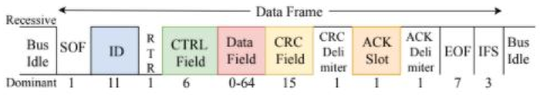
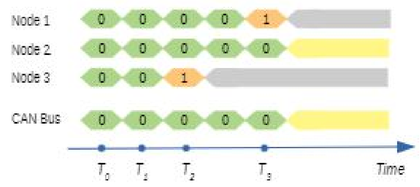
University of Colorado Colorado Springs

Introduction & Problem Statement

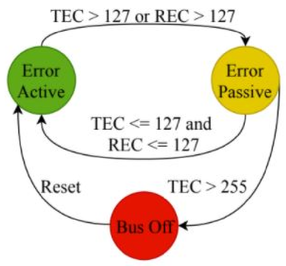
- **Controller Area Network (CAN) bus Attributes:**
  - Predictable system connecting electronic control units (ECUs)
  - Broadcast-based communication of CAN frames



  - Deterministic Resolution of Arbitration



  - Fault Confinement
    (*TEC = Transmit Error Count, REC = Receive Error Count*)



- **These attributes can allow a skillful adversary to:**
  - Obtain parameters related to the messages
  - Launch a timing-based attack on safety-critical components

Objective

Demonstrate how message period can be inferred in the presence of real-time uncertainties(offsets, jitter)

Period Estimation

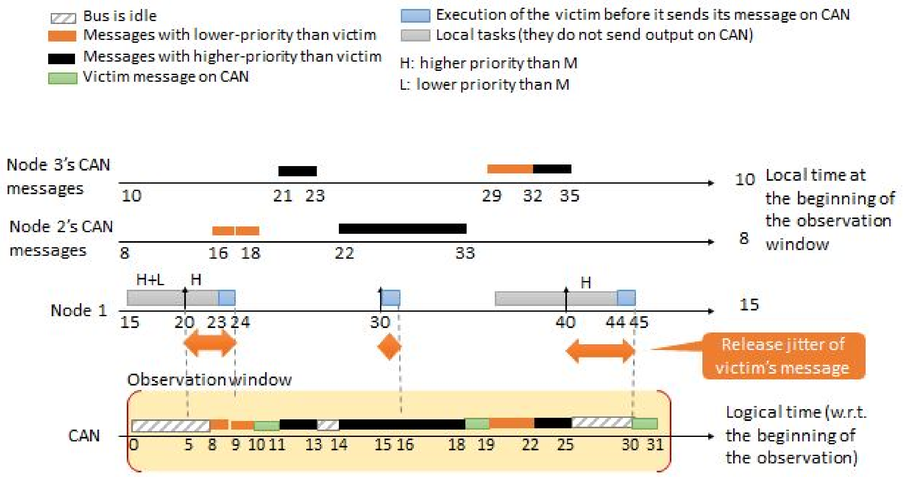


Fig. 5: Attacker's View and Challenges to Message Parameters Estimation

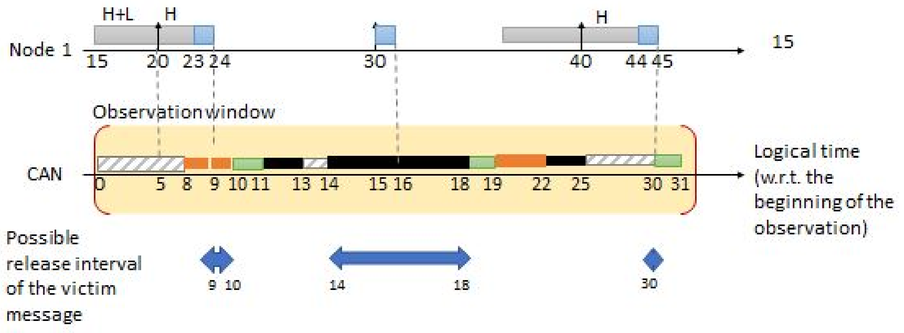


Fig. 6: Period Inference

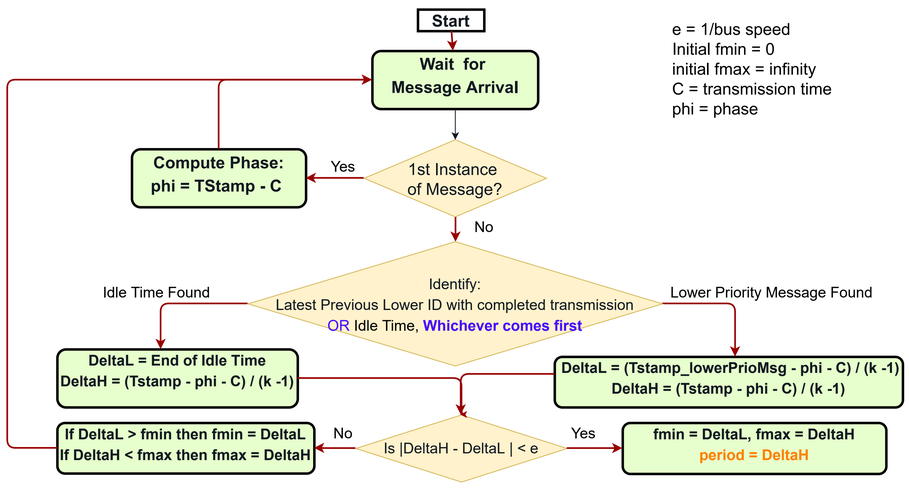
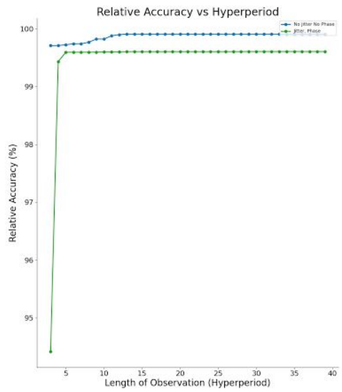


Fig. 7: Period Estimation Flowchart [1]

Results

Sender	Message ID (hex)	Size (bytes)	Period (ms)
VC	A0	1	5
	B0	6	10
	D0	1	1000
Brakes	A1	2	5
	C1	1	100
Battery	B2	1	10
	C2	4	100
	D2	3	1000
Driver	A3	1	5
	B3	2	10
IMC	A4	2	5
	B4	2	10
Trans	A5	1	5
	C5	1	100
	D5	1	1000

Fig. 8: SAE Benchmark [2]



Future Work

- Demonstrate the ability to launch a timing attack
- Evaluate the effects of message and system parameters (priority, utilizat

Acknowledgements

This work is partially supported by NSF CNS-2011620,NSF OAC-200178
Colorado State Bill 18-086

References

[1] Habeeb Olufowobi et al. "Saiducant: Specification-based automotive intrusion detec ing controller area network (can) timing". In: *IEEE Transactions on Vehicular Technolo* (2019), pp. 1484–1494.

[2] K. Tindell, A. Burns, and A. J. Wellings. "Calculating controller area network (can) m response times". In: *Control Engineering Practice* 3.8 (Aug. 1995), pp. 1163–1169. ISSN 0661. DOI: 10.1016/0967-0661(95)00112-8. (Visited on 02/12/2020).