**Secure routing in IoT networks with SISLOF**

**El Hajjar, A., Roussos, G. and Paterson, M.**

This is a copy of the author’s accepted version of a paper subsequently published in the proceedings of the *Global IoT Summit,* Geneva, Switzerland, 6 to 9 June 2017.

It is available online at:

https://dx.doi.org/10.1109/GIOTS.2017.8016278

# Secure routing in IoT networks with SISLOF

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

[1]Department of Computer Science and Information Systems
[2]Department of Mathematics, Economics and Statistics
Birkbeck, University of London, London, UK
Email: [a.elhajjar, g.roussos, m.paterson] @bbk.ac.uk

***Abstract*—In this paper, we propose a modification of the RPL routing protocol by introducing the SISLOF Objective Function ensuring that only motes that share a suitable key can join the RPL routing table. This will ensure that all IoT network motes connect in a secure method. SISLOF uses the concept of key pre-distribution proposed by Eschenauer and Gligor in the context of the Internet of Things. First, we discuss related work that provide evidence that the key pre-distribution scheme in the context of the IoT with default RPL metrics fails to achieve the full network connectivity using the same ring size, however full time connectivity can be achieved but with a great cost in term of the large rings sizes. We introduce the SISLOF Objective Function and explain the modification it does to the RPL messages (DIO and DAO). We finally show the performance of the key pre-distribution in the context of the Internet of Things when SISLOF is used as the Objective Function of the RPL routing protocol.**

***Keywords*-Internet of Things; Security; RPL; Objective Function;**

## I. Introduction

The Internet of Things (IoT) consists of things that are connected to the Internet, anytime, anywhere. It integrates sensors and devices into everyday objects that are connected to the Internet over fixed and wireless networks.

The Internet of Things will be made possible by using IP based network such as the IPv6 Low Wireless Personal Area Network (6LoWPAN). It is a simple low cost communication network that allows wireless connectivity in applications with limited power and relaxed throughput requirements [1]. The 6LoWPAN concept originated from the idea that "the Internet Protocol should be applied to low-power devices to participate in the Internet of Things [2].

The purpose of this paper is to propose an Objective Function (OF) called Shared Identifier Secure Link OF (SISLOF) for the Routing Protocol for Low Power and Lossy Networks that only adds to its routing table motes that share a key and thus can securley communicate.

The distribution of the keys to be used by SISLOF is based on Laurent Eschenauer and Virgil D. Gligor's Algorithm [3] for Distributed Sensor Networks (DSN). We implement it in the context of 6LoWPAN Devices for the IoT. We provide an analysis of the performance of the SISLOF. We also compare its performance with the performance of the key pre distribution algorithm in the context of IoT with the default RPL routing metrics and in the context of DSN.

Section 2 provides an introduction to the Internet of Things, the 6LoWPAN network protocol, the IPv6 Routing Protocol for Low Power and Lossy Networks (RPL) and several solutions that attempts to secure the Internet of Things. Section 3 presents the key pre-distribution algorithm by Eschenauer and Gligor in [3] in the context of IoT when using the minimum ETX value (Default RPL metric) as in [4]. In section 4, we present the proposed SISLOF OF. In section 5 we provide an overview of the experiments setup and parameters used. In section 6 we provide an evaluation of the performance of SISLOF and how it compared with previous experiments. Finally, we present our main conclusions in Section 6.

## II. Background Literature

Routing is a fundamental piece of the overall IPv6 architecture for the Internet of Things, and the Routing Protocol for Low Power and Lossy Networks, standardised as the the IPv6 routing protocol, is designed for large scale implementation of IPv6 in harsh environments that will translate the potential of Internet of Things into reality [5].

RPL organises its topology in a Directed Acyclic Graph (DAG). An RPL DAG must have at least one RPL root and a Destination Oriented DAG (DODAG) is constructed for each root. The root acts as a sink for the topology by storing all routes to all motes in the DODAG in the routing table [6]. For a DODAG to be constructed, the root will need first to broadcast a DODAG Information Object (DIO) message to all motes. The DIO message contains the DAG Metric Container option that is used to report metrics along the DODAG. Multiple metrics can be defined by an OF [6].

The OF is identified by an Objective Code Point (OCP) within the DIO Configuration option. An OF defines how motes translate one or more metrics and constraints, which are themselves defined in [7], into a value called Rank, which approximates the mote's distance from a DODAG root in term of the number of hops it needs to reach it. An OF also defines how motes select parents. When a new DIO is received, the OF that corresponds to the Objective Code Point (OCP) in the DIO is triggered with the

978-1-5090-5873-0/17/$31.00 ©2017 IEEE

content of the DIO. For example, OF0 [8] is identified by OCP0 by the Internet Assigned Numbers Authority (IANA). The Minimum Rank with Hysteresis Objective Function (MRHOF) [9] is another OF defined by IANA and given the identifier OCP1.

Security specifically is a major issue as IEEE802.15.4 mandates link-layer security based on AES, but it omits any details about topics like bootstrapping, key management, and security at higher layers.

Security is Providing key management for confidentiality and group level authentication in a sensor network. The main challenge in public key algorithms when using in the context of Internet of Things, similarly to sensor networks, is the energy consumption of exchanging public key certificates [10] [11].

Key management protocols can be divided into three categories. Arbitrated keying protocols, Self Enforcing protocols and Pre-Deployed Keying protocols. Arbitrated keying protocols such as [12] and [13] are not suitable in the context of the Internet of Things because of the capabilities of sensor motes and leave the network vulnerable to man in the middle attacks. Self Enforcing protocols such as [14] to secure IoT was suggested to provide a lighter and robust security protocol using pairwise key establishment between motes however the communication overhead was considerably large. In the next section we show how the management scheme for Distributed Sensor Networks (DSN) proposed by Eschenauer and Gligor in [3] was used in the context of the IoT with the default RPL routing metric, the minimum ETX.

## III. Previous Work

### A. Key pre-Distribution Scheme

Offline Key pre-distribution algorithm for DSN proposed in [3] describes the method by which keys are distributed to motes in the network. This key pre-distribution mechanism ensures that for each direct link between any two motes in the network, the probability of those two sharing at least a key is $0.5$. Using Stirling approximation, the authors of [3] concluded that the size of key rings $KR$ does not need to be large in order for a network to guarantee full connectivity and only $50\%$ of those motes need to have a shared key. An example in [3] showed that when a pool contained $100\,000$ keys, full network connectivity was achieved with only 75 keys in the rings.

This scheme was used in [4] in order to determine if it produces full connectivity in the context of the Internet of Things.

1) A large pool $P$ of keys $K$ are generated with their identifiers $ID$.
2) The Ring Size $RS$ is equal for both keys rings $KR[RS]$ and identifiers rings $IR[RS]$.
3) Each identifier in $ID[RS]$ is of size $b$ bits.
4) A mote send its identifier $IR_s$ to another mote to establish if common identifiers exist with the receiver's identifier ring $IR_r$.
5) If a common identifier is found, the receiver sends back an acknowledgement with the identifier number i.e. "$ID_s[3]''$ to represent the third identifier in the identifier ring of the sender $ID_s$.
6) Once the sender receives the acknowledgement containing the common identifier found, a secure link is established using the key related to the identifier.

### B. Performance of the Key Pre distribution Scheme in the context of the IoT with RPL using the Minimum ETX metric

Following the simulation of the Key Pre-distribution Scheme in [11] in the context of the Distributed Sensor Networks and using the minimum ETX value as the RPL metric to choose the preferred parent, the results of the simulation experiments showed that out of each pool used, only half of the leaves in the routing table shared a key. The other half was excluded from the RPL routing table. For example, the percentage of motes in the DODAG that has a shared key was $54.01\%$ when the ring size $RS$ was 25 keys in a pool $P$ that contained a 1000 keys and a network of 1000 motes. Only when the ring size was increased to 77 keys that the full network connectivity was achieved and all motes in the network were included in the RPL routing table.

## IV. SISLOF

The Shared Identifier Secure Link Objective Function (SISLOF) is our proposed OF to find secure links (those that share an identifier) between any mote and all of its candidate parents to form a secure RPL routing table while minimising the number of motes that are excluded because of insecure links.

SISLOF will attempt to find shared keys between motes by using the Key pre-distribution algorithm for Distributed Sensor Networks proposed in [3]. This will allow the formation of an RPL routing table that only contains secured links between motes.

### A. Aims and Objectives

The aim of SISLOF is to create a secure RPL routing table with as many motes as possible. Specifically, its objectives are:

- Only motes that share a key can become a leaf in the DODAG tree.
- Nodes that do not share a key with their selected parent will discard this selection and try to form a leaf with one of the other motes that received its DIO (Neighbouring motes).
- If one mote shares a key with two or more motes, it will select as the preferred parent the mote that has a better ETX value in order to form the leaf between the two motes.

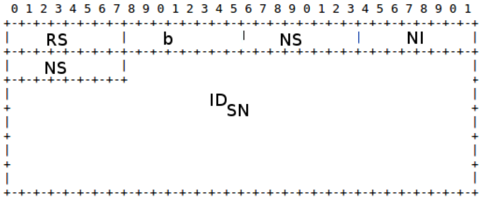


Figure 1. Addition to the DIO message: 1 byte for each of the variables, Ring Size (RS),identifier size (b), Number of identifiers in one message (NI) , Number of Sequence (NS) and Sequence Number (SN). $ID_{SN}$ for the number of identifiers sent in the message.

### B. SISLOF Metrics

SISLOF uses two types of metrics in its process to compute the preferred parent for a mote. First it uses our new mote metric object called Shared Identifiers State (SIS) to compare two arrays of identifiers in order to determine if one or more shared identifier exist.

If the mote that received the DIO determines that it shares one or more identifiers with two or more motes, that mote will need to choose which of the motes that sent the DIO will be selected as the preferred parent. SISLOF will thus need to decide between the motes it shares a key with. This will require SISLOF to use a link metric object as a second criterion in order to select the preferred parent. SISLOF will use the ETX Reliability object to select the preferred parent. The ETX value is calculated for each link from which a DIO message was received and with which it shares one or more identifiers. The mote that has the lowest ETX value will be selected as the preferred parent. The ETX is the number of transmissions the mote expects to make to a destination in order to successfully deliver the packet. This will also require changing the ‘A’ field of the header to 7 for each message (this field is given to indicate that the header will report a minimum or a maximum) [7].

Below is an explanation of the RPL messages modifications to incorporate the metrics required for the Key pre-distribution scheme by Eschenauer and Gligor in [3] as proposed by [4].

### C. Message and Modifications

SISLOF will require the modification of the DIO and DAO RPL messages in order to encapsulate the various variables of SISLOF required to exchange identifier rings and look for a common one. Those variables will be either encapsulated in the DIO message sent to a mote or in the DAO message replying.

SISLOF variables shown in Fig. 1 and explained in Table I are composed mainly of identifiers and other values related to the segmentation of those identifiers. To incorporate the SISLOF variables shown in Table I in a DIO message, the 6LoWPAN message, the ICMPv6 control message and the DIO base object requires 89 bytes [15] which implies that there are 38 bytes in the data frame to be used to embed in frame variables related to SISLOF . In Fig. 1 $RS$ and $b$ are selected to fulfil requirements of the algorithm of [3]. $NI$ provides the number of identifiers that can fit in the DIO payload. $NI$ is calculated as the rounded integer of the available payload (33 bytes) divided by the identifier size $b$. $NS$ is the total number of messages required to transmit the complete identifier ring. $NS$ is calculated as the quotient of $RS$ divided by $NI$. Finally $SN$ identifies the order of the specific message in the complete sequence of messages required to disseminate the identifier ring. It is calculated as the sequence index corresponding to the current message.

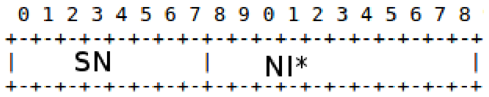
Table I
IDENTIFIER TRANSMISSION CONFIGURATION OPTIONS USED FOR TRANSFERING SISLOF MESSAGES IN DIO AND DAO.

| Variable | Name of Field | Size in bytes |
|---|---|---|
| $RS$ | Ring Size | 1 byte |
| $b$ | Identifier Size | 1 byte |
| $NI$ | Number of identifiers in one message | 1 byte |
| $NS$ | The Total Number of Sequences | 1 byte |
| $SN$ | The Sequence Number | 1 byte |

To encapsulate as many identifiers as possible in each DIO message, variables size in bytes are kept to the minimum by giving only 1 byte for each variable as shown in Table I. This means that each variable can have any value between 0 to 255 in decimal. Several factors were behind choosing these values. From experiments we did and using the same technique used in [3] with a 2500 mote network and the Ring Size $RS$ that we used was $41$ keys/identifiers for each ring. Using the same formula in [3] with the same network size and Pool size, the ring size for a network of $100\,000$ motes will be 250 keys. It can be represented in a 1 byte field. We have also used an Identifier Size of 1 byte. Using 1 byte for the Identifiers is more than enough, since the identifier is not used to encrypt the message and it is only used to identify if a common key exists between two motes. Using both $RS$ and $b$ will not yield a number of identifiers in one message larger than 256. In our example, using the same number of motes as [3] will yield one identifier $NI$ per each message, that is 250 messages or the total number of sequences $NS$. The sequence number $SN$ will of course be smaller than $NS$ as it is a counter that will determine the sequence number of a specific message.

DAO messages takes 69 bytes as per [8]. This leaves us with 58 bytes in the data frame that we used to embed frames related to our OF used as below and shown in Fig. 2. $SN$ is the sequence number received in the corresponding DIO. $NI$ is a bitmap with bits set to 1 if the identifier with the corresponding position is available in the identifier ring of the mote that received the DIO message and 0 otherwise [1]. The DAO messages sent upward by each node that received the DIO is shown in Algorithm 1.

[1] $NI$ size is variable and changes depending on the size of each identifier.



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

Figure 2. Addition to the DAO message. 1 byte for Sequence Number (SN) and $NI$, the bitmap representing shared identifiers bits.

### D. Securing the link

A mote that is propagating the DODAG information, broadcasts the DIO message downwards. The DIO message will contain all information related to 6LoWPAN messages such as the IPv6 header, etc. On top of that, the DIO message will also contain its rank with the root. SISLOF addition to the DIO message, explained in Fig. 1 will contain the identifiers of the first DIO frame from the sequence of frames ($NS$).

One of the constraint variables that is required by the SISLOF is the shared identifier constraint. The calculation of this variable will produce a secure or insecure link. This variable will determine whether a mote is considered a secure candidate parent or not. This is the first constraint/criterion that SISLOF computes before moving to other variables to calculate the path between motes and the root and form the RPL routing table.

Each mote that receives a DIO message replies back with the DAO message the 6LoWPAN header. On top of that, the DAO message will also contain the SISLOF additions explained in Fig. 2.

Each node that receives a DIO message replies back with the DAO message that contains as of Fig. 4, all information related to 6LoWPAN message such as IPv6 header, etc. On top of that, the DAO message will also contain the SISLOF objective function additions explained in Fig. 2 The DAO messages sent upward by each node that received the DIO is shown in Algorithm 1.

The sequence diagram shown in Fig. 3 shows the various control messages and variables exchanged between two nodes in order to determine if a common identifier exists. After a common identifier is found, SISLOF will then compute the link metrics and the parent ETX in order to choose the preferred parent.

### E. Link Metrics and parent ETX calculation.

If one or more secure mote that received the DIO identified that a shared identifier exist then the expected Transmission Count metric (ETX of the parent), similarly to the ETX calculation of RPL link metrics in [7], will become the second criteria on deciding the best parent. This metric will return the values of the DIO origin mote ETX ($parent\_metric$) and its received metric $instance\_etx$. From these two variables the link metric can be calculated to return the ETX of the link $link\_metric$ [15].

**Input :**

- **DIO message** ($DIO_{SN}$)
  $DIO_{SN}$=($n$, $b$, $IR_{SN}$, $NI$, $NS$, $SN$)
- **Identifier Ring of Receiver** $IR_r$
  $$IR_r = \big[ID_1, \quad ID_2, \quad ID_3, \quad ID_4, \quad \ldots \quad ID_{(n-1)}, \quad ID_n\big]$$
- **Ring Size (RS)**

**Output :**

- **Shared identifiers bits** ($SIB_{SN}$)
  $$SIB_{SN} = \big[b_1, \quad b_2, \quad b_3, \quad b_4, \quad \ldots \quad b_{(NI-1)}, \quad b_{(NI)}\big]$$
- **DAO message**
  $DAO_{SN}$=($SN$), $SIB_{SN}$
- **Shared Identifier State** ($SIS$)
  $$SIS = \big[w_1, \quad w_2, \quad w_3, \quad w_4, \quad \ldots \quad w_{(NI-1)}, \quad w_{(NI)}\big]$$

```
$SIB_{SN} = [NI]$;
$x = 0$;
$y = 0$;
$z = 0$;
$w = 0$;
$SIS = [w]$;
for $w = 0$ to $RS - 1$ do
    for $y = 0$ to $NI - 1$ do
        for $z = 0$ to $RS - 1$ do
            if $IR_{SN}[y] = IR_r[z]$ then
                Append 0 To $SIB_{SN}$;
                $SIS[w] = 0$ ;
            else
                Append 1 To $SIB_{SN}$;
                $SIS[w] = 1$ ;
        end
    end
end
AddtoDictionary $DAO_{SN}$ ($SIB_{SN}$ "Shared
  Identifiers bits", ($SN$) "Sequence Number" );
Send $DAO_{SN}$ upward to DIO Sender ;
```

**Algorithm 1:** DAO Messages Algorithm

DAO messages each a reply to a DIO message from the sequence it receives, contains a bitmap stream of bits representing either a value of 1 for a shared identifier and a value of 0 for a not shared identifier in $SIB_{SN}$ for all identifiers in the ring of the receive mote.

## V. Experiment Setup and Parameters

Similarly to the experiments carried on in [4] and [11], the experiments were simulated using the Cooja application in the Contiki Operating System.

A C program was coded to implement the key predistribution algorithm of [3]. This resulted in the generation

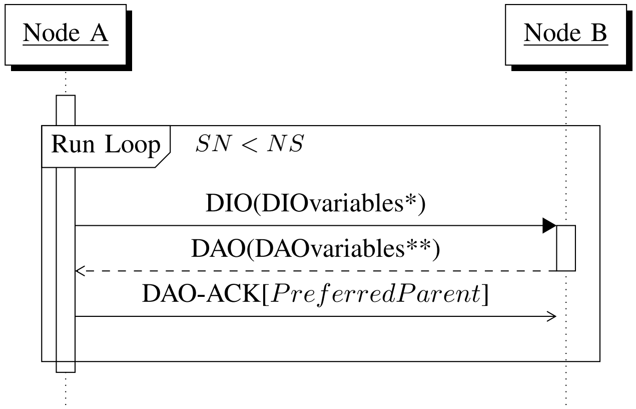


Figure 3. SISLOF Sequence Diagram
**diovariables*:** RI , IS, Num.Of.Seq , Num.Of.Iden, $ID_{SN}$[], Seq.Num
**daovariables**:** Seq.Num,$NI_{SN}$[], ETX

of Keys Pool, IDs pool, Key rings and ID rings [2].

The parameters used in the SISLOF experiment are the same as in [4] and [11]. The overall area of the simulation was kept to $250\text{x}250$ meters, a typical size of a medium size university [3]. The transmitting range for each mote is set to 50 meters (this is the common transmitting range for 6LoWPAN low power devices). We also used the key length $klength$ of 64 bits and the ID length $ilength$ of 32 bits.v The Pool size $P$ for both keys and identifiers is the first parameter. The pools size we run simulations for are: 100, 250, 500, 750, 1 000 and 2 500 motes. The second parameter is the network size $N$.

In this paper we are looking at the maximum number of motes as it is an important factor to determine the number of keys shared between motes in comparison to it. The third parameter is the ring size $RS$ For each pool size (P), keys and identifiers and to ensure the accuracy of experiment simulations, each experiment was run 5 times with the largest and smallest results discarded and the average of the remaining three runs used. In our experiments, if this node does not share a key with its preferred parent, then the link between those two nodes does not exist. Therefore the node will not be in the routing table and any sub leaves will also be discarded. In addition to this, when simulating smaller number and given that the simulation area is not changed, the number Percentage of Shared Keys (SK %) for 10 or 25 motes in the network is low as motes are unable to communicate with each other since the network motes are sparse.

## VI. Results

The proposed Objective Function SISLOF was simulated using the the parameters explained in the previous section. This presented us with three different sets of experiments, the first in [4] where the pre key distribution scheme was simulated in the context of Wireless Sensor Networks. The second in [11] where the scheme was simulated in the context of the IoT using the default RPL routing metric, the Minimum Expected Transmission Count ETX. The third is the simulation where the scheme is simulated in the context of the IoT using SISLOF for RPL. The number of keys in the ring size $RS$ for each of the three set of experiments is shown in Table II below with the percentage of Shared Keys (SK %) between motes that formed leaves in the routing table.

Table II
Comparison table showing precentage of Shared Keys (SK%) when original Ring Size (RS) and Network Size (N) are used, when Minimum ETX metric is used and when SISLOF metrics are used.

| Original values | | | Experiment | | | |
|---|---|---|---|---|---|---|
| | | | Minimum ETX metric [4] | | SISLOF | |
| N | RS | SK % | RS | SK % | RS | SK % |
| 100 | 8 | 50.52 | 23 | 100 | 12 | 100 |
| 250 | 13 | 50.43 | 36 | 100 | 20 | 100 |
| 500 | 18 | 57.14 | 48 | 100 | 28 | 100 |
| 750 | 22 | 49.47 | 63 | 100 | 38 | 100 |
| 1000 | 25 | 57.14 | 77 | 100 | 40 | 100 |
| 2500 | 41 | 48.19 | 104 | 100 | 60 | 100 |

From Table II, we can notice that the ring sizes in DSN was quite low in comparison with the ring sizes for IoT when the Minimum ETX metric was used. However it is also clear that the ring sizes when SISLOF is used, is around $55\%$ less then when RPL was using with the ETX metric. From Fig. 4, we can observe the performance of the key pre-distribution using the three experiment sets results presented in the table. The key-pre-distribution in the DSN networks presented the lowest ring sizes and the IoT using the Minimum ETX metric for RPL showed the highest ring sizes.

Wireless Sensor Networks required the smallest ring sizes to achieve full connectivity simply because in DSN a mote that do not share a key with one of its neighbours can send data to that specific neighbour indirectly through another mote and thus the full network connectivity is achieved even if not all motes share keys.

The ring size needed to achieve full connectivity when RPL was used with its default minimum ETX metric was the largest because only motes that share a key can participate in the RPL routing table. Nodes that did not share key could not communicate. By increasing the size of the ring, we ensured in [11] that all motes can join the RPL routing table and thus communicate.

From [4] and [11], we identified that 104 keys and identifiers in the rings was needed to achieve a $100\%$ guaranteed connectivity in the network comparison with only 60 keys when SISLOF was used. Using the parameters we explained in section 5, we can conclude that the key ring and the identifier ring in each mote for a network of 2 500 motes will

[2] Different random generators were used for keys, IDS and pools [4]
[3] Birkbeck, University of London [11]

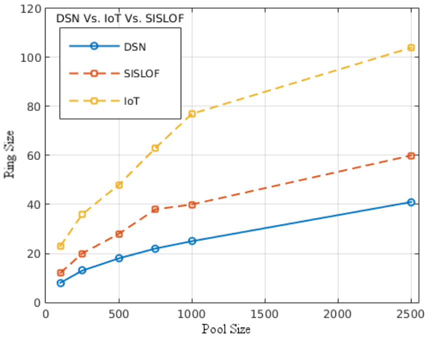


Figure 4. Comparison of the rings sizes used in Key Pre Distribution Scheme (DSN, IoT and RPL with SISLOF).

take up around $0.72kb$. This is an actual saving of nearly $50\%$ in term of capacity in comparison with the required storage of 1.38 kb for a 104 key ring and a 104 identifier ring. In this experiment, we have used Zolertia mote Z1 which features a 92KB Flash memory. This means that more than 90 kB of Flash memory is still free to use for other applications. Using the calculation as of [3], we can expect the ring sizes for $100\,000$ to be in the region of $2400$. This will require around $28.8$ kB of Flash memory.

## VII. Conclusion

In this document we proposed Shared the Identifier Secure Link Objective Function (SISLOF), an Objective Function that identifies motes that share a secure links in the network and uses secure links as the first criterion for calculating the RPL routing table.

We have investigated the performance of SISLOF and its impact on the security of an Internet of Things network. The results of the rings sizes in the SISLOF experiments is clearly a lot smaller then the rings sizes in the IoT experiments. We have provided evidence that by using SISLOF we can secure all communications between motes in the Internet of Things as only motes that share a key can be joined in the routing table and thus all communications between motes are secure.

The experiments simulated indicate that by using SISLOF, the ring size in term of number of keys and identifiers in comparison with the size of ring size wwhen using RPL with minimum ETX metric was nearly half. This resulted in a reduction of storage compairson to nearly half as well. Those savings will also have a direct impact on the power consumption. Less keys and identifiers in the ring will also result in less messages being exchanged between motes and thus using less battery power.

The proposed SISLOF provides evidence that it is able to secure the IoT in an efficient way for small area such a medium size university, however more research is required in order to determine its suitability in term of the overhead it generates in the network when RPL messages are propagating to all motes to form the routing table and the storage space it will consume once networks become larger. One possible solution that is worth exploring is to have multiple DODAGs with secure routes between roots.

## References

[1] Z. Shelby and C. Bormann, *6LoWPAN The Wireless Embedded Internet*, 1st ed. Wiley, 2007.

[2] I. C. Society, “802.15.4 low rate wireless personal area networks (lr-wpans),” 2011.

[3] L. Eschenauer and V. D. Gligor, “A key-management scheme for distributed sensor networks,” in *Proceedings of the 9th ACM CCS*. NY, USA: ACM, 2002, pp. 41–47.

[4] A. E. Hajjar, G.Roussos, and M. Paterson, “Securing the internet of things devices using pre-distributed keys,” in *IC2EW*, April 2016, pp. 198–200.

[5] “Jp vasseur, milestone in connecting the internet of things – rpl routing standard completed,” cisco, 2012.

[6] T. Winter, P. Thubert, and et.al, “Rpl: Ipv6 routing protocol for low-power and lossy networks,” RFC 6550, March 2012.

[7] J. Vasseur, M. Kim, and et.al, “Routing metrics used for path calculation in low-power and lossy networks,” RFC 6551, March 2012.

[8] P. Thubert, “Objective function zero for the routing protocol for low-power and lossy networks (rpl),” RFC 6552, March 2012.

[9] O. Gnawali and P. Levis, “The minimum rank with hysteresis objective function,” RFC 6719, September 2012.

[10] D. W. Carman, Kruus, and et.al, “Constraints and approaches for distributed sensor network security (final),” *DARPA Project report,(Cryptographic Technologies Group, Trusted Information System, NAI Labs)*, vol. 1, no. 1, 2000.

[11] A. E. Hajjar, G.Roussos, and M. Paterson, “On the performance of key pre-distribution for rpl-based iot networks,” in *3rd EAI International Conference on Safety and Security in Internet of Things*, October 2016.

[12] R. Mukundan, K. Morneault, and N. Mangalpally, “Digital private network signaling system (dpnss),” Internet Requests for Comments, RFC 4129, September 2005.

[13] M. Noack, “Optimization of two-way authentication protocol in internet of things.”

[14] D. A. Ha, Nguyen, and et.al, “Efficient authentication of resource-constrained iot devices based on ecqv implicit certificates and datagram transport layer security protocol,” in *The 7th proceedings of SoICT*. NY, USA: ACM, 2016, pp. 173–179.

[15] J. Hui and J. Vasseur, “The routing protocol for low-power and lossy networks (rpl) option for carrying rpl information in data-plane datagrams,” RFC 6553, March 2012.