# TRUST BASED ROUTING METRIC FOR RPL ROUTING PROTOCOL IN THE INTERNET OF THINGS.

Asma Lahbib[1], Khalifa Toumi[2], Anis Laouiti[1] and Steven Martin[3]

[1]SAMOVAR, Télécom SudParis, CNRS, Université Paris-Saclay,
9 rue Charles Fourier 91011 Evry, France
[2]IRT SystemX, 8 Avenue de la Vauve, 91127 Palaiseau, France
[3]LRI, Université Paris-Sud, 15 Rue Georges Clemenceau, 91400 Orsay, France

## *ABSTRACT*

*While smart factories are becoming widely recognized as a fundamental concept of Industry 4.0, their implementation has posed several challenges insofar that they generate and process vast amounts of security critical and privacy sensitive data, in addition to the fact that they deploy IoT heterogeneous and constrained devices communicating with each other and being accessed ubiquitously through lossy networks. In this scenario, the routing of data is a specific area of concern especially with the inherent constraints and limiting properties of such devices like processing resources, memory capacity and battery life. To suit these constraints and to provide the required connectivity, the IETF has developed several standards, among them the RPL routing protocol for Low powerand Lossy Networks (LLNs). However, and even though RPL provides support for integrity and confidentiality of messages, its security may be compromised by several threats and attacks. We propose in this work TRM-RPL, a Trust based Routing Metric for the RPL protocol in an IIoT based environments. TRM-RPL uses a trust management mechanism to detect malicious behaviors and resist routing attacks while providing QoS guarantees. In addition, our model addresses both node and link trust and follows a multidimensional approach to enable an accurate trust assessment for IoT entities. TRM-RPL is implemented, successfully tested and compared with the standard RPL protocol where its effectiveniness and resilience to attacks has been proved to be better.*

## *KEYWORDS*

*Trust, RPL, QoS, Security, Energy efficiency, IoT, IIoT*

## 1. INTRODUCTION

With the advancement in mobile computing and wireless communication, a new paradigm known as IoT has emerged enabling a seamless integration of physical smart devices within the Internet infrastructure, promoting as a consequence thereof a new generation of innovative and valuable services provided by various application domains and industrial systems such as transportation, healthcare and manufacturing systems. The integration of such paradigm within cyberphysical system (CPS) utilizing Cloud Computing (CC) services in addition to big data and data analytics techniques within industrial application scenarios, has introduced the fourth industrial revolution sometimes referred to as Industry 4.0 [1–3]. In smart factories environments smart products know their own identity, specification, history and even control their own production process, to do so a set of specific data need to be collected in real time and sent to some backend storage structure. The collection of such data is guaranteed by IoT devices with different sensing, connectivity, storage, computational, and other capabilities. The resource.

constraints in sensor networks create novel challenges especially in communication and networking in the presence of devices with limited power, computing and storage capabilities and above all unreliable connectivity. For that reason, several standards and protocols were proposed by the Internet Engineering Task Force (IETF), among them the IPv6 over LOW power wireless Personal Area Networks (6lowPAN) adaptation layer introduced in order to enable IP addressing and connectivity over low power and lossy networks [6]. Nevertheless, routing functionalities were very challenging within 6lowPAN based networks due to the unique characteristics of IoT entities which has arisen an increasing need for an efficient routing protocol for 6LoWPAN compliant IoT networks. Hence the development of RPL, the Routing Protocol for Low power and lossy networks [7], considered later as the standard routing protocol for IoT networks. However and even tough RPL provide support for integrity and confidentiality of messages, its security specifications do not address all possible attacks that may compromise the RPL network which makes it necessary to develop suitable solutions to ensure its security against possible attacks (such as the floodingattack, the routing table falsification attack, the black hole attack, the eavesdropping attack, etc.). In this context, several solutions [8,21] have been proposed in an attempt to bring some enhancements to the RPL standard specification. Nevertheless, little attention has been paid to its security concept and justsome works [9,10,12–14] have investigated and incorporated the trust management aspects within the RPL routing procedures. In this direction, this work proposes a trust based routing metric for the RPL routing protocol with the characteristics of lightweight and high ability to detect, isolate and resist against routing attacks while providing QoS guarantees during the construction and the maintenance of the network routing topology. Such model follows a multidimensional approach to enable an accurate trust value computation for IoT entities. It uses security aspects, QoS factors, energy considerations in addition to the reputation parameters considered by participating entities to assess the trustworthiness of their neighboring ones. Thereafter, and based on the proposed trust aware routing metric, a new RPL objective function is developed in order to rank participating entities at the topology establishment and to calculate the most trusted path from each source entity to the root. A set of evaluation results are then analyzed and discussed, to demonstrate the feasibility of our proposal. TRM-RPL is a trust based routing metric for RPL, predicated on our earlier proposed work presented in [14]. However in this last, validation was performed regarding two set of attacks namely black hole and grey hole attacks, this study addresses another kind of routing attack for which a set of experimental results will be provided. In addition, it enforces the multidimensional aspect of our model and more specifically that relatedto its security dimension. The rest of this paper is organized as follows. Section 2 overviews the RPL protocoland presents related proposals regarding its security enhancements and trust aspects. Thereafter, Section 3 provides a brief description of the important properties to be considered as well as the main objectives we attempt to accomplish. Afterwards, an overview of the proposed scheme, its dimensions and the main blocksit relies on is given in Section 4. Section 5 delves into the integration of the proposed scheme within the RPL protocol, a detailed scenario will be presented then. In Section 6, a set of experimental results validating our approach are shown, and finally in Section 7, the paper ends up with some conclusions and an outlook of our future work in this area.

# 2. BACKGROUND AND LITERATURE REVIEW

## 2.1. Routing Protocol for Low Power and Lossy Networks

RPL, developed by the IETF working group, is an IPv6 routing protocol specifically designed for LLNs with very limited resources in terms of energy, computation and bandwidth. This protocol mainly targets collection based networks made up of nodes interconnected according to a specific topology called Destination Oriented Directed Acyclic Graphs (DODAG), where sink nodes and gateways act as the roots of the Directed Acyclic Graphs (DAGs). Within each DODAG, each node is assigned a rank representing its position in the graph. Its computation depends on a set of specific routing metrics (e.g. delay, link quality, throughput,etc.). The translation of these metrics into ranks is based on an Objective Function (OF) responsible for rank computation and parent selection. The DODAG construction and maintenance phases are based on a set of control messages namely DODAG Information Object (DIO) delivered by the DODAG root to build routes, DODAG Information Solicitation (DIS) broadcast by nodes willing to join the network, Destination Advertisement Object (DAO) used to propagate reverse route information and Destination Advertisement Object Acknowledgement (DAO-ACK) messages sent as an acknowledgement of DAO messages.

## 2.2. Review of Existing Works

Several trust management schemes have been developed in the literature in the context of wireless networks ([15], [16], [17]) to ensure secure routing by protecting the network against misbehaving and selfish nodes thatgenerally aim to attack the routing protocol by dropping, modifying and altering the transmitted routing packets, as well as disrupting the routing processes. The integration of trust could solve efficiently the problems to be faced when securing the routing scheme. However the proposed schemes are particularly dependent on the environment they targeted and the routing protocol they are designed to be integrated within. Additionally, some of them have been tailored to wireless sensor networks, without considering the inherent requirements and features of IoT scenarios and more specifically those related to smart factories environments. In fact they do not keep in view wireless interference, QoS and energy constraints which make them little suitable to IoT devices used within smart factories. When it comes to these networks, we may found several enhancements of the RPL protocol. Some of them have just focused on its evaluation [19,20], others have tried to enhance its performance [21,22], while just few ones have addressed its security and trust aspects [23, 24].

In [21], authors tried to overcome the limitations of the standardized RPL OFs providing thereof QoS guarantees for LLNs while considering several routing metrics. However the security aspect was not considered within the proposed approach keeping as a consequence thereof the routing protocol under threat of attacks. This threat analysis was presented in [24] where authors have detailed and classified the different attacks that could be initiated against the RPL protocol according to the attacker's goal as well as the network element to be impacted.

To secure the communication in an RPL based network, authors in [9] used the trusted Platform Module to establish trustworthiness of nodes before exchanging keying material. However, the trustworthiness assessment was only considered for keys' exchange mechanism to verify the identity of their suppliers and not for the routing path selection and establishment. In [10], authors have proposed trusted-RPL in order to strengthen RPL by adding a new trust worthinessmetric during the construction and the maintenance phases of its instances. The trust assessment is based on the evaluation of the neighboring nodes' behaviors during the topology

construction using selfishness, energy, and honesty components. However, they have not proven the defense of the proposed scheme against attacks that could be launched.

For this reason, an amelioration was proposed in [11] which takes into account trust along the path using collaborative trustworthiness evaluation between the different nodes.

In [12], authors have presented Sectrust, a lightweight SECure trust-based routing framework for IoT nodes. The trust evaluation is based specifically on the successful interactions between

IoT nodes and its calculation is based on some metrics such as the prospect of the positive interaction between the different nodes, their satisfaction and their energy level as well. However, although the proposed framework was designed to isolate common routing attacks, its effectiveness under these threats has not been proven nor evaluated.

In [13], a new RPL routing scheme based on lightweight trust computations was proposed as an objective function to secure the RPL network. The evaluation of trust was based on the positive and negative interac-tions regarding a specific target. Therefore, the topology is updated and misbehaving nodes are removed from the routing graph.

In [14], authors have focused on the design and the integration of a novel Link reliable and trust aware model into the RPL routing protocol. The proposed model targets both node and link trust and follows a multidimensional approach to enable an accurate trust value computation for IoT entities during the construction and the maintenance phases of RPL instances.

A summary of proposed secure schemes for RPL is presented in Table 1. As seen, current IoT research has not yet fully and comprehensively investigated how to secure the routing processes in RPL based networks especially those related to the routing topology construction and maintenance phases, the communication establishment and progress and above all how to trust the participating entities and how to secure the network against the different threats and attacks this protocol is exposed to. In this context, several issues need to be seriously considered and more investigated. On the one hand, the trust integration within the routing functions could affect the performance of the routing protocol as longerpaths could be selected to avoid malicious nodes and thus it could cause a more important delay and energy. On the other hand, more research is required in terms of QoS consideration, and attacks resiliency. In fact proposed schemes are generally designed to defend a specific class of attacks while trust could deal with various kind of attacks while meeting both the energy and the QoS requirements. For this purpose, an inspiration could be taken from other similar areas to IoT such as MANETs and WSNs where extensive research has been carried out and several approaches have been proposed regarding trust management for routing procedures. In an attempt to solve such issues, we have tried in our previous proposal [14] to integrate a novel link reliable and trust aware model within the RPL routing protocol. As an amelioration to that proposal, we tried in this version to enforce the multidimensional aspect of our model and more specifically that related to its security dimension. Obviously, more experiments were carried out to prove its efficiency.

Table 1. Comparison of trust based routing protocols

| **Work/Referen ce** | **Performance metrics** | **Addressed attacks** | **Advantages** | **Limitations** |
|---|---|---|---|---|
| Towards a trustcomputing architecture for RPL in Cyber Physical Systems [9] | Not considered | Cryptographic attacks | - Provides node authentication.<br>- Avoids suspicious routing information | - trust is done only for exchanging keys securely, not for routing. |
| trusted RPL[10] | Selfishness,en ergy and honestyNot considered | Not considered | - Adds new trustworthiness metric during the construction and the maintenance of the routing topology. | - Does not consider the trust value along the path.<br>- Simulation and real implementation is still missing. |
| Lightweight SECure trust based routing framework for IoT(SEC-trust) [12] | Prospect of positive interactions, satisfaction level,checks um value and node energy level | Blackhole and Greyhole attacks | - Secure routing decisions among nodes are made, unreliable routes are isolated.<br>- Could be adapted to other environments like e-commerce, online shopping and social media | - Simulation and real implementation is still missing. |
| Trust-based Resilient Routing Mechanism for IoT[13] | Positive and negative interactions | Not considered | - Represents trust by opinion triangles | - Considers just the direct trust and not the recommendati ons |
| Link reliable and trust aware RPL for IoT [14] | Node cooperativene ss and competence. Link quality and performance | Blackhole and Greyhole attacks | - Targets both node and link trust<br>- Follows a multidimensional approach to enable an accurate trust value computation | - Considers just one kind of attacks (routing attacks) |
| a trust aware Secure Routing Framework in WSNs(TSRF) [15] | trust and QoS metrics (delay and packet loss rate) | On-off attack, conflicting behavior, selfish, bad mouthing and collusion attack | - To avoid false recommendations from misbehaving nodes, an inconsistency check mechanism is incorporated | - Do not keep in view energy and wireless in-terference which leads to dead nodes and compromised network life-time. |

| | | | | |
|---|---|---|---|---|
| | | | | - Do not optimize the end-to-end route selection and maintenance |

## 3. DESIGN CONSIDERATIONS

In this section, we will provide a brief representation of the important properties to be considered with in the proposed scheme as well as the key constraints related to each one of them. Therefore, we will present the main objectives we attempt to accomplish in order to respect such considerations.

### 3.1 Problem Statement

A trusted route within our proposed scheme would satisfy the following properties:

- Trust: a route is trusted if only trusted nodes can participate in its establishment, design and maintenance. On the other side malicious and selfish nodes will be isolated and excluded from participating in the routing procedures. This property could be assessed accurately on the basis of the entities historical interactions and their observation of each other forwarding behavior to judge their trust degree.

- Delay awareness: a delay aware route should be able to provide low end-to-end delays. This property can be measured through the offered end-to-end delay from one source to a destination through a particular route.

- Energy Efficiency: a route is energy efficient if it is made up of nodes that have more energy than any other node. Therefore, an efficient topology construction and route selection for RPL must consider the remaining energy of the nodes to maximize the network lifetime. Obviously nodes with low batterylevels should be avoided in the routing process as much as possible.

- Reliability: a route is reliable if it continuously provide available and high quality of the communication links along the path. This property can be evaluated through the link quality estimators, such as(i) the Packet Reception Ratio (PRR), (ii) the Packet Error Rate (PER) representing the number of incorrectly received data packets divided by the total number of received packets, (iii) the Expected Transmission count (ETX) estimating the predicted number of transmissions required to send packets over a link including re-transmissions

### 3.2.Main Objectives

Taking into account these four properties, a brief description of the main objectives to meet is provided hereafter.

1. Security performance improvement: the main goal of our scheme is to select the most trusted routing path from each participating entity to the gateway regarding their willingness to collaborate with others. Thus the scheme design goal is to maximize the ratio of packets successfully forwarded at each entity level.

2. QoS optimization: our goal here is to optimize the offered QoS taking into account the different QoS parameters such as the delay and the link quality estimators particularly the PRR, PER and ETX estimators. Hence we need a minimized delay, a minimized error rate, a minimized transmission count and a maximized reception rate.

1. 3.Network life time maximization: a network life time could be defined as the time taken until the network partition due to battery failure and power outage. To maximize such parameter, the balancing of the consumed energy across the network may be an effective solution to enhance the network lifetime.

## 4. PROPOSED SCHEME

In the routing context, trust relies on the fact that entities within the routing process do not act maliciously or selfishly regarding the forwarding mechanism. To cope with such kind of behavior, trust could be considered as an efficient solution to secure the routing procedure. In this section, we will describe the overall architecture of our proposed scheme. To efficiently compute trust values and to effectively integrate them within the routing procedures, we first need to clearly understand the main meaning of trust as well as the detailed composition of our system. Furthermore, a brief description of the different blocks and the required interactions to be established will be provided.

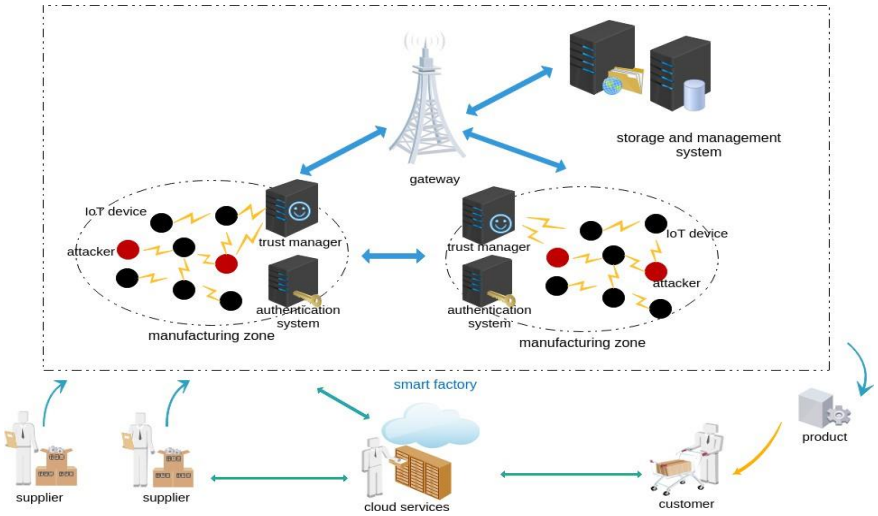


Figure. 1 Network architecture

### 4.1. Overview

The main objective of this work is to propose a novel and multidimensional trust management system for the RPL routing protocol. A new objective function based on our trust model is therefore integrated within the routing protocol and used for its topology construction and maintenance phases. More specifically, our framework aims to define and evaluate a trust score for each entity as well as for the link it is connected through. The evaluated score is then included in the DIO message and used in the rank computation process for the selection of the preferred parent within the DODAG structure. A description of the overall architecture of the proposed system is presented in Figure. 1 above.

## 4.2. System Model

As seen in Figure.1, our system is composed of a number of manufacturing zones constituting the smart factory environment where each zone is made up of a set of physical resources (e.g. machines, ordinary sensors, IoT devices, etc.) along with an authentication manager, which is responsible for making authorization decisions, verifying devices identities and generating authorization tokens. Furthermore, each device is connected to a trust manager, which is in charge of assessing the trustworthiness degree as well as aggregating and computing a final trust score for each participating device within the manufacturing zone according to the proposed model in Section. 4.4. In the case of IoT devices with tight resource constraints, this entity is assumed to be deployed in a more powerful network component that will be connected directly to each device, otherwise it is deployed within the device itself. Thereafter, a storage and management system is deployed to supervise devices state as well as any information associated with them, taking into account their quantified trust scores analyzed, processed and stored within the storage structure.

## 4.3. Trust Definition

A trust management system is often needed to produce reaction based on the real time evaluation of neighboring entities behaviors during established interactions in addition to feedbacks and recommendations gathered from indirect neighbors. These last aggregated together form an overall trust score that once shared and propagated over the network, participating entities could isolate malicious ones and consider secure and trustworthy routing paths for their communications. In our proposal, trust is defined as a relationship between two entities, a trustor and a trustee. The trustor is the evaluating entity willing to join the DAG structure or to update its preferred parent in order to send its data packets. On the other side, the trustee is the evaluated entity which represents the candidate entity that would be chosen as the next hop to the root. This relationship is restricted to a time value, that is, the time in which the evaluation has been carried out. Moreover, this relationship is derived from direct observations and interactions referred as the direct trust and the recommendations exchanged between neighboring nodes termed as the indirect trust.

## 4.4. Proposed model detailed design

A description of the different phases of the proposed model is presented in Figure. 2. This model involves a cyclic succession of operations namely topology creation, authentication, information gathering, trust composition, trust storage, nodes filtering and trust application. It includes as well two main components: an authenticator entity plus a trust manager entity, and four dimensions specifically QoS dimension, Energy awareness dimension, Reputation dimension and Security dimension. These entities and dimensions will be detailed in the next two paragraphs.

### 4.4.1. System Components

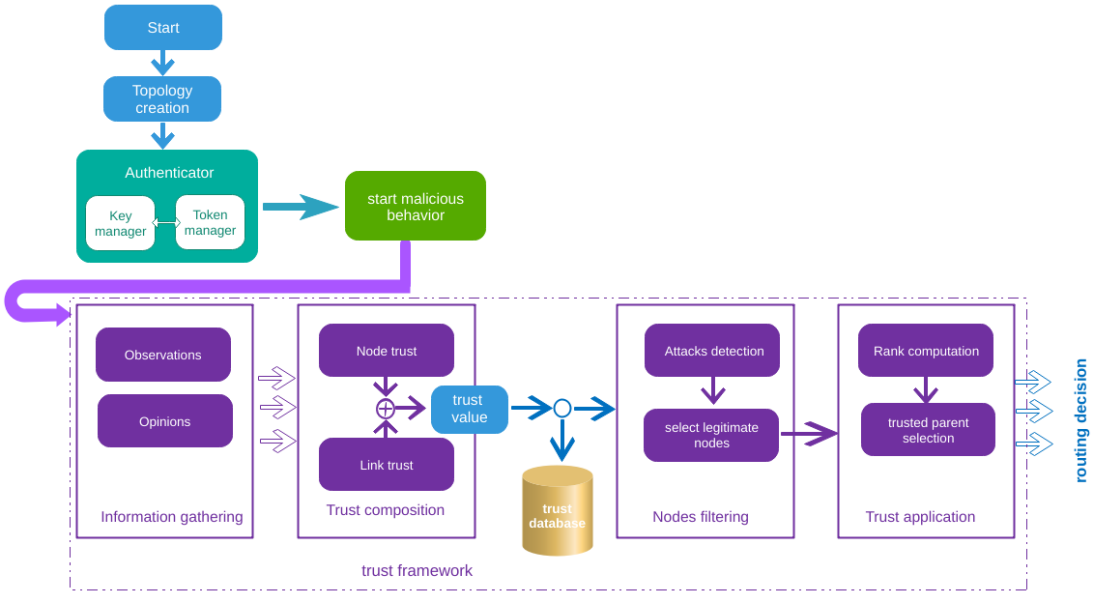


Figure 2. Architecture of the proposed model

**Authenticator:** This entity is mainly responsible for verifying the validity of devices' identities as well as the legitimacy of demands and requests sent to the trust framework. IoT devices and smart objects are authenticated based on the provided credentials. In our framework, we rely on the openID Connect[21] (OIDC) which is an identity layer on top of the OAuth 2.0 protocol [22]. It enables clients to verify the identity of the device based on the authentication performed

by an OpenID Provider, and to obtain basic profile information about the device in an interoperable and REST-like manner [21]. We have chosen OIDC since it has different characteristics related to IoT environments. OIDC is free, open and decentralized (no central authority approves or registers relying parties or service providers). Its integration does not require complicate update in the deployed application. Indeed, it follows a restful approach which make it easy to use and to interoperate. Finally, it gives the possibility to use a JSON structure token that carries information about the device. This entity could be composed of two subcomponents:

I. The Policy Decision Component (PDC): this module is in charge of making authorization decisions based on the policies defined to assign permissions a device has. In case of a successful authentication process, this module generates an access token which is delivered in order to avoid subsequent authentication procedures.

II. The Key Management Component (KMC): this module generates authentication related keys that are used to authenticate devices' validity within the system. Generated keys help to guarantee a level of security of the scheme.

**Trust manager:** This entity helps in the isolation of malicious nodes while providing trustworthy and secure routing paths. Consequently it enables to establish a trusted and reliable environment where devices can interact with each other as well as with external entities and industrial IoT services without worrying about risks related neither to devices changing behaviors nor to

transmitted information confidentiality and integrity. We remind here that the trust framework is assumed to be deployed in the same target entity when it comes to non- constrained devices whereas it could be deployed outside in case of constrained ones. Moreover, as illustrated in Figure. 2, this last is based on five main operational phases namely information gathering, trust composition, trust storage, nodes filtering and trust application.

i. Information gathering: Before being able to produce trust related evidence, each entity has to gather enough information about its neighbors' behavior as well as the links' quality indicators. The trust structure to be sent to the trust manager is made up of the following information: node ID, neighbor ID, RE percentage, PFR value, ETX value, PRR value, PER value, the transmission delay as well as the entity time.

ii. Trust composition: Upon receiving trust related information, the trust manager starts the trust composition process consisting of computing the trust score based on Node Trust (NT) and Link Trust(LT). This value is the weighted average of two parts as follow:

$$T_{ij}(t) = \begin{cases} 0 \;\; if(alert\ generated) \\ w1 * NT_{ij}(t) + w2 * LT_{ij}(t) else \end{cases}$$

$T_{ij}(t)$ represents the trust score an entity ei has for ej at time t. This score is limited to a continuous range from 0 to 1, where 0 denotes complete distrust whereas 1 represents absolute trust.

NTij(t) represents the NT level calculated based on node cooperativeness and node competence.

LTij(t) denotes the LT which is assessed based on link quality and link performance.

The weight factors w1 and w2 are assigned to NTij(t) and LTij(t) respectively where w1+w2=1; 0≤w1≤1 and 0≤w2≤1.
Each computation is based on a set of properties where NTij(t) represents the NT level calculated based on the trustor's direct observation of its one hop neighbors' behavior referred as the direct

trust NTd (t) and on the other hand, on the third parties' attributed recommendations called the indirect or the relative trust NTrij(t)as follow:

NTij(t) = wd * NTd (t) + wr * NTrij(t) , wd and wr are the weights assigned to the direct and the indirect trust respectively.

The direct trust is calculated by considering both node cooperativeness (coop) and node com- petence (comp). At timet, it is defined as:

NTd (t) = NTcoop (t) * NTcomp (t), where NTcoop (t) reflects the cooperativeness level evaluated during the time interval [0..t] and calculated using the Packet Forwarding Ratio (PFR), while NTcompij(t) provides the degree of the entity's ability to perform its intended tasks within the routing process and it is assessed based on the Remaining Energy (RE) percentage hence the energy dimension of our model.

On the other side, the indirect trust NTrij(t) is set up upon recommendations of other entities within the neighborhood which reflects here the reputation dimension. In order to obtain trust recommendations, we first need to select trust recommenders with a trusted communication link, and thus get rid of the impact of malicious recommendations.

When it comes to the link trust LTij(t), its evaluation aims mainly to reinforce the routing DAG establishment and maintenance processes by considering both the quality (qual) and the performance (perf) of the different links connecting the participating entities in order to successfully meet the QoS requirements, its value is defined as follow:

LTij(t) = LTqualij(t) ∗ LTperfij(t) where LTqualij(t) reflects the belief that the connecting link is
efficient enough to respect the QoS guarantees. It is measured by ETX and PRR as indicators of the link quality between the entity and its neighbor. While LTperfij(t) characterize the performance of the link based on the PER and the transmission delay L.

The combination of these properties will produce an overall trust value that can be used efficiently and effectively to ensure security improvement for the RPL routing process.

iii. Trust storage: Once the trust composition process has been completed, trust related evidence will be stored by the trust manager in a trust record table that contains apart the trust information that each entity has gathered for its candidate neighbors, the trust value computed according to the different properties as it has been already explained. To enforce the security aspect of the proposed scheme, a hash algorithm has been employed to encrypt the trust values when stored and retrieved from the trust database or when sent to the evaluating entities.

iv. Nodes filtering: The detection and the isolation of insider attacks is the most important part within a trust framework insofar that malicious nodes are aware of every detail of the network process, they may tamper the content of transmitted packets, deny from sending messages to other legitimate nodes, they can even send fake routes to the legitimate no design order to get the packets or to disturb the operations. Thus a filtering phase is essential to classify network nodes and to isolate malicious ones. The filtering process is mainly based on the trust assessment where nodes whose trust score is above the trust threshold are classified as malicious, otherwise they will be considered as legitimate and thus selected to be candidates for DODAG construction and maintenance process.

v. Trust application, a novel trust based routing metric for RPL routing protocol: The trust model previously described has been integrated into the DODAG construction and maintenance phases of RPL through the development of a new OF in order to rank nodes while calculating the most trusted path from each source to the root. To do so, each node sends to its neighbors the value of its rank which is included by default in the DIO message, once received the evaluating node ejoin will check its record table for the most recent trust values of its $p \geq 1$ candidate parents ecand1..ecandp, already sent by the trust manager. Afterwards, the rank

R(ejoin→ecandq) will be computed according to the trust based OF and with respect to each candidate parent ecandq, according to the formula below:

R(ejoin→ecandq) = R(ecandq)−T(ejoin→ecandq)t

where R(ecandq) is the rank value of the candidate parent. Afterwards, the node with the minimum rank R(ejoin→ecandq) will be chosen as the preferred parent to reach the root.

#### 4.4.2. Main Dimensions

(a) QoS dimension: This dimension refers to the evaluation of the overall QoS provided by the different links along the path. The objective here is to find a path made up of trusted nodes connected by reliable links in terms of link quality and link performance while meeting the end- to-end delay requirements. This evaluation is done using link indicators that include PRR, PER and ETX.

(b) Energy awareness dimension: This dimension refers to the evaluation of the Remaining Energy (RE) of each entity presented as a candidate parent during the construction of the routing path. By this way, only trusted nodes that have residual energy above than a certain specified threshold will be selected.

(c) Reputation dimension: The proposed trust model depends on the neighboring entities' attributed recommendations about a particular entity ej regarding its packet forwarding behavior. Let RTkj be the recommendation about ej given by ek. The trust model weights each recommendation to limit its influence according to the recommender's behavior and on the other hand to the similarities between all the attributed values. Thus, each recommendation coming from a particular entity ek is subject to a credibility factor CRk in the interval [0..1], where 1
represents the highest credibility and 0 the lowest one. Therefore, the reputation property in our trust model is given by $Rkj=RTkj*CRk$.

(d) Security dimension: As it was presented in the network model in Section 4.1, the trust manager after receiving the trust related information sent by the network entities, calculates a trust score for each entity and link by means of a network monitoring and analysis tool that captures the 6LowPAN traffic, renders the network state and identifies the abnormal behaviors related to the RPL routing protocol. In our proposal, we have used the Foren6 analysis tool for6LowPAN/IPv6 networks.[25] The security information collected will be employed after by the trust manager and taken into consideration within the trust computation process.

## 5. SIMULATION AND RESULTS

### 5.1. Simulation Setup

Our experiments were performed using the Instant Contiki 2.7 platform while integrating the proposed trust model (presented in Section 4) into the RPL routing protocol. As we have noted, the Instant Contiki was used as the development environment with the Cooja simulator to implement the proposed model. Let us remind that Cooja provides real environment to build IoT networks with different types of motes, and implemented code could be tested and uploaded to real motes without any modification. The various simulation parameters are listed in Table 2. In this study, we have assumed that the attacking nodes behave as good nodes from inception and begin their malicious activities during time (when activated).

Table 2. Network related parameters used in simulation analysis

| **Simulation parameter** | **Value** |
|---|---|
| Simulation tool | Contiki/Cooja 2.7 |
| Mote type | Tmote Sky |
| Simulation run time | 3600 seconds |
| Simulation coverage area | 300m x 300m |
| Interference range | 100m |
| Wireless communication range | 50m |
| Total number of nodes | 10..50 |
| Number of maliciousnodes | 3..15 |
| Radio environment | DGRM (Directed Graph Radio Medium) |

## 5.2. Performance evaluation results

In order to prove the performance of our proposal, we have performed several simulations in com-parison with RPL and more specifically with RPL based on the MRHOF, Minimum Rank with Hysteresis Objective Function. This last uses hysteresis while selecting the path with the smallest ETX metric value from the source node to the root. In addition, we have varied the number of network nodes, the percentage of malicious ones and we have analyzed the corresponding effect respectively on the Packet Loss Ratio (PLR), the Remaining Energy percentage (RE) and the resiliency to black hole attacks.

### 5.2.1. Remaining energy

We measure here the RE while varying the number of nodes within a network composed of a single DODAG and 30 legitimate nodes. Figure 3 illustrates the distribution of the RE between the network nodes while Figure 4 shows the impact of the network size on the power to be consumed.

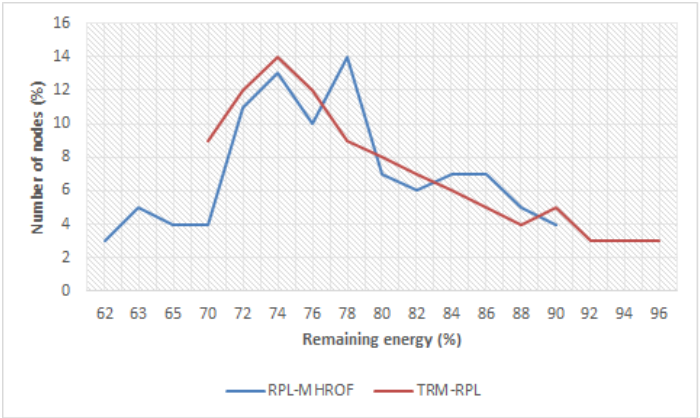


Figure 3. Remaining energy distribution

As seen in Figure. 3, the RE distribution in TRM-RPL based network is more balanced than the normal RPL insofar as relay nodes are chosen function of their RE level during the DAG construction phase which avoids having the same relay node within the routing topology and consequently depleting the power of this last in a faster way as well. The simulation results herereveal that within TRM-RPL, 44% of nodes have a RE above 80%, 14% above 90% and 64% between 70% and 80%. However, we note that within RPL-MRHOF, just 5% of nodes have a RE above 90% and 16% under 70% which could adversely affect the network lifetime

Figure 3. Remaining energy distribution. over time as 16% of nodes are likely becoming to exhaust their batteries in a faster way in comparison with TRM-RPL.

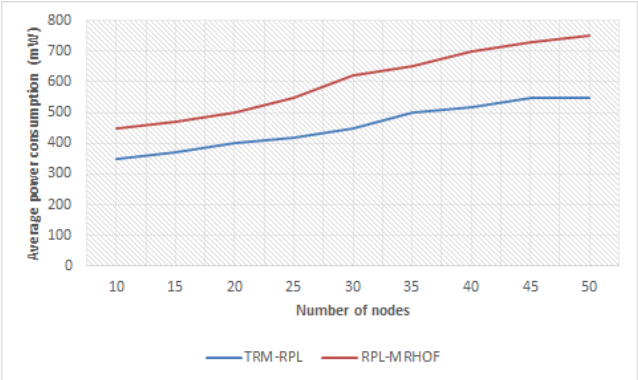


Figure 4. Influence of the network size on the power Consumption

On the other side, when it comes to the network size factor, it is clear that both RPL and TRMRPL consume more energy with the increase of the network size. This increase is due to the additional amount of data and control packets transmitted as each node within a larger network will have more neighbors and consequently it will transmit more control packets which require more power to be consumed. However, the results also show that TRM-RPL consumes less energy when compared to RPL. This high energy consumption for RPL is due to high packet loss. Indeed, a successful transmission consumes less energy than a unsuccessful one. Even with this amount of control packets caused by TRM-RPL, the energy consumption remains low.

**Discussion:** The network lifetime can be defined as the time taken since the simulation begins until the network partition due to battery failure and power outage. We have proved here that TRM-RPL maintains better performance in terms of network lifetime since it performs moderately a certain load balancing on the basis of the RE level of trusted nodes and this even under heavy networks. By this way once a node has a RE level below the specified threshold, it will not be chosen as a preferred parent as long as there are other alternative energy efficient and trusted candidates.

### 5.2.2. Packet loss ratio

We measure here the PLR while varying the number of legitimate and malicious nodes.

Figure 5 shows the variation of the PLR with the increase of the network size while Figure 6 variation in the presence of a number of malicious nodes representing the quarter of the total number of network nodes.

The simulation result in Figure 5 shows that the PLR decreases slightly with the increase in the network size. This is obvious as when there is a high number of neighbors, nodes are able to find alternate paths easily, which reduces packet loss. One can see that TRM-RPL experiences amore reduced packet loss than RPL. This is primarily due to the fact that TRM-RPL takes into consideration more link quality estimators in addition to the node attributes while evaluating the trust worthiness of each candidate parent. Minimizing the ETX, the PER and maximizing the PRR, the RE when selecting the next hop will imply a path with low PLR.

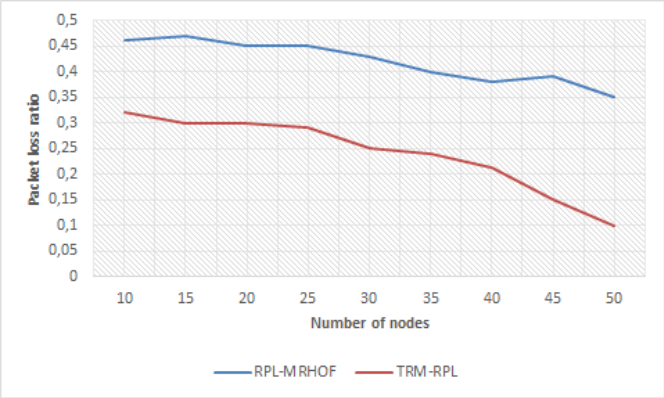


Figure 5. Influence of the network size on the packet loss ratio

### 5.2.3. Comparison of reactions against attacks

In order to prove the effectiveness of our proposal, we evaluate its conduct towards the commonly studied attacks that may occur in trust based routing systems where malicious objects aim to modify the topology of the network and to degrade the performance of the routing protocol. In our experiments, we consider two types of attacks: Black hole attack where malicious node dumps all the packets supposed to be forwarded, and Gray hole attack where malicious node only discard aspecific subpart of the network traffic and forward the other part at random interval. Figure 6 displays a graphical representation of the percentage of packet loss under black-hole at-tacks. While TRM-RPL0 related PLR stayed below 0.4, the standard RPL(MRHOF) recorded as taggering one between 0.6 and 0.95

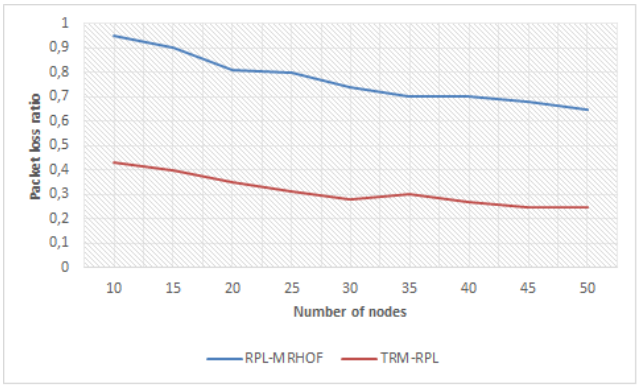


Figure 6. PLR comparison between MRHOF and TRMRPL
under blackhole attacks

Moreover, we have measured the impact of the number of malicious nodes launching black hole attacks on the packet loss. As shown in Figure 7, we can obviously see that the PLR increases when the number of malicious nodes increases respectively for both TRM-RPL and RPLMRHOF.

However, an obvious observation of this simulation result is that TRM-RPL performs better in the presence of malicious nodes since packet loss rate under 0.2 is realized for up to 10 attacking nodes while to 6 attacking ones in RPL-MRHOF. The simulation result in Figure 8 shows well how TRM-RPL detects the malicious behavior of nodes and how it reacts to its presence. The

network here is composed of 50 nodes where 15 among them start to act maliciously over a certain time after the network initialization

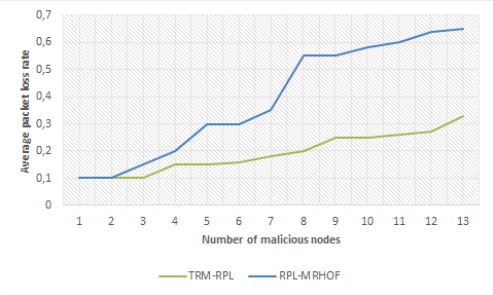


Figure 7. Malicious nodes number impact on the packet loss ratio.

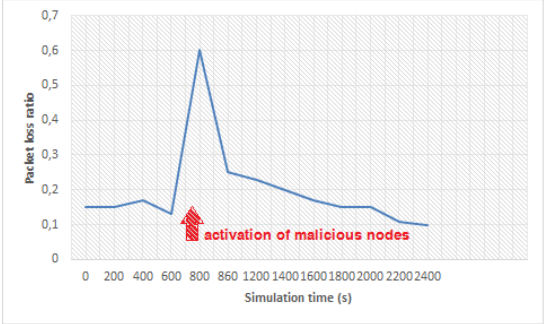


Figure 8.PLR evolution TRM-RPL in a 50 nodes network size.

As shown in Figure 8, once malicious nodes begin their malicious activities consisting of dropping their neighbors' packets, the PLR considerably increase in response to the occurring event. However the integration of the proposed scheme within RPL was shown and proven to be effective in reducing the impact of such behaviors insofar as the attacking nodes will not be chosen anymore as a next hop nodes during the network routing topology construction. As a result thereof, the PLR is reduced and maintained considerably stable over time.

To clearly see the reaction of TRM-RPL in the presence of malicious nodes, we have measured the average trust value while increasing the percentage of activated malicious nodes within a 50 nodes network size where 15 nodes are malicious as illustrated in Figure 9. It is clear that since they start to behave abnormally regarding the packet forwarding behavior, malicious nodes are detected and their trust level significantly drops which justify the decrease of the average trust value of the whole network (the average value of both legitimate and malicious nodes).

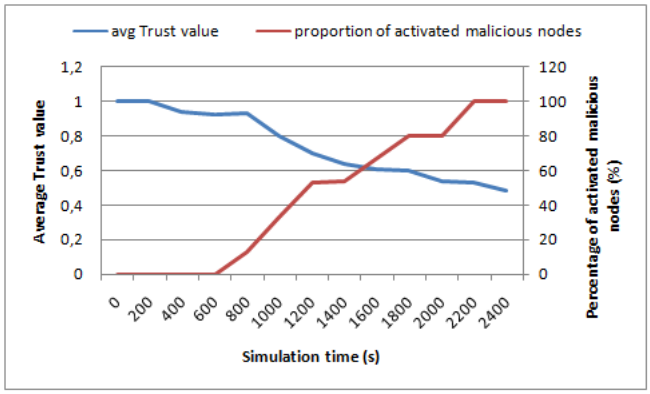


Figure 9. Average trust value evolution

**Discussion:** Our analysis of the packet loss has shown that TRM-RPL gives higher performance incomparison with MRHOF based RPL since it experiences a more reduced PLR even in the presence of malicious nodes launching black hole attacks. The detection, the reaction and the prevention of these behaviors have been proven as well.

## REFERENCES


[1] R. C. Schlaepfer and M. Koch. Industry 4.0 Challenges and solutions for the digital transformation and use of exponential technologies. [Online]. Available: https://www2.deloitte.com/content/dam/Deloitte/ch/Documents /manufacturing/ch-enmanufacturing-industry-4-0-24102014.pdf

[2] K. Schwab. The Fourth Industrial Revolution. World Economic Forum, 2016.

[3] H. Kagermann and W. Wahlster, Industrie 4.0 - Smart Manufacturing for the Future. German Trade and Investment, July 2014. [Online]. Available: https://www.gtai.de/GTAI/Content/EN/Invest/_SharedDocs /Downloads/GTAI/Brochures/Industries/industrie4.0-smart-manufacturing-for-the-future-en.pdf

[4] Miorandi, D., Sicari, S., De Pellegrini, F., & Chlamtac, I. (2012). Internet of things: Vision, applications andresearch challenges. Ad Hoc Networks, 10(7), 1497-1516.

[5] Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015). Internet of things: A survey onenabling technologies, protocols, and applications. IEEE Communications Surveys & Tutorials, 17(4), 2347-2376.

[6] Kushalnagar, N., Montenegro, G., & Schumacher, C. (2007). IPv6 over Low-Power Wireless Personal AreaNetworks (6LoWPANs): Overview, assumptions, problem statement, and goals. Internet Eng. Task Force (IETF),Fremont, CA, USA, RFC4919, vol. 10.

[7] Routing Over Low Power and Lossy Networks (ROLL), 2004. Available: https://datatracker.ietf.org/wg/roll/charter/.

[8] Iova, O., Theoleyre, F., Noel, T. (2015). Using multiparent routing in RPL to increase the stability and thelifetime of the network. Ad Hoc Networks 29(0), 45-62.

[9] Seeber, S., Sehgal, A., Stelte, B., Rodosek, G. D., & Schonwalder, J. (2013, October). Towards a trust computingarchitecture for RPL in CPSs. In Network and Service Management (CNSM), 2013 9th International Conferenceon (pp. 134-137). IEEE.

[10] Djedjig, N., Tandjaoui, D., & Medjek, F. (2015, July). trust-based RPL for the Internet of Things. In Computersand Communication (ISCC), 2015 IEEE Symposium on (pp. 962-967). IEEE.

[11] Djedjig, N., Tandjaoui, D., Medjek, F., & Romdhani, I. (2017, April). New trust metric for the rpl routing protocol.In Information and Communication Systems (ICICS), 2017 8th International Conference on (pp. 328-335). IEEE.

[12] Airehrour, D., Jairo, G., & Sayan, K.R. (2016). A Lightweight trust Design for IoT Routing. Dependable, Autonomic and Secure Computing, 14th Intl Conf on Pervasive Intelligence and Computing,2nd Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress(DASC/PiCom/DataCom/CyberSciTech), 2016 IEEE 14th Intl C. IEEE.

[13] Khan, Z. A., Ullrich, J., Voyiatzis, A. G., & Herrmann, P. (2017, August). A trust-based Resilient RoutingMechanism for the Internet of Things. In Proceedings of the 12th International Conference on Availability, Reliability and Security (p. 27). ACM.

[14] Lahbib, A., Toumi, K., Elleuch, S., Laouiti, A., & Martin, S. (2017, October). Link reliable and trust awareRPL routing protocol for Internet of Things. In Network Computing and Applications (NCA), 2017 IEEE 16thInternational Symposium on (pp. 1-5). IEEE.

[15] Duan, J., Yang, D., Zhu, H., Zhang, S., & Zhao, J. (2014). TSRF: A trust-aware secure routing framework inwireless sensor networks. International Journal of Distributed Sensor Networks, 2014.

[16] Zhan, G., Shi, W., & Deng, J. (2012). Design and implementation of TARF: A trust-aware routing framework forWSNs. IEEE Transactions on dependable and secure computing, 9(2), 184-197.

[17] Ahmed, A., Bakar, K. A., Channa, M. I., Haseeb, K., & Khan, A. W. (2015). TERP: A trust and Energy AwareRouting Protocol for Wireless Sensor Network. IEEE Sensors Journal, 15(12), 6962-6972.

[18] Winter, T. (2012). RPL: IPv6 routing protocol for low-power and lossy networks.

[19] Tripathi, J., de Oliveira, J. C., & Vasseur, J. P. (2010). A performance evaluation study of rpl: Routing protocolfor low power and lossy networks. Information Sciences and Systems (CISS) 44th Annual Conference on (pp. 1-6).IEEE.

[20] Accettura, N., Grieco, L. A., Boggia, G., & Camarda, P. (2011). Performance analysis of the RPL routing protocol.In Mechatronics (ICM) IEEE International Conference on (pp. 767-772). IEEE.

[21] Gaddour, O., Koubaa, A., & Abid, M. (2015). Quality-of-service aware routing for static and mobile IPv6-basedlow-power and lossy sensor networks using RPL. Ad Hoc Networks, 33, 233-256.

[21] N. S. et al., Openid connect core 1.0, OpenID Foundation, Tech. Rep., February 2014

[22] Hardt, Dick. The OAuth 2.0 authorization framework. (2012)