Tested on one PMU one PDC network

Original Packet:

16 phasors

Payload: 86 bytes

Total: 140 bytes

{PDC -> PMU: ANonce

PMU -> PDC: SNonce, AAD, MICPK(SNonce, AAD)

PDC <--> PMU: ENCSK(DATA)

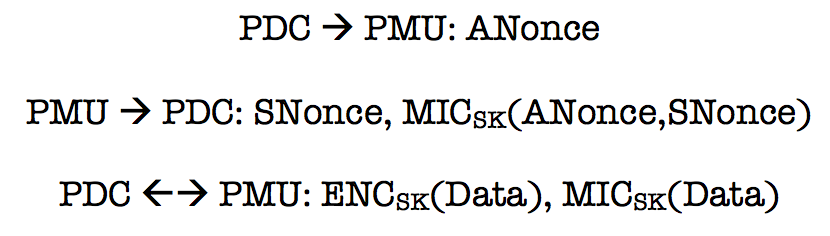
AES-GCM:

Packet length: 194 bytes

Communication overhead: 38.57%

encryption: 3164516 packets/min

decryption: 3981304 packets/min



CBC+HMAC:

Packet length: 318 bytes

Communication overhead: 127.14%

encryption: 954954 packets/min

decryption: 1057614 packets/min

ChaCha20+HMAC:

Packet length: 318 bytes

Communication overhead: 127.14%

encryption: 954954 packets/min

decryption: 1057614 packets/min

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Key size | Encryption Rate | Decryption Rate | Communication Overhead |
| AES-GCM | 256 bits | 54741 packets/s | 66355 packets/s | 19.77% |
| AES-CBC  +HMAC-SHA256 | 256 bits | 51503 packets/s | 50495 packets/s | 76.74% |
| ChaCha20  +HMAC-SHA256 | 256 bits | 41511 packets/s | 40198 packets/s | 86.04% |

Test setting: i7 2.2Ghz 16Gb Ram

Implementation: pyton