

TinySec: Performance Characteristics

Chris K :: **Naveen S** :: David W

January 16, 2004

This Talk

- Recent results
 - Measurements on Mica2s (TOS 1.1.2)
 - Latency
 - Bandwidth
 - Power
 - Stress testing
- Hardware crypto comparison & implications
 - 802.15.4 (e.g. CC2420)

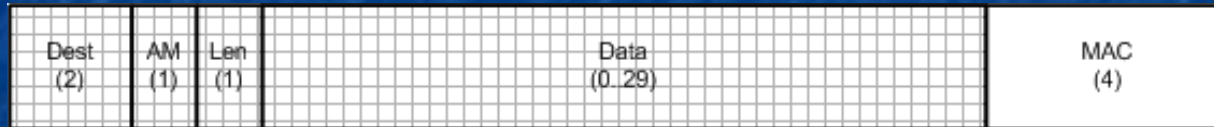
TinySec Review: How & Why

- Link layer security mechanism
 - Hop-by-hop, not end-to-end
 - Better support for aggregation
 - Enables higher level keying protocols
- Low overhead security in software
- Cryptographic checksum
 - Ensures integrity
 - Enforces access control
- Optional encryption

TinySec Performance

- Characterize Overhead: Energy, Latency, Bandwidth.
- Factors for TinySec overhead
 - Computation
 - Larger Packet Sizes
- Can predict overhead caused by packet sizes
- Measurement goal: Show computation overhead is minimal
- Note: crypto HW only reduces computation overhead

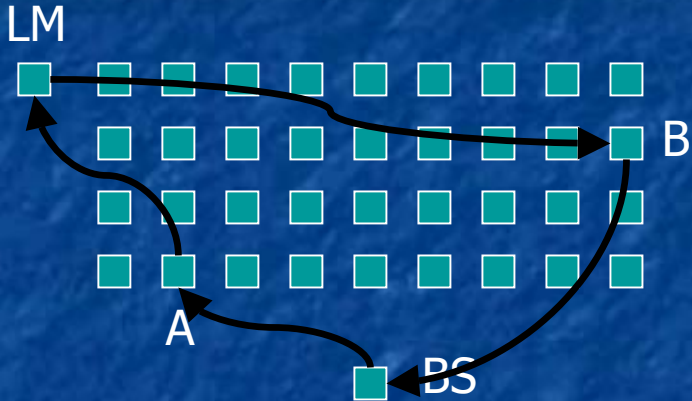
Packets & Predicted Overhead



IV

	Overhead (b)	Total Size (b)	Xmit time (ms)	Increase
CRC	39	63	26.2	--
TinySec-Auth	40	64	26.6	1.5%
TinySec-AE	44	68	28.8	8%

Latency Test Setup



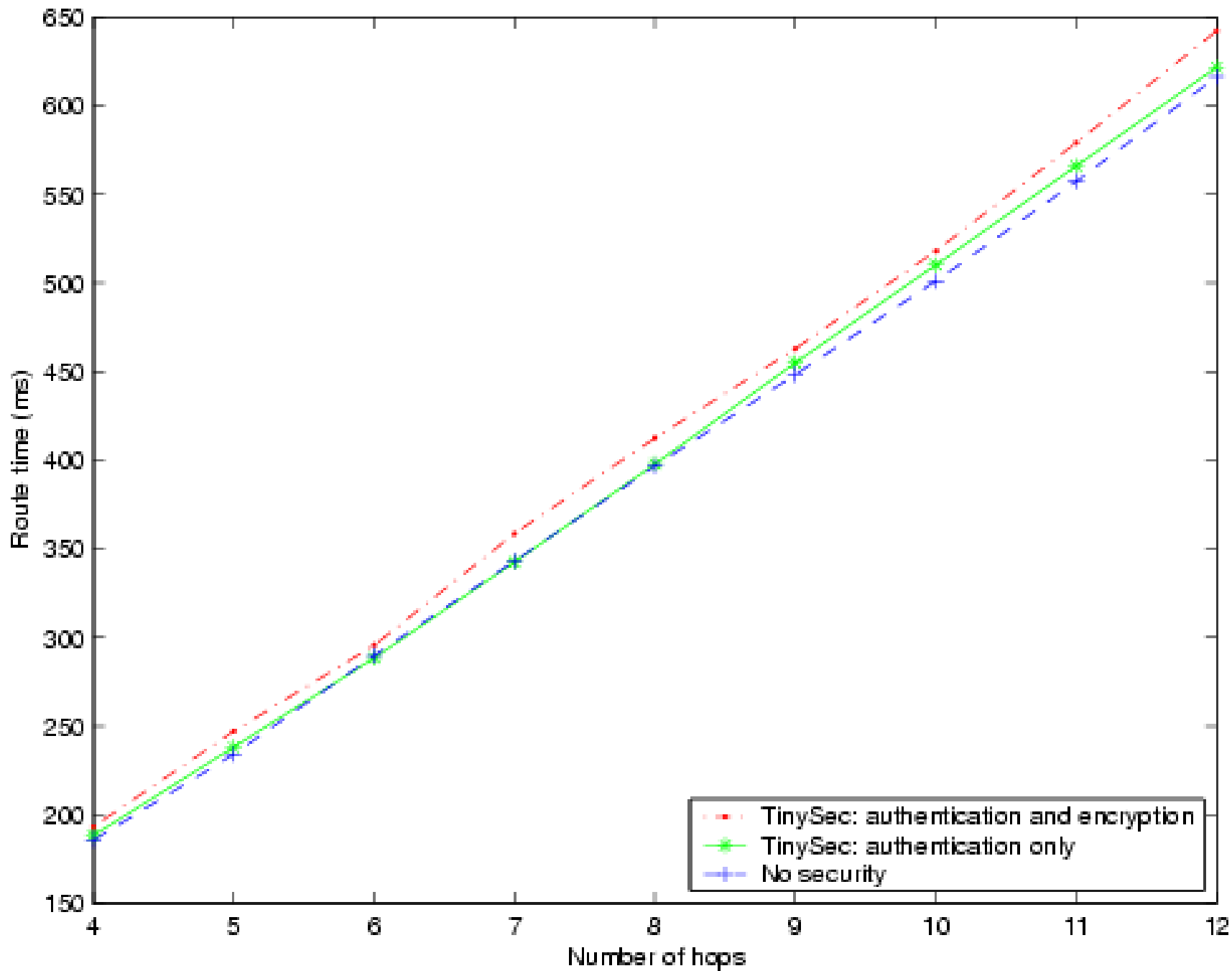
■ Setup:

- 4x9 grid in Woz of Mica2s
- Landmark routing code from midterm demo
- 200 measurements per hopcount

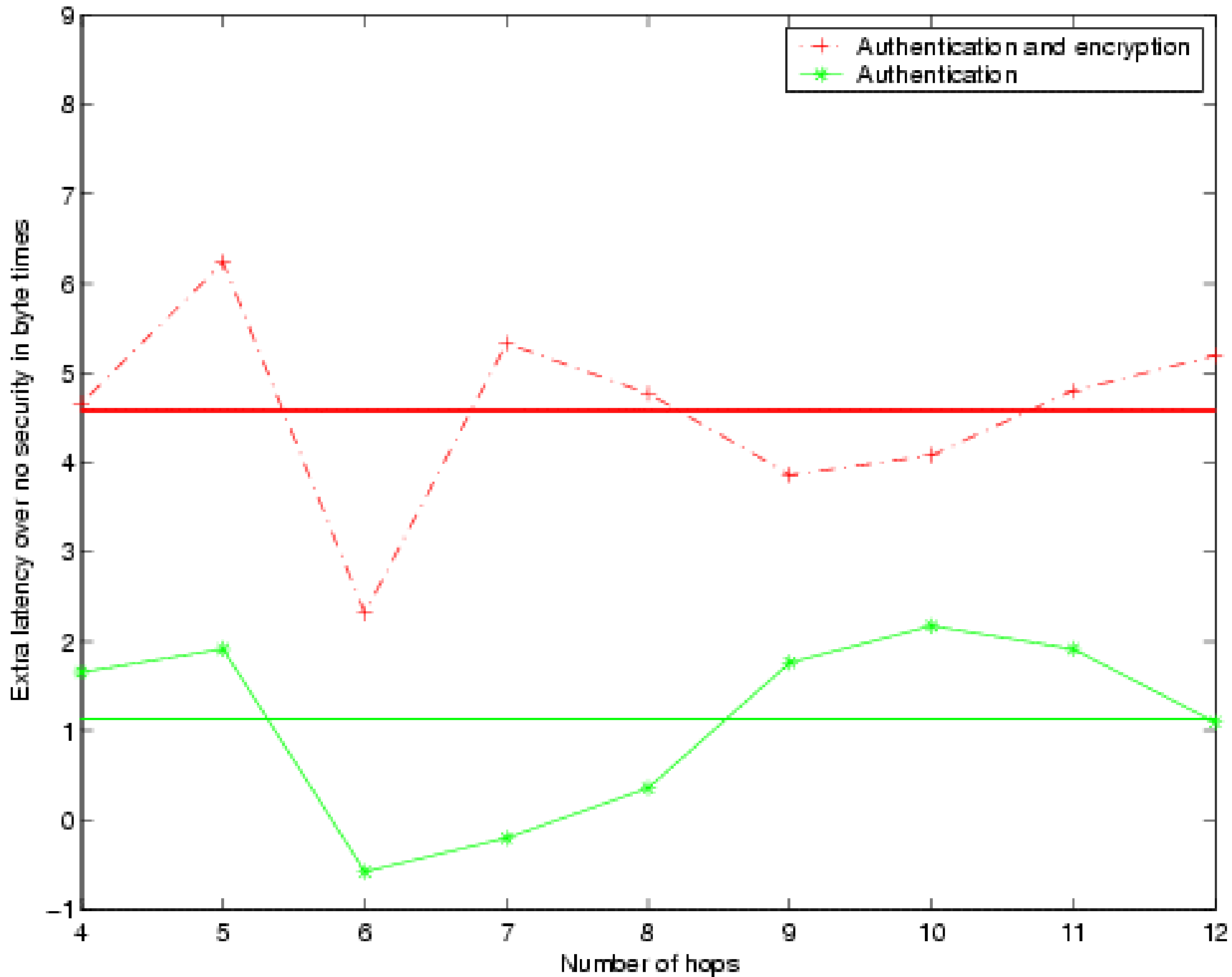
■ Test purpose:

- Measure latency at different hopcounts
 - Determine difficulty in adding TinySec to existing application
- ## ■ Integrate with SystemC
- ## ■ Successfully transmitted 70,000+ packets: Our stress test

Latency



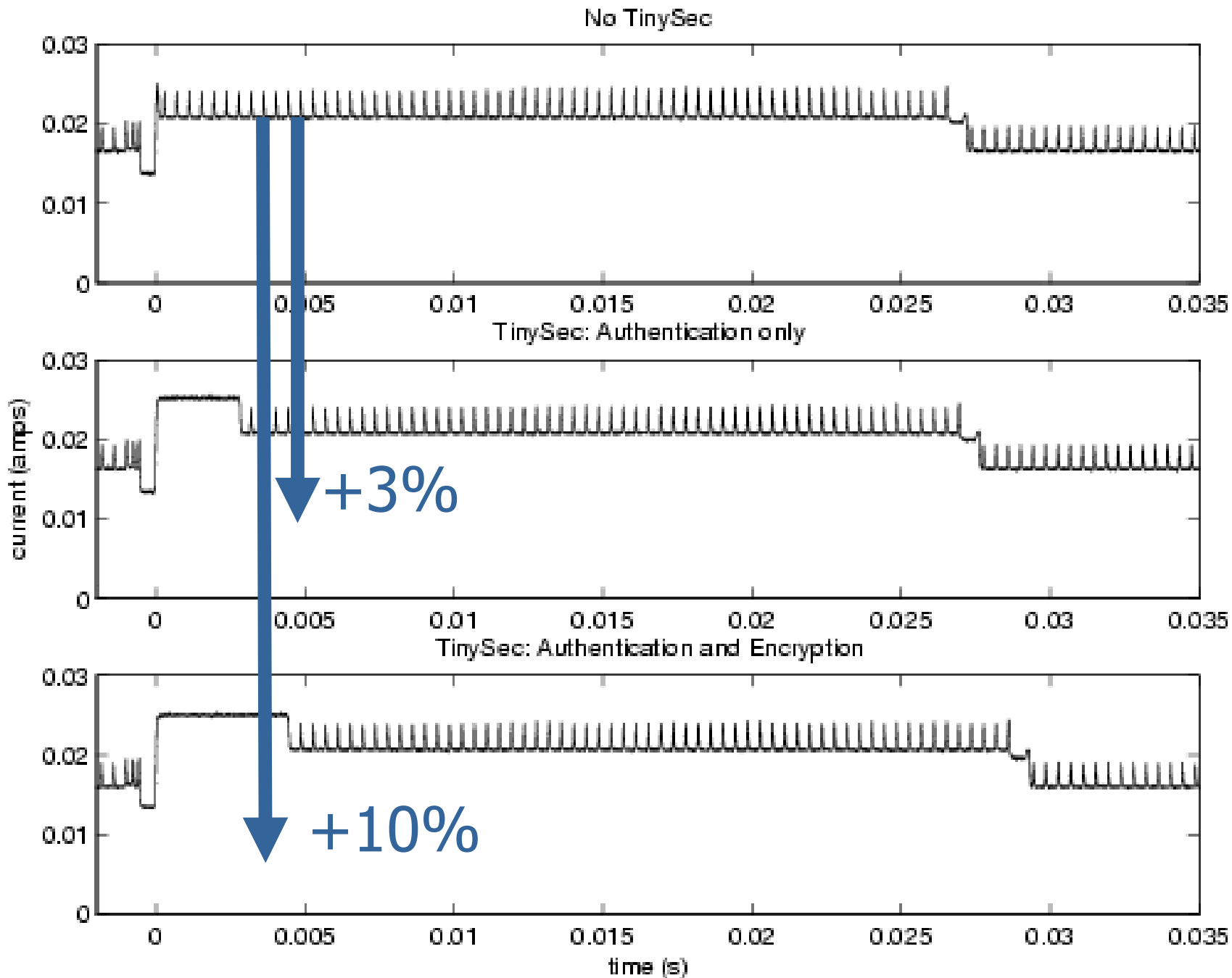
Latency: Byte Times



Energy Test Setup

- Single mote transmitting a packet
- Measure voltage drop with oscilloscope

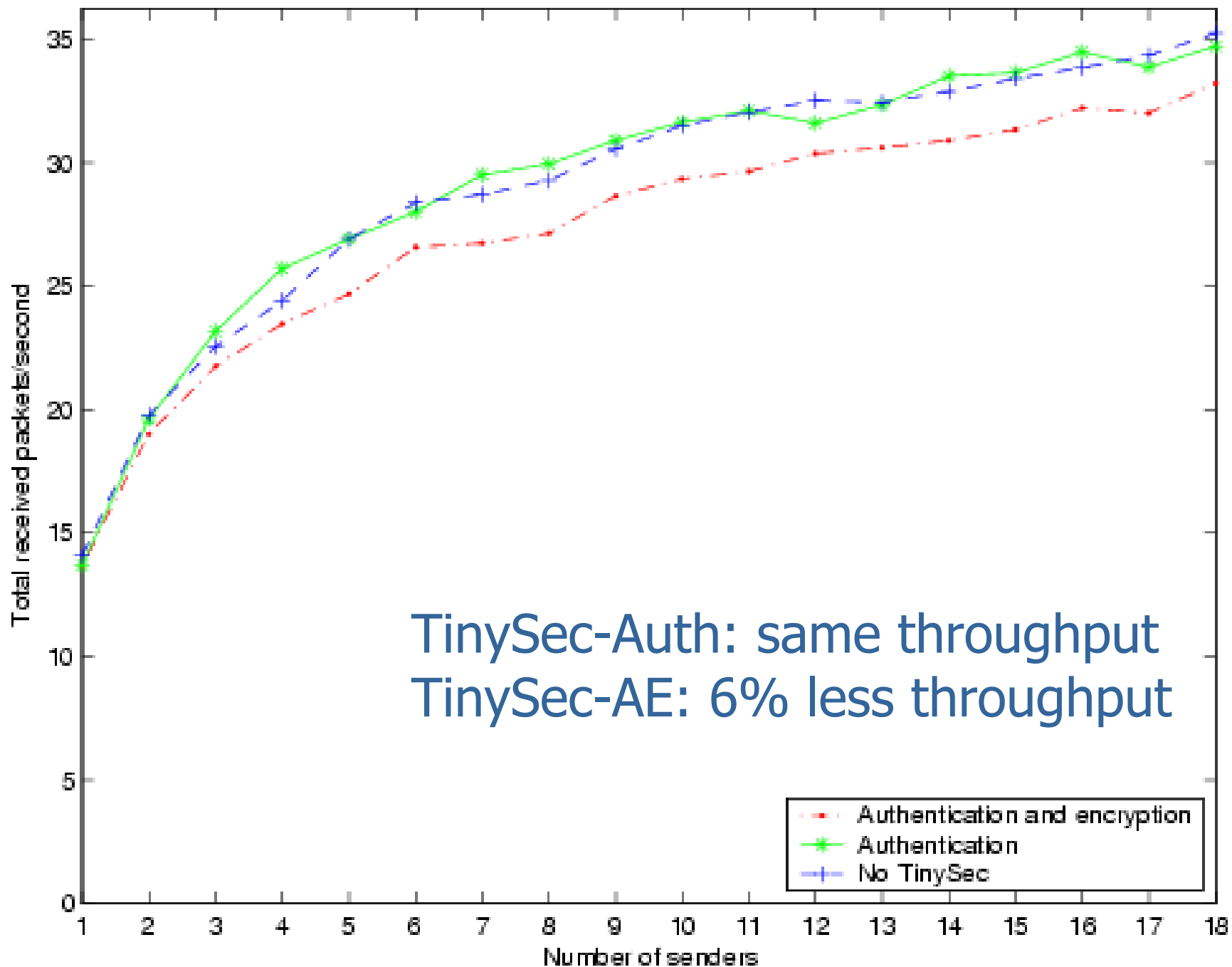
Energy



Bandwidth Test Setup

- Vary number of senders
- Each sender sends as fast as it can
- Measure number of packets successfully received in a time period

Bandwidth



TinySec-Auth: same throughput
TinySec-AE: 6% less throughput



Performance Summary

	Predicted (packet size only)	Latency Overhead	BW Overhead	Energy Overhead
CRC (No TinySec)	---	---	---	---
TinySec- Auth	1.5%	1.7%	Negligible	3%
TinySec- AE	8%	7.3%	6%	10%

TinySec Status

- New version working with 1.1.3 stack
- To use: TINYSEC=true
- Suggestion:
base new stacks off of TinySec stack

802.15.4



- New standard supported by ChipCon 2240.
- Link-layer security provisions
 - Key management left to higher protocols (ZigBee)
- Design similarities to TinySec:
 - 3 security modes: off, auth, auth + encryption (also include encryption only).
 - Block cipher based
 - 16 byte IV; format similar to TinySec format

802.15.4: (cont)

- Design differences to TinySec
 - Larger security parameter choices
 - Performance hit?
 - AES in hardware
 - MAC size variable, 0..16 bytes
 - Encryption: CTR mode
 - Encryption: 16 byte IV. Similar to TinySec Format

Conclusion

- Increased packet length dominant factor in overhead
- HW right long term solution
 - Ease
 - Energy savings
 - Faster block cipher ops, but not the right metric
 - But: requires design at chip time
- Hardware not needed for acceptable performance
 - Software Crypto is efficient and feasible
 - Relies on an underutilized CPU
 - Our implementation is low overhead

Acknowledgements

- D. Molnar for help in running the latency test
- R. Szewczyk for measuring the energy plots
- A. Woo for the key piece of Matlab trivia so we could write our scripts

802.15.4: IV Format

1 byte	8 bytes	4 bytes	1 byte	2 bytes
Flags	Source Address	Frame Counter	Key Sequence Counter	Block Counter

Table 7. IEEE 802.15.4 Nonce [1]