Intrusion Detection in the RPL-connected 6LoWPAN Networks

Dharmini Shreenivas
Ericsson AB
Kista, Stockholm, Sweden
dharmini.shreenivas@ericsson.com

Shahid Raza
RISE SICS AB
Stockholm, Sweden
shahid@sics.se

Thiemo Voigt
RISE SICS AB
Stockholm, Sweden
Uppsala University, Sweden
thiemo@sics.se

ABSTRACT

The interconnectivity of 6LoWPAN networks with the Internet raises serious security concerns, as constrained 6LoWPAN devices are accessible anywhere from the untrusted global Internet. Also, 6LoWPAN devices are mostly deployed in unattended environments, hence easy to capture and clone. Despite that state of the art crypto solutions provide information security, IPv6 enabled smart objects are vulnerable to attacks from outside and inside 6LoWPAN networks that are aimed to disrupt networks.

This paper attempts to identify intrusions aimed to disrupt the Routing Protocol for Low-Power and Lossy Networks (RPL). In order to improve the security within 6LoWPAN networks, we extend SVELTE, an intrusion detection system for the Internet of Things, with an intrusion detection module that uses the ETX (Expected Transmissions) metric. In RPL, ETX is a link reliability metric and monitoring the ETX value can prevent an intruder from actively engaging 6LoWPAN nodes in malicious activities. We also propose geographic hints to identify malicious nodes that conduct attacks against ETX-based networks. We implement these extensions in the Contiki OS and evaluate them using the Cooja simulator.

Keywords

RPL, ETX, Internet of Things, 6LoWPAN, Intrusion Detection, Cyber Security, IPv6

1. INTRODUCTION

The Internet Protocol (IP) connects standard computers and similar devices with the Internet since some decades. It has also been realized that the IP capabilities should be extended to the less traditional everyday resource-constrained computing devices. The interconnection of billions of everyday objects and the Internet forms the Internet of Things. IPv6, with potentially unlimited address space, is a favorable candidate for the IoT, as IPv4 addresses are not even enough to handle the current load of traditional Internet hosts. However, *things* (resource-constrained devices in the IoT) have limited storage, processing, and energy resources and it is not feasible to use full-fledged IPv6 for these constrained devices. Therefore, IPv6 over Low-powered Wireless Personal Area Networks (6LoWPAN) has been standardized to route IPv6 packets in low-power and lossy IEEE 802.15.4-based networks [Kushalnagar et al. 2007, Montenegro et al. 2007], called 6LoWPAN networks.

Due to the connectivity with the untrusted Internet, security is necessary in 6LoWPAN deployments. We have developed a number of security solutions for the IoT including lightweight end-to-end communication security protocols [Raza et al. 2013a][Raza et al. 2014], a scalable key management solution by using only symmetric keys [Raza et al. 2016], and an efficient data-at-rest security mechanism [Bagci et al. 2015].

Due to the low-power and lossy nature of 6LoWPAN networks, traditional Internet routing protocols are not feasible for such networks. Therefore, the Routing Protocol for Low-Power and Lossy Networks (RPL) [Winter et al. 2012] has been standardized. For RPL too, it is important that the routing protocol should work as intended and hence must be robust against attacks aimed to disrupt the network. Previously, we have conducted different attacks against RPL-connected 6LoWPAN networks [Wallgren et al. 2013], and demonstrated that RPL is vulnerable to multiple attacks. Le et al. [Le et al. 2012] have also presented different attacks against 6LoWPAN networks. In order to mitigate these attacks we have devised SVELTE [Raza et al. 2013b], an intrusion detection system for RPL-based networked. Zarpelão et al. [Zarpelão et al. 2017] provide a comprehensive survey of intrusion detection mechanisms designed for IoT, which also covers SVELTE.

SVELTE is primarily based on the RPL rank parameter and defends against attacks that are based on the illegal manipulation of ranks. The RPL rank determines the position of individual nodes with respect to the root and relative to other nodes in the networks. RPL also uses the Expected Transmission Count (ETX) to estimate the link quality to a node's neighbors. The ETX path metric is an important path quality metric in RPL-connected 6LoWPAN networks, which could be exploited to launch different attacks.

In this paper, we propose an extension to the SVELTE intrusion detection system using the ETX metric. We also propose intrusion detection based on geographical hints, which can be used in situations when both rank-based and ETX-based solutions are not able to detect the majority of the attackers. We implement our intrusion detection systems in

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than ACM must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from permissions@acm.org.

IoTPTS'17, April 02 2017, Abu Dhabi, United Arab Emirates

© 2017 ACM. ISBN 978-1-4503-4969-7/17/04…$15.00

DOI: http://dx.doi.org/10.1145/3055245.3055252

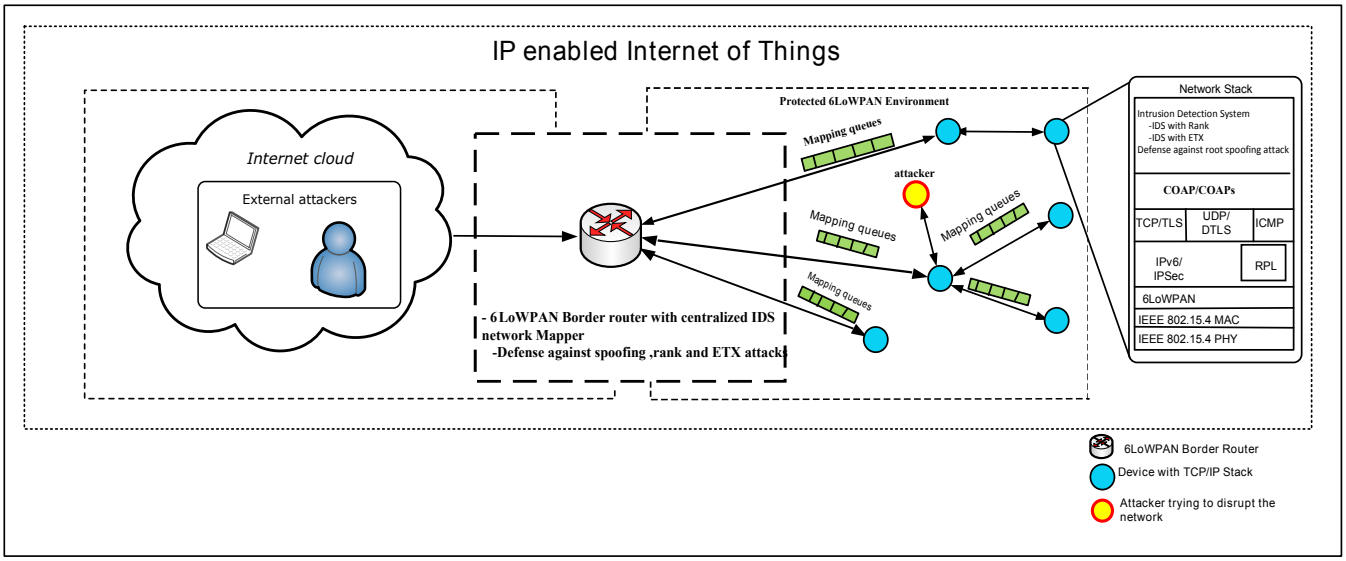

Figure 1: An IoT setup showing the interconnection of 6LoWPAN networks with the Internet through a 6BR. It also shows the placement of IDS modules in *things* and in 6BR.

the Contiki OS [Dunkels 2003] and evaluate them using the Cooja simulator [Eriksson et al. 2009]. In our experiments we use a realistic IoT setup, shown in Figure 1. We introduce the relevant IoT technologies, depicted in Figure 1, in Section 2.

The main contributions of this paper are:

- We propose an extension to SVELTE and include an IDS module for the RPL ETX metric.
- To improve the detection rate, we propose the use of geographical hints.
- Last but not least, we implement and evaluate our extensions in a simulated RPL network that uses actual IoT protocols: IPv6, 6LoWPAN, UDP, RPL, and IEEE 802.15.4.

The rest of the paper is organized as follows. The next section briefly discusses RPL and related technologies necessary to understand this paper. Section 3 presents our intrusion detection extensions for RPL-connected networks. In Section 4 we describe the implementation and evaluation details and present our results. Finally, Section 5 concludes the paper.

2. THE RPL PROTOCOL

The Routing Protocol for Low-Power and Lossy Networks (RPL) is a new standard for resource-constrained environments. RPL is a distance vector protocol that builds the destination oriented directed acyclic graph (DODAG). In the DODAG topology traffic from all the edges converges towards a single destination called the DODAG root. In the case of 6LoWPAN networks the DODAG root is the 6LoWPAN border router (6BR), which is shown in Figure 1. The DODAG also consists of routers and leaf nodes.

RPL defines the following ICMPv6 control messages: DODAG Information Object (DIO), Destination Advertisement Object (DAO), and DODAG Information Solicitation (DIS) to construct the DODAG. Each DODAG is identified by its topological information such as RPLInstanceID, DODAGID and DODAGVersionNumber. These identifiers are periodically advertised by the DODAG nodes to build the DODAG tree.

In order to define the routing path for datagrams in the DODAG, RPL uses the Objective function (OF). The OF could be determined by either one or many RPL metrics defined in the DAG metric container [Vasseur et al. 2011]. All the nodes along with the DIO advertisements advertise the DAG metric container. Based on these advertisements, the routing path is built from the leaf nodes to the 6BR to form a DODAG tree like structure. Figure 2 depicts a RPL DODAG and shows the rank and ETX metrics, which we discuss in Section 2.2. A trickle timer is used to synchronize communications between the ICMPv6 messages for node-to-node communications [Winter et al. 2012].

2.1 RPL DODAG building process

When all the nodes boot up, the system administrator configures the 6BR. This means that the objective function would also be configured for a 6LoWPAN network. All ICMP messages are managed by the trickle timer to avoid ambiguity in the network. The participating nodes advertise their presence and their positions and related routing metrics through the DIO messages to all neighboring RPL nodes.

Initially after neighbor discovery, the DIO messages are sent upon the expiration of the trickle timer [Levis et al. 2011]. All DIO messages are advertised via link local multicast advertisements. Then every node starts advertising their DIO messages. Upon every single received DIO messages, all nodes first verify the authenticity of the DIO and also whether they do adhere to local policies, routing metrics, etc. Primarily each and every node which receives DIO messages checks the incoming DIO messages for two purposes, first to adhere to the DODAG policy, i.e., the rank of the sending node should be lower than that of the receiving node; the DIO should have a rank greater than

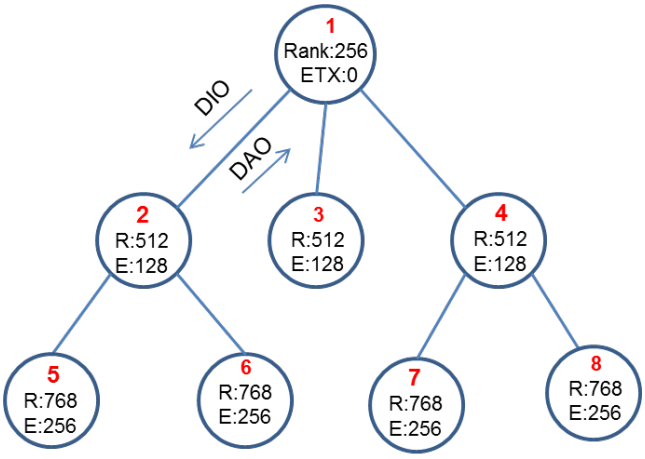

Figure 2: The RPL DODAG

MinHopRankIncrease (Section 2.2.1) and not greater than DAGMaxRankIncrease. Second, for the Mode of Operation (MOP) flag in the DIO, which is responsible for recording the type of route the node is going to follow in the DODAG (upward or downward). In case the downward routes are preferred, the child nodes would trigger the DAO messages advertising its reachability in the DODAG towards its parents along with DAO lifetime and other parameters. The DIO message could also be configured according to the OF and the nodes can discard DIO messages based on those OF constraints [Winter et al. 2012].

2.2 RPL Routing metrics

The RPL routing metrics determine the routing path dictated by the OF in any DODAG, advertised by the 6BR [Winter et al. 2012]. RPL being a distance vector protocol, paths with low cost are chosen by the routing protocol for better efficiency [Vasseur et al. 2011]. Routing metrics are either aggregated or recorded. An aggregated metric is modified along the path that it traverses with the DIO. Routing metrics are encoded in a DAG metric container that is in turn carried by the DIO messages. On receiving the DIO message from a set of parents, the child node decides its own parent set according to the OF. RPL is a lossy network; hence a group of metrics is necessary to evaluate the condition of every node. Depending upon the implementation environment even a single metric could be chosen to determine the state of RPL nodes.

There are various routing metrics that RPL utilizes for building the DAG, which are standardized by the IETF [Vasseur et al. 2011]. SVELTE has used rank and for this paper we also utilize the ETX metric to detect malicious nodes.

2.2.1 *Rank Metric*

The rank is a 16-bit integer that is present in the DAG metric container. The rank determines the relative position of a node with respect to the Border router. The rank value is a monotonically increasing value from top to bottom. The nodes that are closer to the 6BR will have a lower rank value and farther nodes will have a higher rank value. All nodes should advertise a rank value to the least of MinHopRankIncrease. The nodes should not advertise any value greater than the total sum of the least rank in a DAG and DAGMaxRankIncrease. MinHopRankIncrease is the minimum increment of a rank value in each hop between any node and any of its DODAG parents. DAGMaxRankIncrease is the configured upper limit value of all nodes. The DAGMaxRankIncrease is provisioned by the Border Router and is present to avoid loop formation in a DODAG.

2.2.2 *ETX Metric*

Expected Transmission (ETX) metric is a path reliability metric for lossy networks [De Couto et al. 2005]. The ETX is defined as the number of transmissions necessary for a packet to reach the DODAG root. The ETX is measured by sending periodical probe packets between the participating neighbors. Hence, the ETX indicates the communication quality of the neighbors. In ContikiRPL, ETX is a scalar value, a multiple of 128 that is encoded as 16-bits in the DAG metric container. When RPL uses the ETX metric as an OCP[1], the OF builds routes with nodes having minimum ETX values [Gnawali and Levis 2011]. Thus ETX is referred to as the link quality of the node along with its neighbors. The Collection Tree Protocol (CTP) is an example of a popular protocol [Levis et al. 2005] that utilizes ETX for network formation.

The ETX path metric is a cumulative sum of a node's own ETX value to a neighbor and the ETX value advertised by its neighbor, which indicates the distance of that neighbor from the root. The ETX path metric is calculated whenever the ETX link values are updated on a node's link and by the neighbor. All nodes in a DODAG compute the ETX path metric for each candidate neighbor reachable on all the interfaces. If any node cannot compute the ETX value of its neighboring nodes then the failed node should not be included in the candidate neighbor and parent sets. The formula used to calculate ETX is:

$$\frac{1}{D_f * D_r} = ETX$$

Where D_f is the measured probability of the received packets and D_r is the measured probability of the received acknowledgments for the sent packets.

With this background we are now going to propose our SVELTE extensions.

3. INTRUSION DETECTION IN RPL-CONNECTED NETWORKS

SVELTE is a state of the art IDS designed primarily for RPL-based 6LoWPAN networks [Raza et al. 2013b]. SVELTE mostly relies on the RPL rank metric to defend against different attacks. In this paper we include the ETX metric in the SVELTE design. We also introduce an IDS mechanism with geographic hints, in an attempt to locate malicious nodes that cause instability inside 6LoWPAN networks.

Before presenting these two extensions we discuss the changes in SVELTE to support our new extensions. An important part of SVELTE is the 6LoWPAN Mapper (6Mapper) that constructs the RPL DODAG in the 6BR and adds each node's neighbor and parent information in the DODAG. To reconstruct the DODAG, the 6Mapper collects necessary information from each node at regular intervals. SVELTE defines a request packet that contains the information needed

[1]The Objective Code Point (OCP) indicates which routing metrics are in use in a DAG.

to identify an RPL DODAG. We complement the 6Mapper packet with the ETX value and send it with each received request.

Effects of inconsistent ETX values in 6Mapper:.

Timing consistencies are important for a mapping authority to receive the latest information about the participating nodes in 6LoWPAN networks. In RPL, the quality of a path is described by the ETX value [Gnawali and Levis 2010]. If the 6Mapper has incorrect ETX values of the nodes, it would indicate misplaced logical coordinates of the node, which is intolerable in RPL as many DAGs build their routing path based on the ETX values.

In RPL, the ETX value of a parent should be lower than that of the children. The root node has the lowest ETX. Figure 3 shows a simple RPL DODAG with ETX values, which shows that with a simple manipulation of ETX values, a routing loop can be created. A malicious node can launch different attacks by illegally modifying the ETX value. For example an attacker can modify the ETX value and get a better position in a DODAG, which helps the attacker to launch further attacks such as sinkhole or selective forwarding attacks [Raza et al. 2013b].

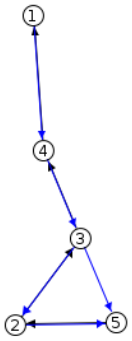

Figure 3: Loop formation with ETX Attack

3.1 Our IDS with ETX Metric

By advertising a false ETX value an attacker can make neighboring nodes believe that the compromised node has a stronger or a weaker link. Also if the attacker's node is present on the routing path, it can advertise a low ETX value to attract traffic and conduct a selective forwarding attack. Attackers can also launch other attacks, for example, by placing the attacker's node(s) in the routing path to attract traffic and create loops (Figure 3) to exhaust the energy of authorized nodes. While link level encryption could help to prevent these attacks it is still possible to compromise a legitimate node. In the best case, we could use an asymmetric cryptography with a Public Key Infrastructure (PKI) but this is too resource hungry and often not feasible in constrained environments.

In this paper we attempt to detect an intruder in 6LoWPAN networks by calculating the ETX values [De Couto et al. 2005]. In order to do so, the 6Mapper traverses through the entire DAG and records metrics for all the nodes participating in the DAG. In Algorithm 1, we detect intruders who advertise false ETX values to gain more strength or to perform DoS attacks. We also defend against root spoofing attacks by verifying the rank values against the ETX values. The ETX values are calculated for every single node and their neighbors. The thumb rule for ETX verification is that the parent's ETX value should be lower than that of its children. An intruder is determined if any of the node(s) ETX values are abnormal. Lower ETX values depict a better path to the 6BR and hence falsified values could indicate the adversary node is closer to 6BR. The adversary node that manages to attract traffic by advertising a low ETX value is capable of disrupting the entire 6LoWPAN network. On the other hand, a adversary node can distract the nodes in its sub DODAG that the adversary node is far away from 6BR, by advertising a higher ETX value than the calculated actual ETX value.

Algorithm 1 Intrusion detection by verifying the propagation of ETX inside 6LoWPAN networks

Require: N - Set of nodes
Require: P - Parent set of the node
Require: $Neighbors$ - Neighbor set of Node N
for $Node$ in N **do**
  for all $Neighbor$ in $Node.Neighbors$ **do**
    if $Node.etx == 0$ **then**
      if $Parent.etx == 0$ **then**
        if $Node.Rank == Root.Rank$ **then**
          $Node.fault = Node.fault + 1$ {The node is trying to advertise a root etx value}
        end if
      end if
    end if
    if $Node.etx > 0$ **then**
      if $Node.etx < Parent.etx$ **then**
        if $Node.Rank > Parent.Rank + MinHopRankIncrease$ **then**
          $Node.fault = Node.fault + 1$ {The node is trying to advertise an invalid etx value}
        end if
      end if
    end if
  end for
end for
for $Node$ in N **do**
  if $Node.fault > FaultThreshold$ **then**
    A new parent is chosen
  end if
end for

To include fault tolerance, we also check the node and the parent's rank value. Recall that the least increase in rank should be that of MinHopRankIncrease and not exceeding DAGMaxRankIncrease values. Network administrators can decide these values based on the implementation specifications. In our implementation we set the MinHopRankIncrease to 256 and DAGMaxRankIncrease is set to 2048. We mark a fault threshold to not tolerate too many fraudulent attempts and we demarcate the routing path when it exceeds the fraudulent threshold.

3.2 Our IDS with Geographic Hints

Though ETX and ranked based solutions can detect some attacks, an attacker can compromise a node plus some of its neighbors. In that case it is difficult for the 6Mapper to distinguish the inconsistencies in the rank and ETX using our algorithms. In those situations, geographical hints can help

Algorithm 2 Intrusion Detection with geographical information inside 6LoWPAN networks

Require: N - Set of nodes participating in the 6LoWPAN networks
Require: Tx - Nodes within the receiving vicinity
Require: NT- Neighbor table listing a collection of nodes
Require: $Neighbor$ - Neighbor of the Node N
  for all $Node$ in N **do**
    $NT = nodeswithin|Node.Tx|$
    if $NodeinNT$ **then**
      $Node.ETX < Node.Neighbor.ETX$
    end if
  end for

to mitigate the rank and ETX attacks. The requirement is, however, that the nodes' locations are known.

In Algorithm 2 we attempt to cluster the nodes with limitations of their transmission power to deduce their immediate neighbors. The goal of this technique is to determine the intruders who fake identities to conduct various attacks in an IoT environment. Firstly, we calculate the transmission limits for every node in the network and maintain a neighbor table listing the identities of the nodes within their transmission range. This would be effective for RPL 6LoWPAN networks because if any intruder attempts to fake the identity we could determine that from the respective neighbor table. Also, the neighbor table would consist of group of nodes with similar transmission ranges, so they would consist of similar nodes with small differences in rank and ETX values. If a node from a much lower cluster attempts to fake the identity of a node from a much higher cluster the IDS can identify the node as intruder. For example, the 6Mapper could detect an intruder claiming it has an ETX of 128 for a link while its neighbors are of 768 since it is practically impossible for nodes at level 6 to have a neighbor at level 1. Recall that ETX is a scalar value, a multiple of 128.

4. IMPLEMENTATION AND EVALUATION

We extend the SVELTE implementation with the new ETX and geographical parameters. We implement it in Contiki, an operating system for the IoT [Dunkels et al. 2004] . We perform our evaluations using Contiki 2.6 and Cooja [Eriksson et al. 2009] simulations.

4.1 IoT Demo Environment

Our IoT environment consists of a 6LoWPAN Border Router (6BR) as DODAG that connects a 6LoWPAN network to the Internet. The nodes that forward packets on behalf of other nodes are called routers. Devices at the edge of the tree are leaf nodes [Winter et al. 2012]. The 6BR could be attached to a large processing system as it the converging point for network traffic to enter or leave the 6LoWPAN environment. In this paper the 6BR is assumed to be trusted. For our simulations we use Tmote sky as *things* in 6LoWPAN networks. A Tmote sky has a CCC2420 transceiver [Moteiv 2006] and 48kB of ROM.

4.2 Experimental Setup

The experiments are run on an emulated 6LoWPAN network with RPL as the routing protocol and ContikiMAC as the MAC protocol. We use the same seed for all measurements. For intrusion detection analysis we evaluate the true positive rate and also measure the energy and ROM/RAM usage. To achieve this we use the base values of the Tmote sky (Table 1) [Moteiv 2006]. We evaluate the energy/power consumption and true positive rate of a network that consists of 4,6 and 8 legitimate nodes. Due to the simulation limitations, we show results for up to eight legitimate nodes. Our simulations also consist of two attacker nodes. We document the results when the first malicious node is detected. We do this every five minutes. At the first 2 minutes the node starts to map the information, and from the next round onwards the 6Mapper runs the detection modules.

In this paper, we use 3V as standard voltage for our calculations. All participating node are on either of the two states: Idle or listening. A node is in low power mode (LPM) when the radio is off and the micro controller unit (MCU) is idle. We calculate the CPU time when the micro controller unit (MCU) is on.

4.3 Power Usage

Energy/Power is one of the most important resources in constrained IoT devices, as most of them run on batteries. Therefore the communication and security protocols should be energy efficient and meet the constrained energy resources of IoT devices. We measure the power consumption with duty cycling and without duty cycling.

4.3.1 With Duty cycling

We measure the energy usage of a node using the energest module [Dunkels et al. 2007]. We record the CPU, LPM, Rx and Tx values respectively. We calculate the energy of a node using the formula

```
Energy(mWs) =
transmit * 19.5 + listen * 21.8 + LPM *
0.0545 + CPU 1.8
```

where transmit and listen are tx and rx values respectively. We calculate the average energy consumption of a node at the time when it detects an intruder node. We calculate the average power consumption of a single node when the intrusion is detected by the 6Mapper, using the following formula.

$$Power(mW) = \frac{Energy(mWs)}{Time(s)}$$

For the power consumption in Figure 4, we compare our results with the power estimation of SVELTE [Raza et al. 2013b]. Our IDS with ETX module computes almost the same power when compared with the IDS with rank module. This is because the energy consumed by sending the additional ETX value is negligible when compared with the overall energy usage by the network.

For our setup where the 6Mapper requests mapping information every two minutes, we calculate the average battery life with average supply voltage as 3V and average power consumption as 1.3 mW .

$$\frac{3000mAh * 3V}{avgpower(mW)}$$

$$\frac{3000mAh * 3V}{1.3(mW)} = 6,923.07(h)$$

We can thus except the node to stay for $6,923.07/24 = 288$ days.

Typical Operating Conditions	MIN	NOM	MAX	UNIT
Supply voltage	2.1		3.6	V
Supply voltage during flash memory programming	2.7		3.6	V
Current Consumption: MCU on, Radio RX		21.8	23	mA
Current Consumption: MCU on, Radio TX		19.5	21	mA
Current Consumption: MCU on, Radio off		1800	2400	μA
Current Consumption: MCU idle, Radio off		54.5	1200	μA
Current Consumption: MCU standby		5.1	21.0	μA

Table 1: Base measurement units for Tmote-Sky nodes

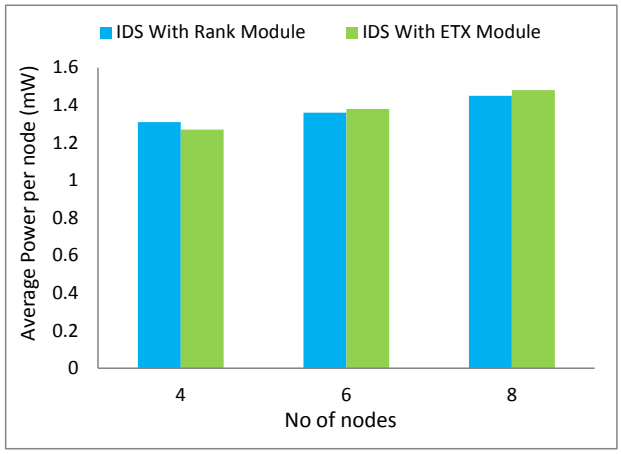

Figure 4: Power estimation for the two IDS modules when experiments are conducted with duty cycling.

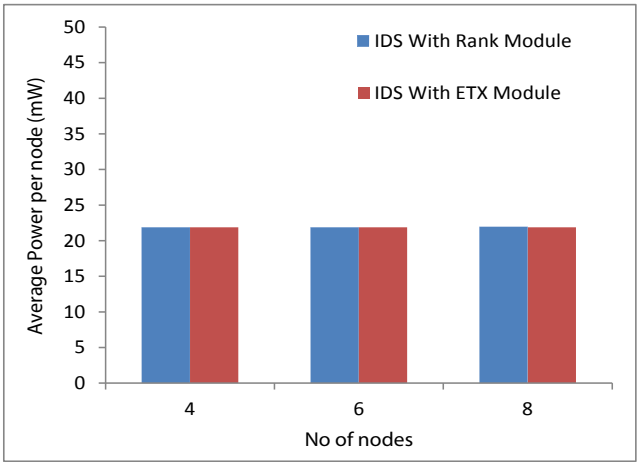

Figure 5: Power estimation for the two IDS modules when experiments are conducted without duty cycling.

4.3.2 *Without Duty cycling*

We evaluate the energy and power consumption when the radio is always on and nodes never sleep. As expected the results are same for both the IDS with rank and the IDS with ETX, as the CPU consumes negligible energy when compared with the energy consumed by the radio. As the radio is always turned on, we cannot really see the difference in energy consumption by the two different techniques. In fact, there is a 0.02% increase in power consumption between 4 and 8 nodes. For completeness, the results are anyhow shown in Figure 5.

We also compute the CPU power consumption in Figure 6 in order to compare the two IDS modules. Our results show that the ETX module consumes less CPU power than the Rank module.

4.4 IDS True Positive Rate

We also evaluate the true positive rate of the IDS with the ETX metric. True positive rate is the number of alarms successfully detected out of the total number of alarms. For this experiment, the information in the 6Mapper is processed every 2 minutes. This means that for the first round of 2 minutes we analyze the mapped information and during the next round of 2 minutes we display the fake nodes in the 6Mapper. Recall that we use a set of 4, 6, and 8 nodes respectively with 2 malicious nodes.

Figure 7 displays the true positive rate for the three sets of nodes. We cannot directly map these results with the SVELTE because the experiments in SVELTE are conducted with different sets of nodes, and our IDS with ETX parameter does not support more nodes in the simulated/emulated Cooja environment due to its limited resources of the Tmote sky. However, we learn that as the number of nodes increases the true positive rate decreases. Interestingly, we have also realized that on a combined analysis with the rank and the ETX module, the overall true positive rate increases. This is inline with the motivation to use the ETX in addition to using the rank for intrusion detection.

4.5 RAM and ROM usage

IoT devices have limited ROM and RAM resources. Therefore it is important that security and other protocols should be optimized for these environments. Table 2 shows the RAM and ROM overhead of our IDS with the ETX module. ROM usage in Contiki differs according to its implementation. Our implementation utilizes 48620 Bytes for the full Contiki with an overhead of 5,570 Bytes for the IDS with ETX module. Also, it consumes an additional 6 Bytes of RAM.

5. CONCLUSION

In this paper we have extended SVELTE, an intrusion

Overhead	**ROM** (*Bytes*)	**RAM** (*Bytes*)
Additional storage	5,570	6

Table 2: Additional RAM and ROM required by our IDS with ETX module.

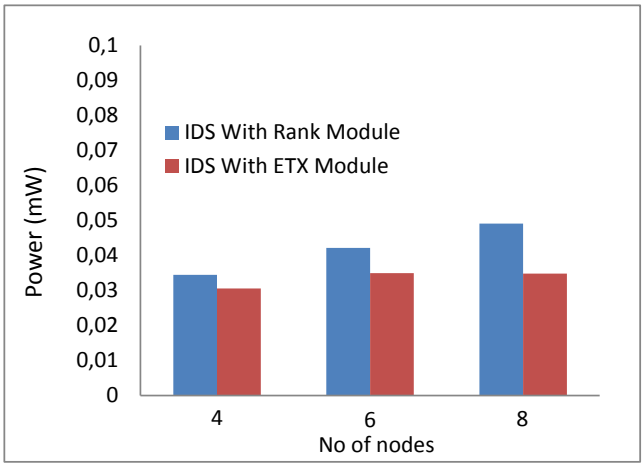

Figure 6: Comparison of power consumed by CPU while performing the intrusion detection using the rank metric and the ETX metric.

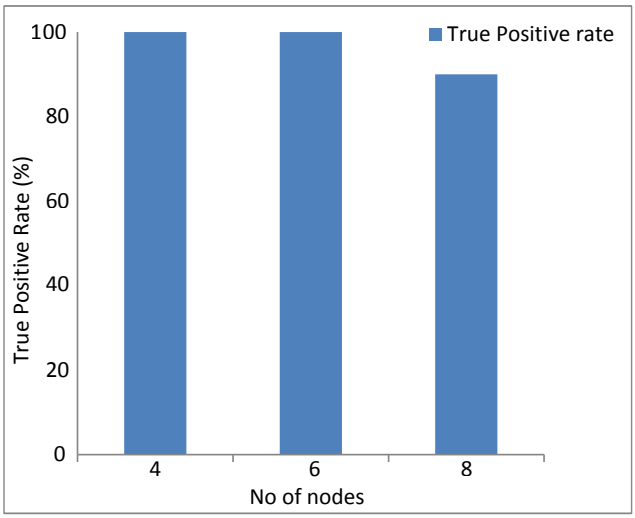

Figure 7: True positive rate with our IDS with ETX module for a set of 4, 6, and 6 nodes.

detection system for the IoT, and complemented it with the ETX metric and geographical hints. In RPL, an attacker can exploit the ETX metric and can launch different attacks by getting a better position in the RPL DAG. To overcome these attacks and also to find the malicious nodes, we have developed ETX-based and geographical detection algorithms. While our IDS module with ETX parameter can defend against ETX and rank attacks, the geographical detection algorithms can locate the proximity of a node to the 6Mapper and test its authenticity. Our results show that compared with rank-only mechanisms the overall true positive rate increases when we combine the EXT and rank based detection mechanisms.

6. ACKNOWLEDGEMENTS

This work was financed partially by VINNOVA and partially by the EU project NobelGrid under the grant no. 646184.

7. REFERENCES

[Bagci et al. 2015] Ibrahim Ethem Bagci, Shahid Raza, Utz Roedig, and Thiemo Voigt. 2015. Fusion: coalesced confidential storage and communication framework for the IoT. *Security and Communication Networks* (2015). DOI:http://dx.doi.org/10.1002/sec.1260

[De Couto et al. 2005] Douglas SJ De Couto, Daniel Aguayo, John Bicket, and Robert Morris. 2005. A high-throughput path metric for multi-hop wireless routing. *Wireless Networks* 11, 4 (2005), 419–434.

[Dunkels 2003] Adam Dunkels. 2003. Full TCP/IP for 8 Bit Architectures. In *Proceedings of the First ACM/Usenix International Conference on Mobile Systems, Applications and Services (MobiSys 2003)*. San Francisco. http://dunkels.com/adam/mobisys2003.pdf

[Dunkels et al. 2004] Adam Dunkels, Björn Grönvall, and Thiemo Voigt. 2004. Contiki - a Lightweight and Flexible Operating System for Tiny Networked Sensors. In *Proceedings of the First IEEE Workshop on Embedded Networked Sensors (Emnets-I)*. Tampa, Florida, USA. http://dunkels.com/adam/dunkels04contiki.pdf

[Dunkels et al. 2007] Adam Dunkels, Fredrik Osterlind, Nicolas Tsiftes, and Zhitao He. 2007. Software-based on-line energy estimation for sensor nodes. In *Proceedings of the 4th workshop on Embedded networked sensors*. ACM, 28–32.

[Eriksson et al. 2009] Joakim Eriksson, Fredrik Österlind, Niclas Finne, Nicolas Tsiftes, Adam Dunkels, Thiemo Voigt, Robert Sauter, and Pedro José Marrón. 2009. COOJA/MSPSim: interoperability testing for wireless sensor networks. In *Proceedings of the 2nd International Conference on Simulation Tools and Techniques*. 27.

[Gnawali and Levis 2010] Omprakash Gnawali and P Levis. 2010. The ETX Objective Function for RPL. *draft-gnawali-roll-etxof-01* (2010).

[Gnawali and Levis 2011] O Gnawali and P Levis. 2011. The minimum rank objective function with hysteresis. *draft-ietf-roll-minrank-hysteresis-of-04 (work in progress)* (2011).

[Kushalnagar et al. 2007] N Kushalnagar, G Montenegro, C Schumacher, and others. 2007. IPv6 over low-power wireless personal area networks (6LoWPANs): overview, assumptions, problem statement, and goals. *RFC4919, August* 10 (2007).

[Le et al. 2012] Anhtuan Le, Jonathan Loo, Aboubaker Lasebae, Mahdi Aiash, and Yuan Luo. 2012. 6LoWPAN: a study on QoS security threats and countermeasures using intrusion detection system approach. *International Journal of Communication Systems* 25, 9 (2012), 1189–1212.

[Levis et al. 2011] Philip Levis, T Clausen, J Hui, O Gnawali, and J Ko. 2011. The trickle algorithm. *Internet Engineering Task Force, RFC6206* (2011).

[Levis et al. 2005] Philip Levis, Sam Madden, Joseph Polastre, Robert Szewczyk, Kamin Whitehouse, Alec Woo, David Gay, Jason Hill, Matt Welsh, Eric Brewer, and others. 2005. TinyOS: An operating system for sensor networks. In *Ambient intelligence*. Springer, 115–148.

[Montenegro et al. 2007] Gabriel Montenegro, Nandakishore Kushalnagar, J Hui, and D Culler. 2007. Transmission of IPv6 packets over IEEE 802.15. 4 networks. *Internet proposed standard RFC* 4944 (2007).

[Moteiv 2006] Moteiv. 2006. *Tmote Sky Datasheet http://www.sentilla.com/pdf/eol/tmote-sky-datasheet.pdf*.

[Raza et al. 2014] Shahid Raza, Simon Duquennoy, Joel Höglund, Utz Roedig, and Thiemo Voigt. 2014. Secure Communication for the Internet of Things - A Comparison of Link-Layer Security and IPsec for 6LoWPAN. *Security and Communication Networks, Wiley* 7, 12 (Dec. 2014), 2654–2668. DOI: http://dx.doi.org/10.1002/sec.406

[Raza et al. 2016] Shahid Raza, Ludwig Seitz, Denis Sitenkov, and Göran Selander. 2016. S3K: Scalable Security with Symmetric Keys - DTLS Key Establishment for the Internet of Things. *IEEE Transactions on Automation Science and Engineering* 13, 3 (July 2016), 1270–1280. DOI: http://dx.doi.org/10.1109/TASE.2015.2511301

[Raza et al. 2013a] Shahid Raza, Hossein Shafagh, Kasun Hewage, René Hummen, and Thiemo Voigt. 2013a. Lithe: Lightweight secure CoAP for the internet of things. *Sensors Journal, IEEE* 13, 10 (2013), 3711–3720.

[Raza et al. 2013b] Shahid Raza, Linus Wallgren, and Thiemo Voigt. 2013b. SVELTE: Real-time Intrusion Detection in the Internet of Things . *Ad Hoc Networks, Elsevier* (2013). DOI: http://dx.doi.org/10.1016/j.adhoc.2013.04.014

[Vasseur et al. 2011] J. Vasseur, M. Kim, K. Pister, N. Dejean, and D. Barthel. 2011. Routing metrics used for path calculation in low power and lossy networks. *draft-ietf-roll-routing-metrics-19 (work in progress)* (2011).

[Wallgren et al. 2013] Linus Wallgren, Shahid Raza, and Thiemo Voigt. 2013. Routing Attacks and Countermeasures in the RPL-Based Internet of Things. *International Journal of Distributed Sensor Networks* 13, 794326 (2013). DOI: http://dx.doi.org/doi:10.1155/2013/794326

[Winter et al. 2012] T. Winter, P. Thubert, A. Brandt, J. Hui, R. Kelsey, P. Levis, K. Pister, R. Struik, J. Vasseur, and R. Alexander. 2012. RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks. RFC 6550 (Proposed Standard). (March 2012). http://www.ietf.org/rfc/rfc6550.txt

[Zarpelão et al. 2017] Bruno Bogaz Zarpelão, Rodrigo Sanches Miani, Cláudio Toshio Kawakani, and Sean Carlisto de Alvarenga. 2017. A Survey of Intrusion Detection in I nternet of Things. *Journal of Network and Computer Applications* (2017).