Enhancing RPL Resilience Against Routing Layer Insider Attacks

Karel Heurtefeux
Qatar Mobility Innovations Center
Doha, Qatar
karelh@qmic.com

Ochirkhand Erdene-Ochir
Texas A&M University at Qatar
Doha, Qatar
o.erdene-ochir@qatar.tamu.edu

Nasreen Mohsin
Qatar Mobility Innovations Center
Doha, Qatar
nasreenm@qmic.com

Hamid Menouar
Qatar Mobility Innovations Center
Doha, Qatar
hamidm@qmic.com

***Abstract*—To gather and transmit data, low cost wireless devices are often deployed in open, unattended and possibly hostile environment, making them particularly vulnerable to physical attacks. Resilience is needed to mitigate such inherent vulnerabilities and risks related to security and reliability. In this paper, Routing Protocol for Low-Power and Lossy Networks (RPL) is studied in presence of packet dropping malicious compromised nodes. Random behavior and data replication have been introduced to RPL to enhance its resilience against such insider attacks. The classical RPL and its resilient variants have been analyzed through Cooja simulations and hardware emulation. Resilient techniques introduced to RPL have enhanced significantly the resilience against attacks providing route diversification to exploit the redundant topology created by wireless communications. In particular, the proposed resilient RPL exhibits better performance in terms of delivery ratio (up to 40%), fairness and connectivity while staying energy efficient.**

I. Introduction

Low-power Lossy Networks (LLNs) are formed by a hundreds or thousands of constrained network devices with limited processing, memory, and energy when they are battery operated or energy scavenging. In this context, the Routing Over Low power and Lossy networks (ROLL) working Group was formed in Internet Engineering Task Force (IETF) to develop an adapted routing solution. After 4 years, RPL was adopted by IETF in March 2012 [1].

A typical example of such networks is Wireless Sensor Networks (WSNs). WSNs have become popular in gathering data from multifunctional sensor devices which communicates wirelessly at short distance to collect and transmit data to data collectors. Security is particularly challenging in WSNs not only due to the limitation of the capabilities of the sensors, but also because of their open and unattended deployment, in possibly hostile environments. Powerful adversaries can easily launch Denial-of-Service (Dos) attacks, cause physical damage to sensors, or even capture them to extract sensitive information (encryption keys, identities, addresses). In this case, sensor node is considered as compromised and an attacker could introduce numerous malicious activities such as injecting bad data to the network to control actions, and/or introduce numerous attacks such as Selective forwarding, Sinkhole, Sybil, node replication, Wormhole, etc. to disrupt data gathering process.

Motivations. RPL is one of the first routing standards available for wireless sensor and constraints networks. As a recent protocol, RPL has not been fully and deeply studied and assessed [2], [9], [17], in particular on the security vulnerabilities. In a previous paper [10], we have shown that the RPL's logical structure, DODAG (Direction-Oriented Directed Acyclic Graph), is supported by only few nodes. This particular structure has been found to be sensitive to node failures and we believe, it could be also sensitive to physical attacks.

Even though the security functionalities have been considered in RPL, they are based on the traditional cryptographic solutions which provides authentication, confidentiality and integrity and do not provide protection against compromised nodes allowing an adversary to be considered as a legitimate node inside the network. In this study, we investigate a security threat known as the selective forwarding or gray hole attack. In a selective forwarding attack, a compromised node refuses to forward all or a subset of the packets it receives. As per a multihop routing is based on the cooperation between nodes to route the traffic, such attack is very damaging for such networks and recent studies show that this vulnerability should be taken seriously [14], [19]. In addition, selective dropping is challenging to detect due to the uncertainty if that packet loss is due to medium access collision, bad channel quality or because of selective forwarding attack. Moreover, traditional security properties (confidentiality, integrity, authentication, etc.) provided by cryptographic algorithms are inoperative in such context.

Because RPL behavior under real-world dynamics is still not mature, it needs simple and efficient by design security mechanisms. In such a context, algorithmic approaches are needed to complement cryptographic solutions to mitigate insider attacks. Resilience is required to tolerate such attacks by RPL protocol.

Novelty. As per our best knowledge, this is the first study proposing to enhance the resilience of RPL protocol by design. Resilient techniques such as random routes and data replication are introduced to RPL protocol to provide route diversification in order to take advantage of the structural redundancy created by wireless communications.

Contributions. The contributions include:

- Firstly, a study evaluating the classical RPL performance in presence of packet dropping malicious insiders has been conducted on the Contiki/Cooja simulator. Cooja is a Java-based simulator compiling

and executing Contiki 2.7 operating system for a native platform as a shared library.
- Secondly, this paper presents 2 variants of RPL to enhance its resilience (*i.e.* its capacity to deal with node and link unreliability and node compromise due to an insider attacks) and their performance is compared with the classical RPL protocol in adversary condition.

The rest of this paper is organized as follows. Section II provides an overview of previous work emphasizing on information which is relevant in the context of this paper: previous studies on RPL and the resilience concept are discussed. In Section III, RPL functionality is briefly described. In Section IV, resilient techniques based on random routes and data replication are introduced to RPL considering its specificity. Section V provides resilience evaluation through simulations of RPL protocol and its resilient variants. Finally, Section VI concludes and discusses potential further work directions.

II. Related Work and Scope

In this section, a comprehensive overview of RPL performance studies is presented. A discussion on the resilience concept is also proposed and compared with other close notions such as survivability and robustness.

A. Performance Studies on RPL

Before the standardization of RPL protocol, the authors in [18] experimentally exposed that the gradient-based routing, proposed by IETF ROLL, was robust against topological changes. The routing process of RPL is based on such gradient. They implemented a gradient-based protocol, similar to RPL, on TI eZ430-RF2500 platform (MSP430 microcontroller with 2.4GHz CC2500 radio). To investigate their protocol robustness, they deployed 12 nodes during 8 hours, sufficiently far from each other to obtain weak links. The node degree variation and delivery ratio are measured. Despite the constantly changing topology, 74% of sent packets had reached the sink. However, the robustness was not studied in case of nodes outage or adding new nodes. Moreover, the small number of deployed nodes reduces drastically some common issues: collision, interference or bottleneck [12].

In [17] and [2], the authors present a performance evaluation of RPL based on simulations. In [17], the simulations are performed with topology and link quality data from a real sensor network. The authors investigated path quality, routing table size, control packet overhead and connectivity. They observed that the number of control packets decreases during the simulations and the stabilization of the DODAG (Destination Oriented Directed Acyclic Graph). In [2], the authors show that RPL allows a fast network set-up: however, contrary to [17], they also find that RPL has an important control packet overhead during the simulation. In this study, the considered hypotheses on the simulation environments are strong: Unit Disk Graph (UDG) and uniform packet error rate. They do not reflect what is generally observed in real environments. For instance, the packet error rate is often more important next to the sink due to a bigger congestion.

[9] presents the most relevant research effort proposed for RPL, and an experimental performance evaluation of RPL. The experimentations are based on 30 TelosB motes, and give a performance evaluation in terms of packet loss, packet delay, DODAG time convergence and power consumption. However, the authors did not investigate the impact of power transmission on packet delivery ratio, the overhead and the robustness against node failures.

More recently, [10] conducted a study on 2 large WSN platforms. The behavior of RPL has been investigated in terms of delivery ratio, control packet overhead and dynamicity when nodes are removed or added to the network. This previous paper shows that the stability of the routing structure could be affected when few nodes fails. However, the paper focus on hardware or software failures. The current paper investigates the RPL's performance dealing with malicious behavior such as selective forwarding attack.

B. Concept of Resilience

Resilience study encompasses a wide range of multidisciplinary research topics and it is still a relatively new concept in networking. This term is originally defined in physics to characterize the mechanical properties of the materials to resist a shock, and later used also in several fields such as psychology, ecology and economics. In the field of networking and telecommunications, resilience has been initially defined in relation to fault tolerance [8].

Several similar concepts such as *survivability* [5], *robustness* [16] and *resilience* [15] have been considered in the literature. The common point of these approaches is not considering specifically physical compromission due to *insider* attacks which pose even more severe damages in the network than faulty nodes. Node compromise is particularly challenging issue and creates numerous security and reliability vulnerabilities as discussed previously. By considering node compromise in the network, the resilience is defined as the ability of a network to absorb the performance degradation under some failure pattern (random or intentional) and to continue delivering messages with an increasing number of k compromised nodes [13], and several resilient routing techniques have been proposed in [6]. In this paper, we adopt this concept to enhance the RPL protocol resilience.

III. RPL Overview

RPL [3] is a hierarchical, proactive and IPv6 distance vector protocol. It constructs a DODAG and the data packets are routed through it. DODAGs have the property that all edges are destination oriented in such a way that no cycles exist. Based on DODAG, each node has a rank, which defines the node's position relative to other nodes with respect to the DODAG root. The node's rank strictly increases from the root towards the leaf nodes. The rank is computed depending on the DODAG's objective function (OF): hop counts, link metrics such as expected transmission count (ETX) [4], or other constraints. To build and maintain its logical topology (route, parents, neighbors table), RPL uses IPv6 control messages: DIO (DODAG Information Object), DIS (DODAG Information Solicitation), and DAO (Destination Advertisement Object). Finally, RPL has been designed to deal with constraints in energy and channel capacity. As a result, to reduce the control messages overhead, RPL uses a slow proactive process to

maintain a routing topology but a reactive process to resolve routing inconsistencies [3].

IV. Resilient RPL

In our previous work, several resilient routing techniques have been proposed [6] consisting of two elements : (i) introduction of random behavior and (ii) introduction of data replication. Random behaviors increase uncertainty for an adversary, making the protocols unpredictable. It allows route diversification between a source and a destination, thus improving the delivery success and fairness. Data replication takes advantage of route diversity by random behavior to increase delivery success. The present study extends widely this work by implementing the resilient techniques to the standardized routing protocol RPL. It also considers a realistic propagation model and an hardware emulation of sensor nodes running ContikiOS.

A. Randomized RPL

Classical RPL routing protocol selects the best parent depending of the OF in order to increase the routing efficiency and minimize the energy consumption. The presence of a single compromised node on the best route leads to a complete disconnection of a source from the sink. Hence, a random behavior in route selection is introduced according to RPL protocol specificity to increase the route diversity. By default, a RPL node maintains information on its neighbors and identifies a set of potential parents. In order to introduce a random behavior in the route selection, packets are sent to random potential parents instead of the best parent. Therefore, packets can dodge the malicious nodes on one of its random routes insuring those packets reach its destination safely.

B. Randomized RPL with Data Replication

To improve delivery success, the packet duplication is introduced at the sources. If the original packet is lost, the replicated copy could reach the sink successfully. The classical RPL protocol cannot take advantage of data replication as a source uses the same best route for all messages, whereas the randomized variants may increase the delivery success due to route diversification for each message. Nodes are programmed to duplicate their own packets and send them to randomly selected parents. The forwarding nodes do not duplicate data packets but instead forward those packets to the sink again through randomly selected routes. In case one of the packets is lost on its selected route due to compromised node, its duplicate can continue to reach the sink through another route due to random selection thereby increasing delivery success.

V. Resilience Evaluation

In this Section, we study through simulations, the influence of (i) insider attacks on the performance of classical RPL protocol (ii) random behavior and data replication introduced to RPL.

Node position	Random
Size of the deployment area	100m x 100m
Number of Nodes	50
Sensor Nodes	Tmote Sky Board (MSP430-based board with a CC2420 radio chip)
Propagation model	Unit Disk Graph Model, Transmission range: $20m$, Interference range: $30m$
Physical Layer	IEEE 802.15.4
MAC Layer	ContikiMAC, IPv6
Network Layer	ContikiRPL
Transport Layer	UDP
DATA packet period	45 s
Simulation duration	1h
Objective Functions	Hops count and ETX

TABLE I: Summary of the simulation parameters.

A. Assumptions and Simulation Parameters

The results have been obtained through simulations on Contiki/Cooja, a network simulator for wireless networks. 50 Tmote Sky emulated nodes (*i.e.* the entire hardware is emulated) are randomly deployed on a plane square and are considered motionless. Each node periodically sends data packets to one data collector called the sink. In these simulations, one sink is assumed to be at the centre of the field. RPL protocol is considered to maintain a logical structure and routing the data packets. The default RPL's OF (*i.e.* how a RPL node selects and optimizes routes based on the information objects available) is considered, using hop counts and ETX as metrics. Due to the time needed for emulation-based simulation, the results are averaged over 10 simulations. Table I sums up the simulation parameters.

B. Adversary Model and Scenarios

In this article, we deal with an *insider* attacker, where ordinary network devices can be captured and compromised, and who is *active* with the intention to disrupt communications in the network. *Selective forwarding* attack [11] is considered, where relaying malicious nodes drop all data packets instead of retransmitting. We consider this attack not only because it is common to all protocols but also because reliable data delivery characterizes the success of routing protocols. k represents the probability for each node to be compromised.

Three scenarios have been defined: Classical RPL using the Contiki2.7 implementation ; Randomized RPL and Randomized RPL with data replication as defined above.

C. Evaluation Metrics

To gain insight concerning the RPL performance and its resilience in presence of insider attacks, the following metrics are measured:

Average Delivery Ratio represents the ratio between the total number of packets successfully received by the sink and the number of packets sent by the sources. This is an important metric to evaluate the success of routing functionality, i.e., packet delivery;

Jain's Fairness Index is defined by the Raj Jain's equation: $\frac{(\sum_{i=2}^{n} x_i)^2}{n \sum_{i=2}^{n} x_i^2}$ with x_i, the throughput for the ith node.

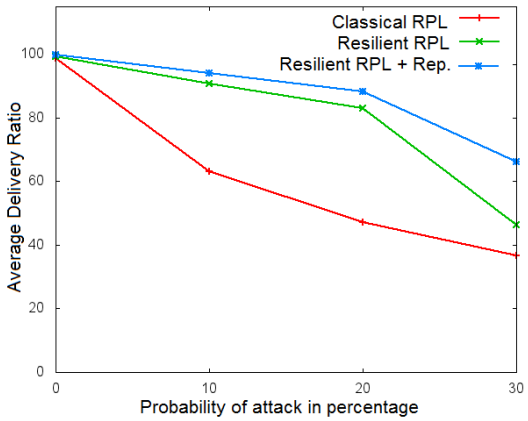

Fig. 1: Average delivery success for the RPL protocol variants.

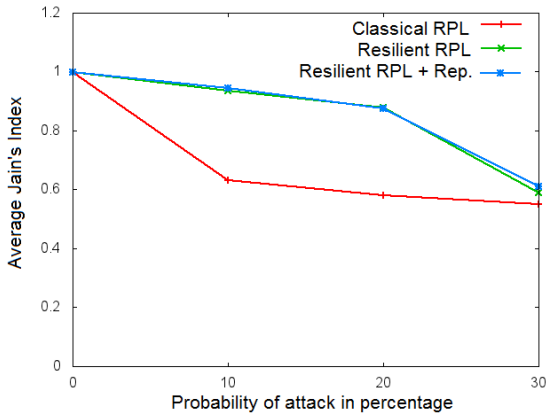

Fig. 2: Delivery success distribution among all network nodes.

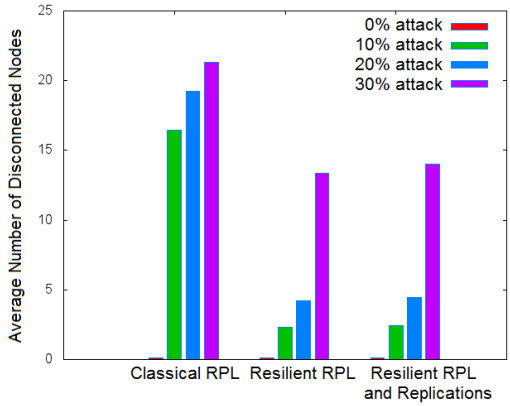

Fig. 3: Disconnected nodes according to the RPL protocol variants.

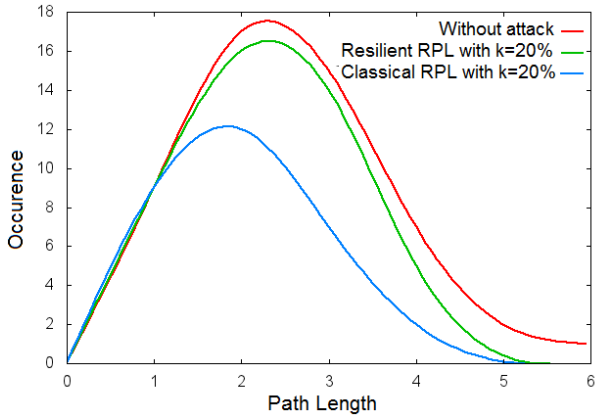

Fig. 4: Distance in hops of connected nodes.

It characterizes both facts that the packets from the sources will eventually reach the sink as the data delivery success distribution among the sources. The distribution should be as uniform as possible for a good geographic coverage.

Normalized Power Consumption defined as the overall energy expenditure normalized by classical RPL without attacks. It characterizes the network efficiency in terms of protocol overhead. RPL routing protocol designed for low power and lossy networks should be able to save energy.

Average Path Length is the number of hops crossed for each received packet. This allows to determine the number of forwarding nodes of a route.

D. Results and Analysis

Simulation results of the classical RPL routing protocol and its resilient variants are presented considering the attacks described in Section V-B and the metrics defined in Section V-C.

1) Data Delivery Success: Firstly, we present the data delivery success in presence of attacks in the network. As expected, the average delivery ratio (ADR) decreases for all RPL variants with increasing intensity of attacks (Figure 1). ADR decreases rapidly for classical RPL, because the route selection is deterministic based on the best route principle (shortest path). In classical RPL and in absence of dynamic in the network (link or node failures), a source uses the same route to deliver packets to the sink. However, if the selected route is compromised due to faults or attacks, all data packets from the source will be lost.

In contrast, the randomized RPL, or resilient RPL, allows to diversify routes between a source and a destination by sending each data packet through randomly selected route among alternative routes. With the randomized RPL, not only the average delivery ratio has increased as shown on Figure 1, but also the delivery fairness has risen (Figure 2). This is due to the route diversity created by random route selection ; each sent data packet may take potentially different route. As we observe on the Figure 3, the number of disconnected sources also decreased for randomized RPL. The network connectivity is so improved, since a larger number of devices remains connected to the sink despite increasing intensity of attacks, even with low average delivery success. In addition, Figure 5 shows that random behavior introduced to RPL does not increase significantly the route length in absence of attacks

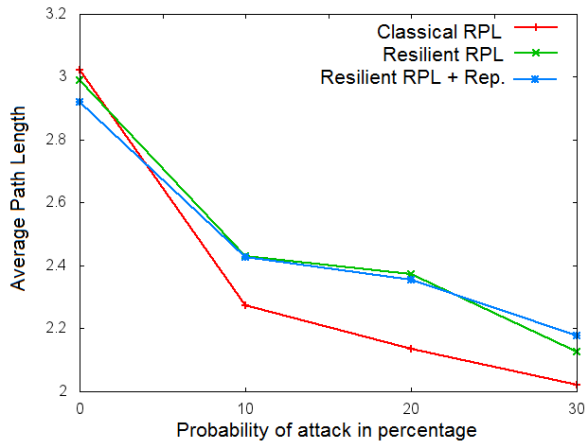

Fig. 5: Average path length of received packets.

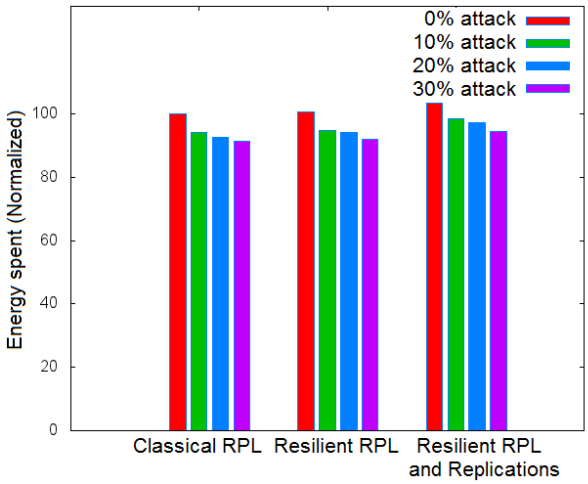

Fig. 6: Total energy consumption of the network.

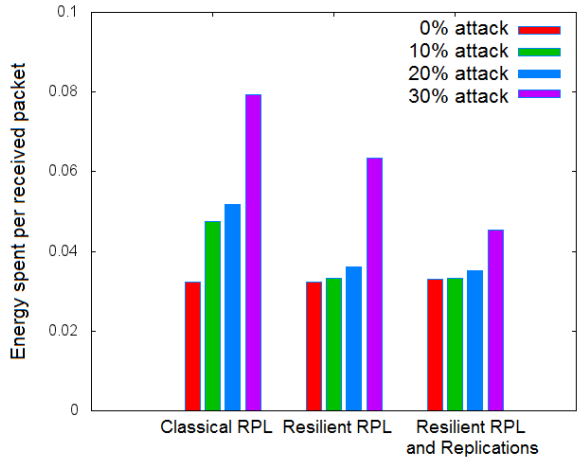

Fig. 7: Energy consumption per received packet.

because the random selection is provided among shortest paths (*i.e.* using parents with a rank similar to the best parent's rank). In presence of attacks, the average path length decreases as the received messages mostly come from the devices close to the sink. This increased connectivity by the resilient RPL is illustrated in Figure 4: in absence of attacks, the average path length of the connected nodes evolves from 1 to 6. However, with $k = 20\%$, the farthest nodes are disconnected from the sink with the classical RPL. In the opposite, with Resilient RPL the average path length is slightly reduced.

Another means to effectively exploit the route diversity created by random behavior is to enforce some degree of replication of the sent packets. Each replica will then follow its own path to reach the sink. Note that the classical RPL cannot take advantage of redundant transmissions to increase their delivery success, as all redundant packets take always the same best route. The average delivery ratio has increased for the randomized RPL with data replication (Figures 1). However, the delivery fairness (Figure 2) and the number of disconnected nodes (Figure 3) remain unchanged. Note that this result differs from a previous study [6] studying resilience in gradient-based routing protocols. This is due to a more reduced average density allowing less diversity in route in our simulations. Moreover, RPL protocol, unlike idealist gradient-based routing protocols studied in [6], are limited in number of parents each node maintains in its memory.

2) Overhead: The efficiency of RPL protocol and its resilient variants are presented in terms of energy consumption. It is important to note that the randomized RPL does not need additional control packets as the underlying classical RPL already maintains a set of parents. Randomized RPL simply exploits this underlying mechanism by introducing route diversity and random behavior to increase uncertainty against attackers.

The total energy consumption decreases for all RPL variants with increasing attack intensity as observed on Figure 6 which is counter-intuitive. This is due to decrease in overall traffic as compromised nodes drop the forwarded packets. Here, the randomized RPL does not show a significant overhead in terms of energy consumption. In addition, the randomized RPL allows fair distribution of the energy consumption of network nodes as the most solicited nodes are relieved through the use of alternative routes.

For the randomized RPL with data replication, the total energy consumption has significantly increased due to increase in the number of retransmissions in the network; data replication brings an additional overhead.

However, when average energy is measured for each received packet (*i.e.* the efficiency in terms of energy consumption), the gain is obvious, in particular when the number of attackers is high. This signifies that resilient RPL with replications is a good trade-off between energy consumption and network reliability.

To summarize, the simulation results show that introducing random mechanism to RPL enhances significantly its resilience in presence of attacks without bringing a significant extra cost in terms of latency and energy consumption. It exploits the alternative paths available to the classical RPL; thus, without need of additional control packets. Data replication has improved significantly the resilience of randomized RPL protocol even though it brings an additional cost, especially in terms of the energy consumption. Therefore, data replication is allowed to exploit the route diversification provided by random behavior for increasing delivery success of each data packet

and to take advantage of the structural redundancy created by wireless communications.

VI. Conclusions

This paper presents a study of the resilience of RPL routing protocol in presence of packet dropping malicious insiders. To enhance RPL resilience by design, we proposed to introduce random behavior and data replication. In particular, a resilient RPL node uses a set of parents to route instead of relying on one single (best or preferred) parent. Simulation results show that such routing mechanisms greatly enhance the RPL resilience without bringing additional overhead in terms of control packets. It allows to exploit the existing neighbor discovery process of the classical RPL to provide route diversity. Uncertainty against adversaries is increased as the route selection becomes unpredictable. Data replication improved the delivery success of each data packet; however, increased the energy consumption of the network. Note that the overhead provided by data duplication is not significant compared to the important amount of control packets of classical RPL.

Future Works. For better resilience-cost tradeoff, instead of replicating at the routing layer, cross-layer mechanisms could be considered to take advantage of the broadcast nature of wireless communications. Anomaly detection schemes should be considered as well to save energy in absence of attacks. We are also planning to investigate the RPL resilience through experimentations on INRIA IoTLab, a very large wireless network testbed developed in France [7]. In addition, it seems to us that more attack scenarios should be considered such as byzantine or Sybil attacks.

VII. Acknowledgments

This work was made possible by NPRP grant #NPRP4-553-2-210 from the Qatar National Research Fund (a member of The Qatar Foundation). The statements made herein are solely the responsibility of the authors.

References

[1] Internet engineer task force. http://www.ietf.org.

[2] N. Accettura, L. Grieco, G. Boggia, and P. Camarda. Performance analysis of the rpl routing protocol. In *Mechatronics (ICM), 2011 IEEE International Conference on*, pages 767 –772, april 2011.

[3] A. Brandt, J. Hui, R. Kelsey, P. Levis, K. Pister, R. Struik, J. Vasseur, and R. Alexander. Rpl: Ipv6 routing protocol for low-power and lossy networks, March 2012.

[4] D. S. J. De Couto, D. Aguayo, J. Bicket, and R. Morris. A high-throughput path metric for multi-hop wireless routing. *Wirel. Netw.*, 11(4):419–434, July 2005.

[5] R. J. Ellison, R. C. Linger, T. Longstaff, and N. R. Mead. Survivable network system analysis: A case study. *IEEE Software*, 16(4):70–77, July 1999.

[6] O. Erdene-Ochir, M. Minier, F. Valois, and A. Kountouris. Toward resilient routing in wireless sensor networks: Gradient-based routing in focus. In *Sensor Technologies and Applications (SENSORCOMM), 2010 Fourth International Conference on*, pages 478–483, July 2010.

[7] O. Fambon, E. Fleury, G. Harter, R. Pissard-Gibollet, and F. Saint-Marcel. Fit iot-lab tutorial: hands-on practice with a very large scale testbed tool for the internet of things. In *10mes journes francophones Mobilit et Ubiquit (UbiMob)*, 2014.

[8] T. R. Farley and C. J. Colbourn. Multiterminal resilience for series-parallel networks. *Networks*, 50(2):164–172, September 2007.

[9] O. Gaddour and A. Koubia. Survey rpl in a nutshell: A survey. *Comput. Netw.*, 56(14):3163–3178, Sept. 2012.

[10] K. Heurtefeux, H. Menouar, and N. AbuAli. Experimental evaluation of a routing protocol for wsns: Rpl robustness under study. In *IEEE WiMob*, pages 491–498, Oct 2013.

[11] C. Karlof and D. Wagner. Secure routing in wireless sensor networks: attacks and countermeasures. *Ad Hoc Networks*, 1(2-3):293–315, August 2003.

[12] M. Liu and D. Hutchson. Toward resilient netwoks using situation awareness. In *The 12th annual PostGraduate Symposium on the Convergence of Telecommunications, Networking and Broadcasting (PGNet)*, Liverpool, UK, June 2011.

[13] O.Erdene-Ochir, M.Minier, F. Valois, and A. Kountouris. A new metric to quantify resiliency in networking. In *In IEEE Communication Letters*, October 2012.

[14] D. Shila and T. Anjali. Defending selective forwarding attacks in wmns. In *Electro/Information Technology, 2008. EIT 2008. IEEE International Conference on*, pages 96–101, May 2008.

[15] J. P. Sterbenz, D. Hutchison, E. K. Cetinkaya, A. Jabbar, J. P. Rohrer, M. Scholler, and P.Smith. Resilience and survivability in communication networks: Strategies, principles, and survey of disciplines. *Computer Networks*, (54):1245–1265, March 2010.

[16] J. P. G. Sterbenz, R. Krishnan, R. R. Hain, A. W. Jackson, D. Levin, R. Ramanathan, and J. Zao. Survivable mobile wireless networks: issues, challenges, and research directions. In *Proceedings of the 1st ACM workshop on Wireless security*, WiSE '02, pages 31–40, New York, NY, USA, 2002. ACM.

[17] J. Tripathi, J. de Oliveira, and J. Vasseur. A performance evaluation study of rpl: Routing protocol for low power and lossy networks. In *Information Sciences and Systems (CISS), 2010 44th Annual Conference on*, pages 1 –6, march 2010.

[18] T. Watteyne, K. Pister, D. Barthel, M. Dohler, and I. Auge-Blum. Implementation of gradient routing in wireless sensor networks. In *Global Telecommunications Conference, 2009. GLOBECOM 2009. IEEE*, pages 1–6, 2009.

[19] Y. Zhang and M. Minier. Selective forwarding attacks against data and ack flows in network coding and countermeasures. *Journal of Computer Networks and Communications*, 2012, September 2012.