Secure routing in IoT networks with SISLOF

Ayman El Hajjar[1,*], George Roussos[1], Maura Paterson[2]

[1] Department of Computer science and Information systems

[2] Department of Economics, Mathematics and Statistics

Birkbeck University of London, UK

a.elhajjar@bbk.ac.uk - @azelhajjar

June 8, 2017

Outline

- Litterature Review
- Routing protocol for Low Power and lossy networks (RPL)
- Shared Identifier Secure Link Objective Function (SISLOF) Rationale
- SISLOF Objective Function : How does it work
- Message and Modifications
- TestBed: Experiment Design
- TestBed: Experiment parameters
- SISLOF Rationale (Previous experiments Results)
- SISLOF Performance Results
- Sumnary and Further Work

Litterature Review

1. Internet of Things networks properties are similar to DSN and WSN
2. DSN and WSN Security with Eschenauer and Gligor key pre-distribution scheme:
   - Probability of 50% for nodes [1] in the network to share keys is enough to guarantee full secure network connectivity.
3. Conventional routing protocols are not suitable for the Internet of Things.
4. The Routing Protocol for Low-Power and Lossy Networks (RPL) is a distance vector IPv6 routing protocol optimized for the IoT networks.
   - RPL organises its topology in a Directed Acyclic Graph (DAG).
   - Only nodes that are in the DAG can communicate with each other.

[1] Stirling approximation

Routing protocol for Low Power and lossy networks (RPL)

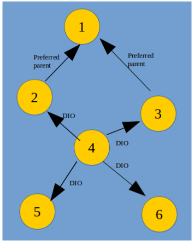


Figure: Mote 4 sends a DIO multicast message to all neighbours (candidate parents)

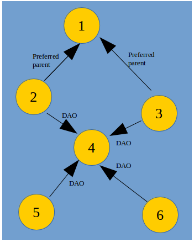


Figure: All motes that received the DIO message reply with a unicast DAO message

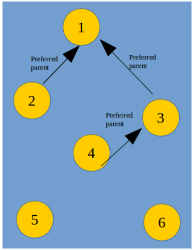


Figure: Mote 4 decides on which mote will be the preferred parent

RPL routing table formation. Mote 4 choosing a preferred parent.

Shared Identifier Secure Link Objective Function (SISLOF) Rationale

- Many of the available standards and protocols for conventional IP based networks are not suitable for the internet of Things networks
  - Eschenauer and Gligor key pre-distribution algorithm on IoT networks does not achieve full connectivity when applied on IoT networks using RPL and same ring sizes as DSN.

Shared Identifier Secure Link Objective Function (SISLOF) Rationale

- Many of the available standards and protocols for conventional IP based networks are not suitable for the internet of Things networks
  - Eschenauer and Gligor key pre-distribution algorithm on IoT networks does not achieve full connectivity when applied on IoT networks using RPL and same ring sizes as DSN.
  - To achieve full connectivity using the Eschenauer and Gligor keys pre-distribution Algorithm, much larger key rings were needed.

Shared Identifier Secure Link Objective Function (SISLOF) Rationale

- Many of the available standards and protocols for conventional IP based networks are not suitable for the internet of Things networks
  - Eschenauer and Gligor key pre-distribution algorithm on IoT networks does not achieve full connectivity when applied on IoT networks using RPL and same ring sizes as DSN.
  - To achieve full connectivity using the Eschenauer and Gligor keys pre-distribution Algorithm, much larger key rings were needed.
    - For a $100\,000$ motes network a $4\,600$ keys in the ring will be needed to achieve full connectivity.

Shared Identifier Secure Link Objective Function (SISLOF) Rationale

Birkbeck UNIVERSITY OF LONDON

- Many of the available standards and protocols for conventional IP based networks are not suitable for the internet of Things networks
  - Eschenauer and Gligor key pre-distribution algorithm on IoT networks does not achieve full connectivity when applied on IoT networks using RPL and same ring sizes as DSN.
  - To achieve full connectivity using the Eschenauer and Gligor keys pre-distribution Algorithm, much larger key rings were needed.
    - For a $100\,000$ motes network a $4\,600$ keys in the ring will be needed to achieve full connectivity.
    - Each mote has 90 kb of memory storage.

Shared Identifier Secure Link Objective Function (SISLOF) Rationale

- Many of the available standards and protocols for conventional IP based networks are not suitable for the internet of Things networks
  - Eschenauer and Gligor key pre-distribution algorithm on IoT networks does not achieve full connectivity when applied on IoT networks using RPL and same ring sizes as DSN.
  - To achieve full connectivity using the Eschenauer and Gligor keys pre-distribution Algorithm, much larger key rings were needed.
    - For a $100\,000$ motes network a $4\,600$ keys in the ring will be needed to achieve full connectivity.
    - Each mote has 90 kb of memory storage.
    - 54 kb of this will be used for rings storage (identifiers and keys).

Shared Identifier Secure Link Objective Function (SISLOF) Rationale

- Many of the available standards and protocols for conventional IP based networks are not suitable for the internet of Things networks
  - Eschenauer and Gligor key pre-distribution algorithm on IoT networks does not achieve full connectivity when applied on IoT networks using RPL and same ring sizes as DSN.
  - To achieve full connectivity using the Eschenauer and Gligor keys pre-distribution Algorithm, much larger key rings were needed.
    - For a $100\,000$ motes network a $4\,600$ keys in the ring will be needed to achieve full connectivity.
    - Each mote has 90 kb of memory storage.
    - 54 kb of this will be used for rings storage (identifiers and keys).
    - Motes took on average 23 seconds to compute and compare larger rings and used 87% of the processing power.

Shared Identifier Secure Link Objective Function (SISLOF) Rationale

Birkbeck UNIVERSITY OF LONDON

- Many of the available standards and protocols for conventional IP based networks are not suitable for the internet of Things networks
  - Eschenauer and Gligor key pre-distribution algorithm on IoT networks does not achieve full connectivity when applied on IoT networks using RPL and same ring sizes as DSN.
  - To achieve full connectivity using the Eschenauer and Gligor keys pre-distribution Algorithm, much larger key rings were needed.
    - For a $100\,000$ motes network a $4\,600$ keys in the ring will be needed to achieve full connectivity.
    - Each mote has 90 kb of memory storage.
    - 54 kb of this will be used for rings storage (identifiers and keys).
    - Motes took on average 23 seconds to compute and compare larger rings and used 87% of the processing power.
  - Eschenauer and Gligor key pre-distribution algorithm on IoT is not feasible without any modification.

SISLOF Objective Function : How does it work

Birkbeck UNIVERSITY OF LONDON

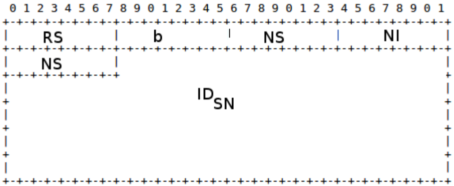
How does SISLOF achieve this:

1. Motes select random rings (keys and identifiers)
2. DIO messages send downward to all neighbours.
   - The number of DIO messages defer depending on the number of identifiers in the ring.
   - Each time a mote receive a DIO message, it consider the originator of the message a "candidate parent"
   - It compares its own identifier ring with the identifier ring embedded in DIO message
3. For each DIO message, the receiver mote replies back with a DAO message informing the sender if they will be chosen as a preferred parent
   - If yes: Which identifier they have in common?
   - If no: The mote cannot be a preferred parent $\Longrightarrow$
     - No shared identifier
     - Shared identifier exist but another more will be chosen as preferred parent.

Message and Modifications

- Addition to the DODAG Information Object (DIO) message:
- 1 byte for each of the variables
    - Ring Size (RS)
    - Identifier size (b)
    - Number of identifiers in one message (NI)
    - Number of Sequence (NS)
    - Sequence Number (SN)
- ID SN for the number of identifiers sent in the message.
    - 33 bytes in the payload remain for sending identifiers from the ring.

Addition to the DIO message



Message and Modifications

- Addition to the Destination Advertisement message (DAO) message:
  - 1 byte for Sequence Number (SN)
  - 1 byte for Number of identifiers in one message (NI) where the bitmap representing shared identifiers bits.

Addition to the DAO message.

```
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     SN        |       NI*            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

TestBed: Experiment Design

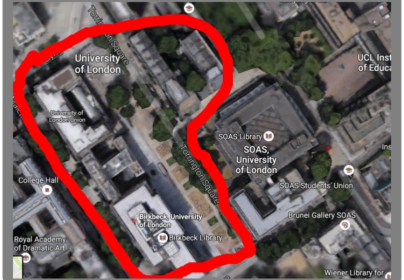
Independent variables

- Pool size & Number of motes $(100, 250, 500, 750, 1000, 2500)$
- Ring size (8,13,18,22,25,41)

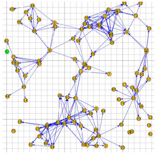
Control Variables

- 64 bits key.
- 32 bits identifier.
- $250m^2$ simulation area - similar to the university campus area.
- 5 runs for results consistency.

Simulation environment



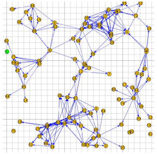
TestBed: Experiment Parameters



Experiment Platform

- Zolertia Z1 motes were used.

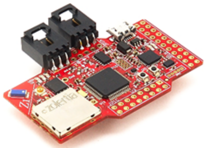
TestBed: Experiment Parameters



Experiment Platform

- Zolertia Z1 motes were used.
  - 90 Kb memory storage
  - 50 meters transmitting range
- Contiki OS for the 6LoWPAN stack (RPL, CoAP, ContikiMAC).
- Cooja Simulator

Zolertia Z1 low-power wireless module for IoT and WSN



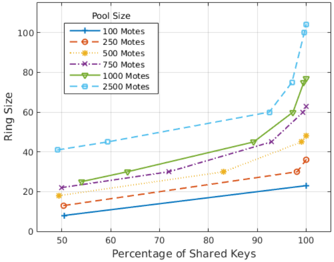
SISLOF Rationale (Previous experiments Results)

1. Key pre-distributed for DSN on IoT
2. Larger key ring size to achieve full connectivity

Pool Size	DSN	IoT
100	8	23
250	13	36
500	18	48
750	22	63
1000	25	77
2500	41	104

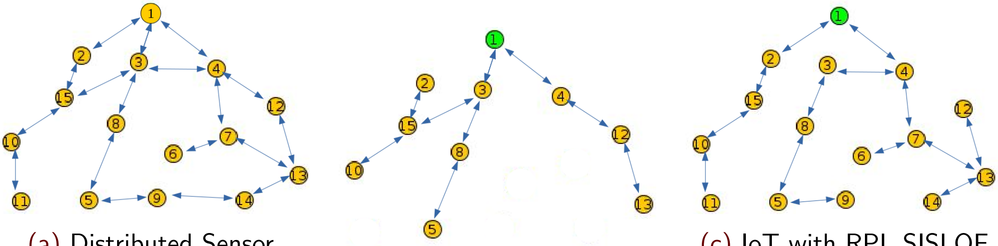
DSN ring sizes vs. IoT ring sizes to achieve full connectivity.

Ring Size vs. % of Number of DAGs with a shared key until 100% is achieved.



SISLOF RESULTS - Topology comparison

- All motes participate in the network in comparison with RPL using OF0 where note all motes



(a) Distributed Sensor Network

(b) IoT with RPL OF0

(c) IoT with RPL SISLOF Objective Function

Figure: Network Topology as seen for various implementation

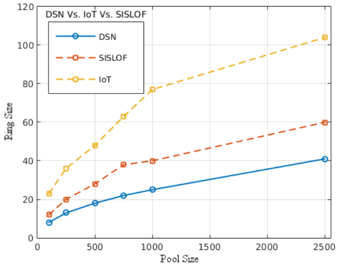
SISLOF RESULTS - Ring size comparison

Birkbeck UNIVERSITY OF LONDON

- **Decrease** in the number of keys/identifiers needed in the ring.

Table: Results Comparison: Number of motes N, Shared Keys SK (100% for IoT), Ring Size (RS)

	DSN		IoT OF0	IoT SISLOF
N	RS	SK %	RS	RS
100	8	50.52	23	12
250	13	50.43	36	20
500	18	57.14	48	28
750	22	49.47	63	38
1000	25	57.14	77	40
2500	41	48.19	104	60



IoT SISLOF performance in comparison with DSN and IoT network (RPL with OF0)

Summary and Further Work

- **Summary**
  1. **Validated** that SISLOF provide **full connectivity** of the network while maintaining a smaller ring size for all motes within reach.
  2. **Validated** that modifications of SISLOF **do not add** a large overhead on RPL messages
  3. **Convergence of secure routing table** occured without the exchange of the keys.
  4. **Decreased** the storage size of the ring for 100,000 motes network from 54Kb to 28.8 Kb.
  5. **Keys** are not transmitted in any message. Only **identifiers** are transmitted.
- **Further work**
  - Investigate mobility impact on SISLOF
  - Analyse overhead and changes SISLOF add to PRL in term of:
    - Number of hops
    - CPU usage
    - Duration for Routing table to converge
    - Number of exchanged control messages

Thank you