\text{-}V_1/V_2)$$

- Plugging in some typical numbers from 802.3af Table 33-2
  - □ A typical R_{GOOD} range: 16.5k to 30k.
  - □ Some typical voltage levels: V_1=3V and V_2=6V.
  - □ Result: Invalid signatures from 33k to 60k can fool the PSE.
- Worst-case
  - □ Extreme limits of R_{GOOD} range: 15k to 33k.
  - □ Extreme voltage limits: V_1=9V and V_2=10V.
  - □ Result: Invalid signatures from 150k to 330k can fool the PSE.

Suggested Fix

- Change the PSE state diagram to require two consecutive successful detection cycles before it turns on power to the PD.
- The timing requirements of 802.3af Table 33-5 can stay as they are:
  - Detection time (T_{det}) is 500ms maximum.
  - Midspan backoff time (T_{dbo}) is 2 seconds minimum.
  - Therefore an endspan PSE is guaranteed enough time for at least 4 detection cycles.