Secure Lossless Aggregation in Smart Grid M2M Networks

Authors: A. Bartoli, J. Hernández-Serrano, M. Soriano, M. Dohler, A. Kountouris and D. Barthel

Presenter: Vignesh Sridhar

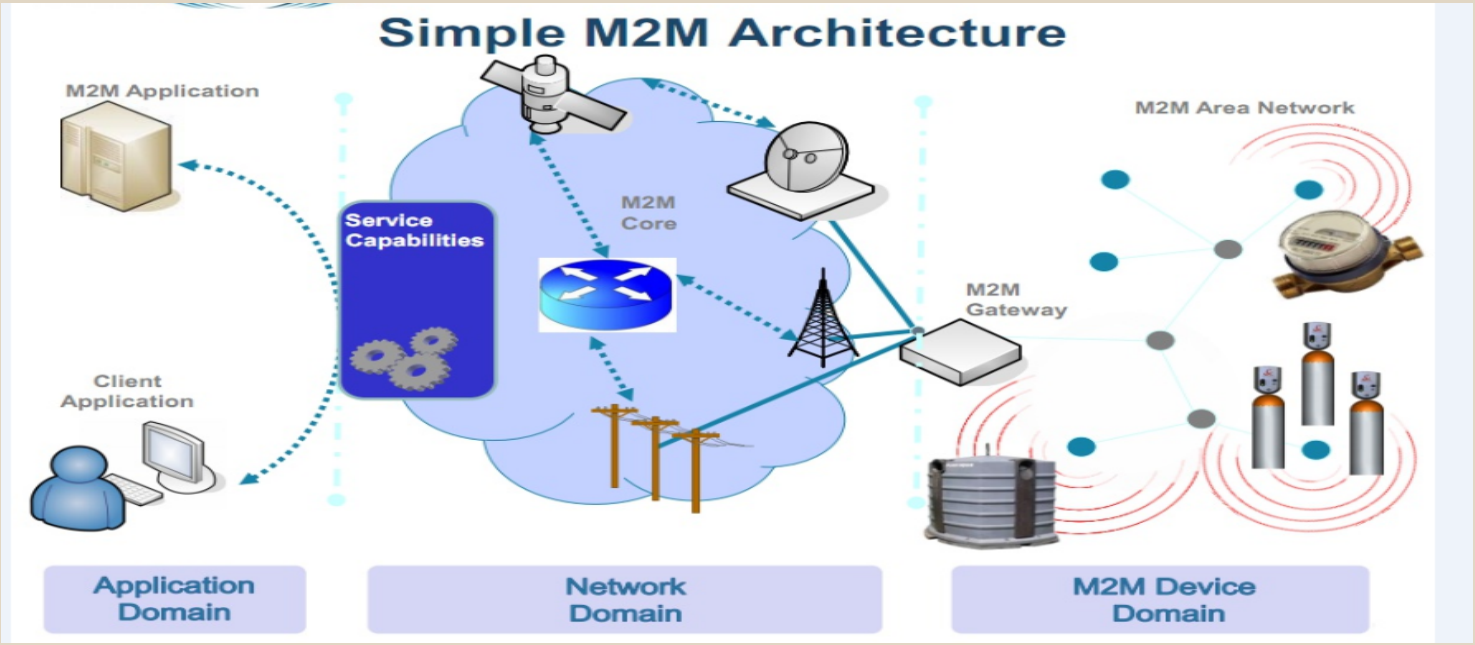
Submitted in Partial Fulfillment of the Course Requirements for
ECEN 689: Cyber Security of the Smart Grid
Instructor: Dr. Deepa Kundur

Overview

- Introduction to M2M Networks
- Description of design requirements
- Performance Analysis
- Critical assessment
- Conclusion

Introduction to Smart Grid M2M

- Machine networks are a suite of technologies that form a confluence of existing utilities with communication technology for enhanced application deployment



Model of a M2M Network, taken from (2)

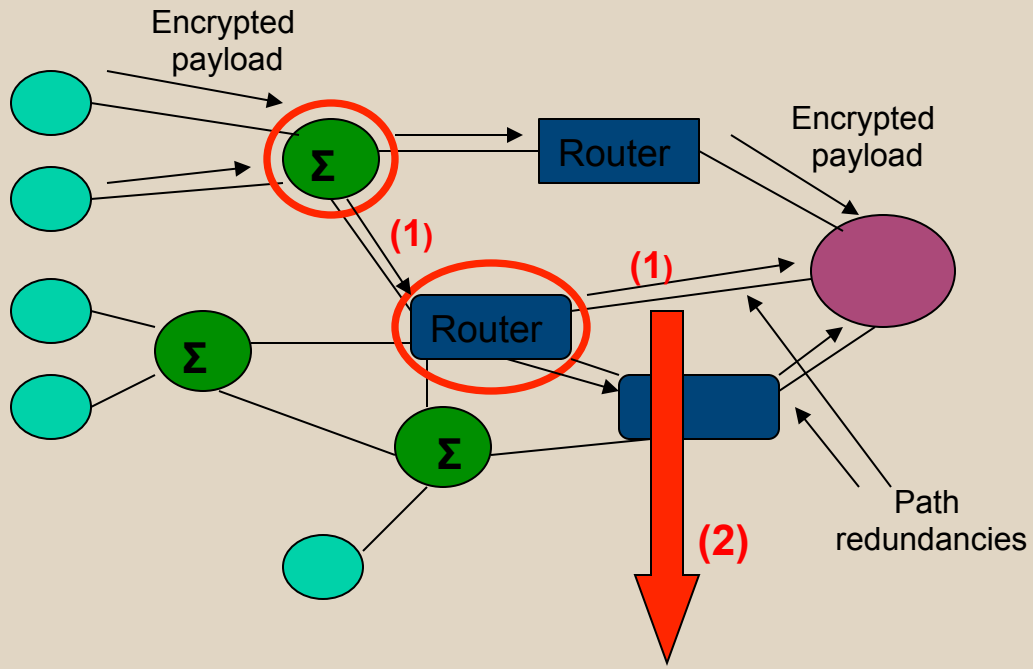
- Real time monitoring of system parameters & communicating with local devices
- New grid designs using wireless media for connectivity between control/base station and individual metering / actuating devices
- Wireless offers convenience in implementation and interfacing with smart devices

Introduction - Limitations

- Wireless media inherently insecure
  - Medium accessible to all users
  - Prone to data errors, retransmissions will be required
  - Strong encryption required
- Limited resources and end nodes/meters
  - Low power supply to network nodes
  - Hardware and software limitations (memory/hard drive space, encryption software, etc.)
  - Physical location of end device

Introduction – Problem Analysis

- High level of network security to prevent cyber attacks, ensure reliable un-corrupted data transmission
  - Ensure secure data transfer at application level (between end node and base controller)
- Link level data should not be tampered

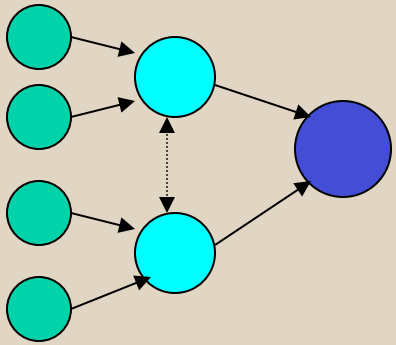


End-to-end encryption will encode only meter data/payload

(1) Packet is susceptible to attack as header and trailer are not encrypted, aggregator / router become targets of attacker

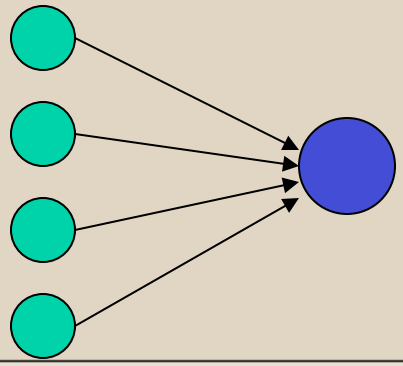
(2) Link becomes a vulnerability in network layout, attack can execute an attack to tamper with messages

- **Conserve power resources and grid nodes**
  - reduce dependence on end devices
  - place resources for critical operations at higher level / accessible devices
  - remove redundancies in data patterns



With aggregation,

1. Stored at summating node till buffer filled
2. Hierarchical transition as tree/graph structure
3. Routers/aggregators provide path redundancies
4. Time complexity = O (log n); O(E*logV) (for graph)



Without aggregation

1. Continuous data transmission of data to base station whenever available, ongoing power consumption
2. Time complexity = O (n), O(EV) (for graph)

Proposed Solution

Protocol implementing:

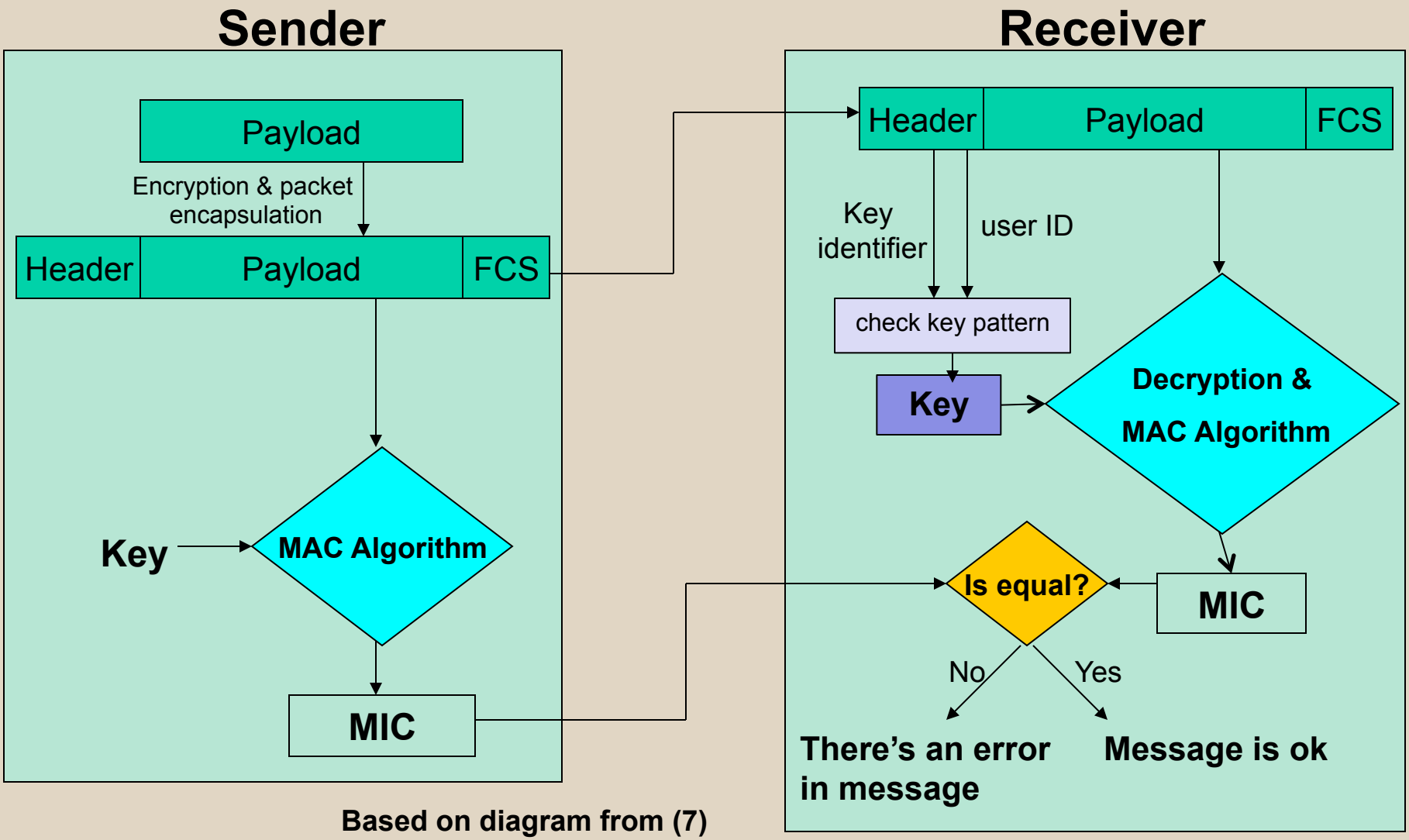
- Offer 2-tier security
  - End-to-end: encrypt data transmission between source (end meter) and destination (base station) – application level
  - Hop-by-hop: encrypt data transmission between every link in network, i.e. check key/identifier between node and its next hop – data link / medium access layer
- Reduce transmissions and storage and end nodes
  - Data aggregation: accumulate data from several nodes at single point (aggregator unit or larger sensor node)
  - Use store-forward mechanisms to pass data to next hop
  - Removal of redundant data during accumulation
  - Sends one long packet rather than several short packets

End-to-End Security

- Application layer encryption
- Security offered between source and destination only
- Encompasses CIA paradigm:
  - Protect **data** from interception, modification, etc. (C)
  - Check the order and correctness of received data (I)
  - Check the source of the data to verify originality (A)
- Data alone encrypted, header (source/destination IPs, timestamps, frame length, etc.) and trailer (frame check sequence) not encrypted
- Chance of exposure of details over wireless link, interception, modification or fabrication data detected only after transmission at receiver

- Packet structure:
  - source/destination IPs: end meter and base station IP addresses
  - timestamp: time of transmission of packet from sender through frame counter
  - Key identifier: along with the session key/user ID, will form a unique value to identify the key at recipient to decrypt that payload
  - Message Integrity Code (MIC): pattern of information agreed upon by sender and receiver, to ensure data is protected against tampering by verifying against MAC algorithm
  - Payload
- Parameters to check integrity & authenticity
  - Key identifier, which will define the key to use by recipient
  - MIC to check for any modification of data in packet
  - Timestamp to check freshness of data

Schematic Diagram



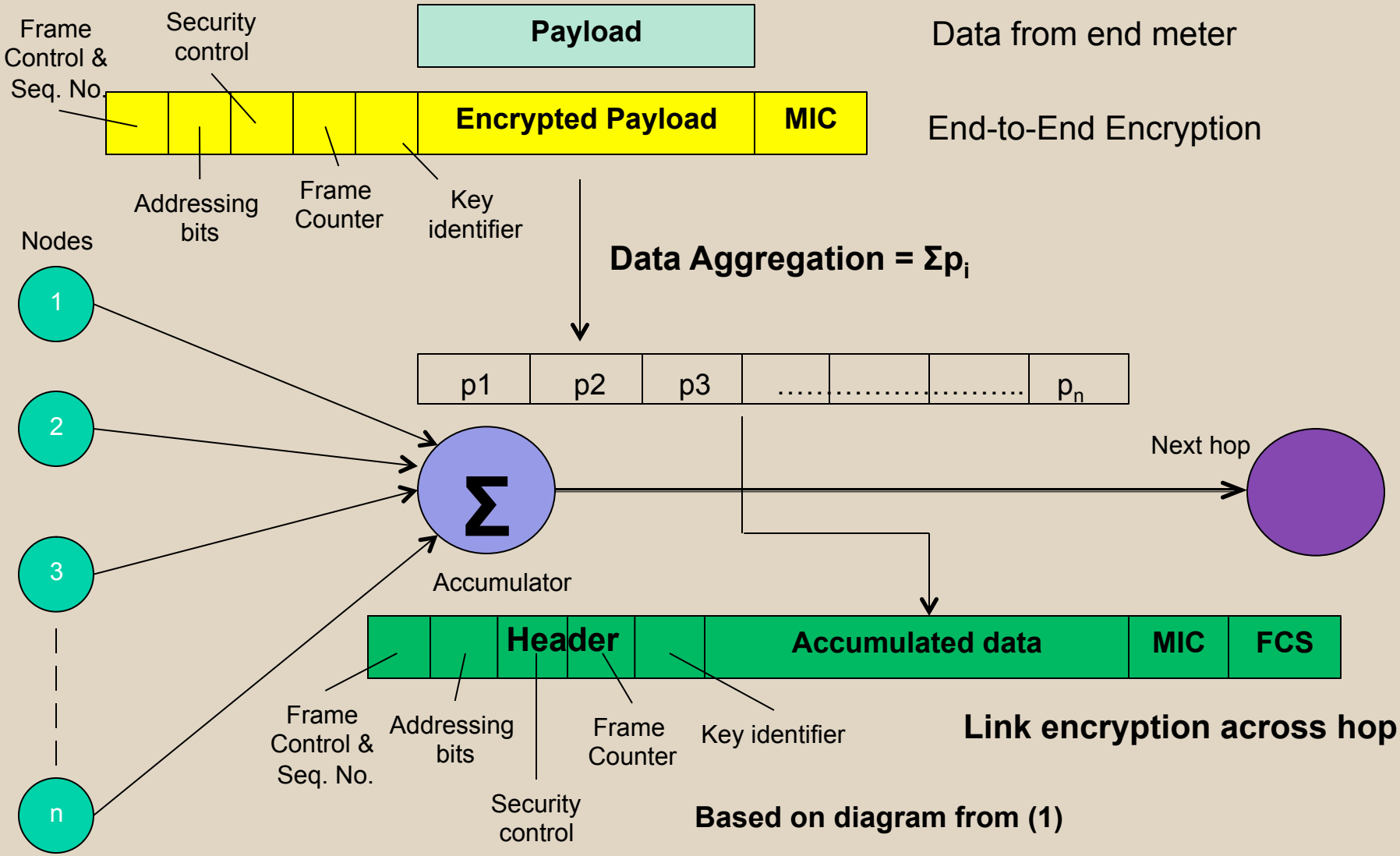
Based on diagram from (7)

Hop-by-Hop Security

- End-to-end security offers no encryption of header/trailers
- No protection at intermediate wireless links, data susceptible to attack at hops
- Aggregators need to forward data to other nodes in topology and verify correctness of data (else error increases over data accumulation)
- Need for :
  - checking data between hops to verify integrity and authenticity of data, rather than at end of transmission
  - Protect data at intermediate links from attack
  - **Conceal header and trailer information of source and destination**

- Data at one aggregator/router is encrypted again for link level protection.
- Use another set of MAC to check for inconsistencies in data
- A new key identifier is shared amongst all aggregators and routers to check correctness of data and MACs
- Packets are forwarded to next hop and decrypted by use of shared key identifier for link encryption
- Once destination is known and MAC is verified by algorithm, data is encrypted again and passed to next hop

End-to-end and Hop Security



Data Aggregation

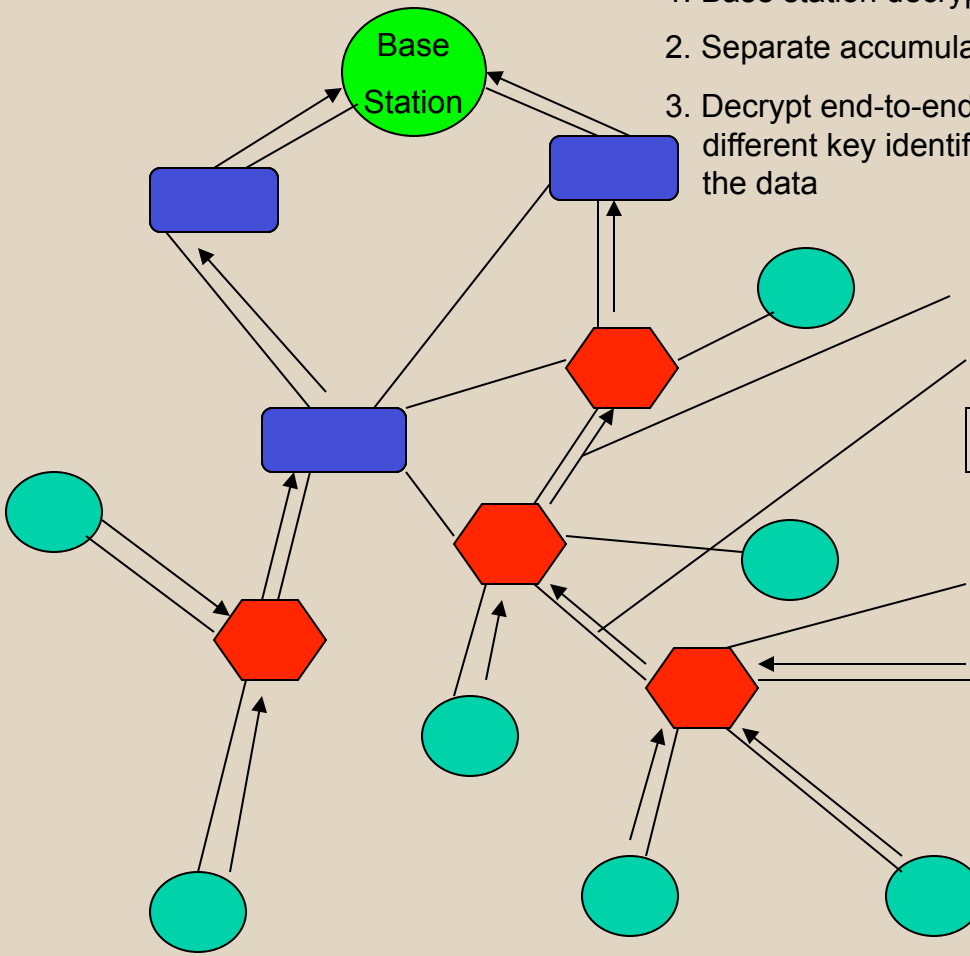
- Accumulate data from several nodes (meters) in the grid and sent newly concatenated packet (store – forward operation)
- Data packets of each node are concatenated at the aggregator, and forms new data payload
- Redundant data (like duplicate headers) are removed to reduce transmission load
- Accumulation of data goes till the payload capacity of aggregator is reached, or if last input packet is reached or at timeout, then send new packet to next node

Algorithm

```
osize=0; opacket_id=0; // initilaize output packet data
createopacket(opacket_id) // create new output packet
for every input packet from nodes connected to aggregator
  if MIC == TRUE then
    retrieve the MAC & payload data of input packet
    if osize > (payload buffer size of aggregator) then
     create header data (MIC, key identifier, etc.) for newly formed packet
     send the new packet
     reinitialize all output packet parameters for new transmission
    end if;
    osize = osize + sizeof(input_data); // accumulate data as long as aggregator buffer not full
    if (last packet received in session || TIMEOUT) then
     create new header (MIC, key identifier)/trailers for packet
     send output packet
    end if;
  end if;
end for;
```

Consolidating …….

1. Base station decrypts the link encrypted data, removes hop header & trailer
2. Separate accumulated meter data with algorithm or delimiters
3. Decrypt end-to-end encrypted data by use of agreed key; each meter(s), may have different key identifiers/session keys, identifying which key recipient uses to decrypt the data



Link encryption adds next level of encryption, new header, trailer added to accumulated payload; key identifier for link level encryption/decryption of packets at other nodes/routers

Header	Aggregator input (new payload)	MIC

Aggregator sums individual packets = Σ(input packets)

p1	p2	p3	p4

Data with end-to-end encryption (p_i)

Header	Payload	MIC

Node
Aggregator
Router

Summing up ……

- 2-level security makes wireless transmissions secure
  - End-to-end gives flexibility in choosing encryption techniques, encodes payload data and source without chance of access at intermittent nodes
  - Hop-by-hop ensures no attacks occur across any link on the network topology by checking packets between node and ist next hop, encrypting packet headers as well
  - Additional infrastructure required to place re-designed security
- Data accumulation
  - Reduces continuous transmissions through store-forward mechanism
  - Power savings in reduction in transmissions
  - Reduces buffer requirements on leaf nodes / end devices
  - Changes in infrastructure, re-allocate resources to aggregators

Performance Analysis

N – number of meters

OH_p – overhead at physical layer

OH_m – overhead at the MAC layer

OH_n – overhead at network layer

P_m – packets generated by meter

O = (number of meters / aggregated output)

$bytes_a = N(P_m\text{-}OH_p\text{-}OH_m) – O(OH_p+OH_m)$

$bytes_{na} = NP_m$

$bytes_{na} – bytesa = (N - O)(OH_p + OH_m)$

N	collected data (bytes)	P_m (bytes)	$bytes_{na}$	$bytes_a$	Δ (bytes)	Δ (%)
2	16	61	122	97 ($O = 1$)	25	20.49%
3	16	61	183	133 ($O = 1$)	50	27.32%
19	16	61	1159	859 ($O = 7$)	300	25.88%
31	16	61	1891	1391 ($O = 11$)	500	26.44%
53	16	61	3233	2358 ($O = 18$)	875	27.06%
97	16	61	5917	4353 ($O = 33$)	1564	26.43%

Table showing byte difference between aggregation &non-aggregation of data (1)

Assuming a lossless channel,

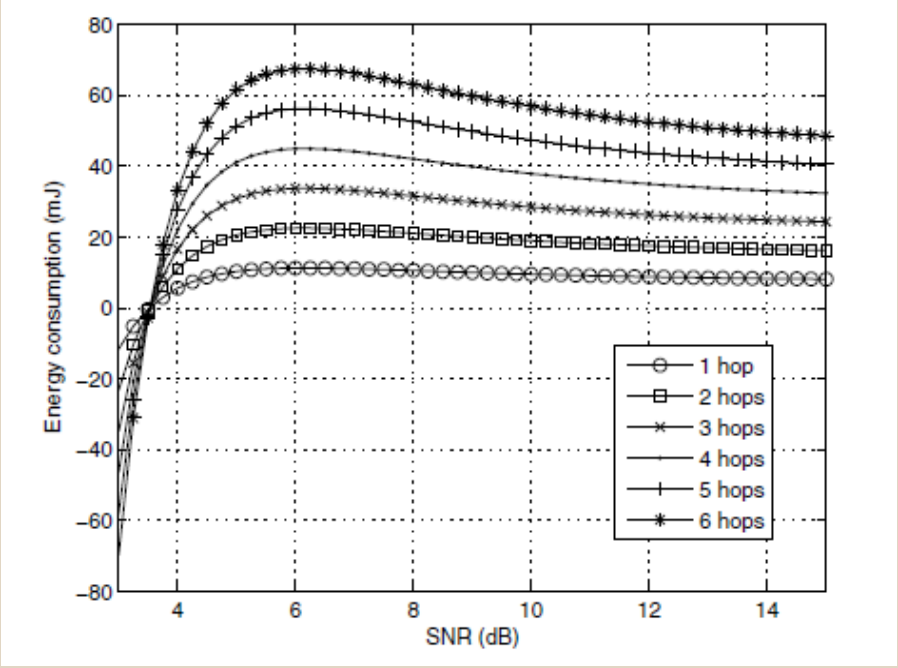
- Packet overhead translates to energy savings
- Average of 25-27% power savings for given data length
- Power savings offsets the additional cost in implementing revised security designs

Simulating over wireless channel

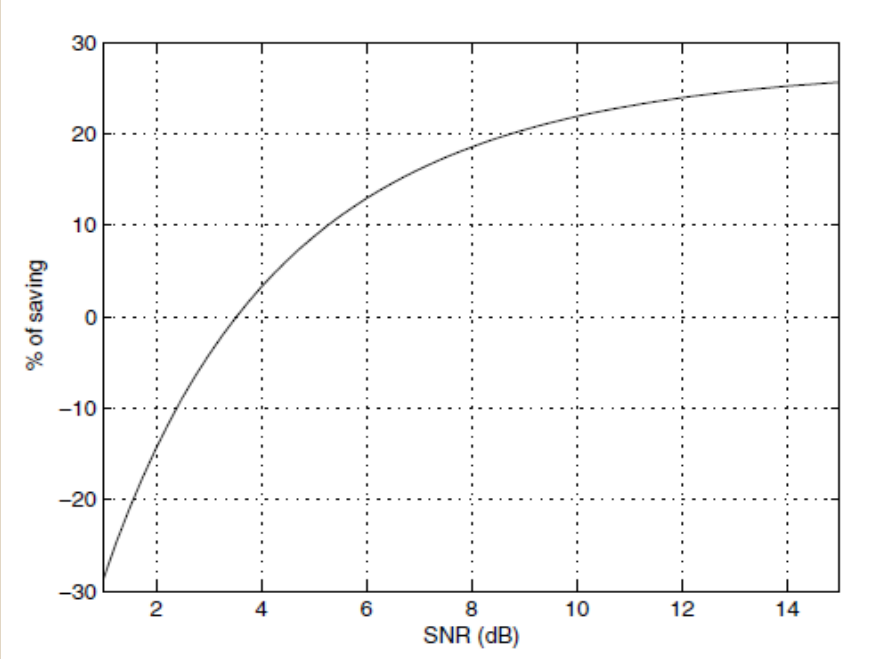
N	$OH_P + OH_M$ (bytes)	collected data (bytes)	SNR (dB)	$\overline{N_{tx}}$ w/o aggr.	$\overline{N_{tx}}$ with aggr.	Total tx bytes w/o aggr.	Total tx bytes with aggr.	Energy consumption w/o aggr. (mJ)	Energy consumption with aggr. (mJ)
3	21	16	0	100.77	207	18440.9	27531	2743.9	4096.6
3	21	16	5	4.3	5.4	786.9	718.2	117	106.868
3	21	16	10	1.586	1.7	290.238	226.1	43.19	33.6436
3	21	16	15	1.157	1.1836	211.731	157.41	31.5	23.422
2	21	32	0	124.93	201	19239.22	26545	2862.76	3949.896
2	21	32	5	4.6	5.35	708.4	690.15	105.41	102.672
2	21	32	10	1.62	1.7	249.48	219.3	37.12	32.63
2	21	32	15	1.165	1.1826	179.41	152.478	26.696	22.6887

Energy savings of with/without data aggregation w.r.t. to SNR values [1]

Graphs



Energy savings of data aggregation w.r.t. to SNR values for different hops[1]



Energy savings of data aggregation w.r.t. to SNR values [1]

Critical Assessment

- Paper offers simple, modular understanding of problem, requirements and approach to solution
- Good, basic algorithm designed for data aggregation
- Clear demarcation of security requirements for end-to-end connectivity and hop-by-hop
- Requires more depth in the interfacing/dependencies of security and power conservation techniques (1)
- More work to go into defining exact protocols/schemes used for end-to-end / link encryption (5)
- More information required on type of aggregation used based on network topology (tree, cluster, mesh, etc.) (4)

Conclusion

- Dual level security needed for reliable wireless transmissions
- Data aggregation helps in power savings within reasonable SNR values
- Additional costs involved in new protocol implementation are offset by power savings
- More work to make end-to-end and link encryption work together efficiently
- Scope for better choice of aggregation protocols for maximum packing of payload data

References

(1) ***"Secure Lossless Aggregation for Smart Grid M2M Networks***"; A. Bartoli, J. Hernández-Serrano, M. Soriano, M. Dohler, A. Kountouris, and D. Barthel at SmartGridComm 2010

(2) ***http://www.cardinalus.com/blog/tag/smart-grid/***

(3) ***"Network Security Essentials: Applications & Standards";*** William Stallings

(4) ***"Secure data aggregation in wireless sensor networks: A comprehensive overview"***; Suat Ozdemir, Yang Xiao

(5) ***"LHAP: A Lightweight Hop-by-Hop Authentication Protocol for Ad-Hoc Networks"*** ; Sencun Zhu, Shouhuai Xu, Sanjeev Setia, and Sushil Jajodia

(6) ***End-to-end vs. Link Encryption***; Knol Beta (http://knol.google.com)

(7) *http://en.wikipedia.org*