A Trust-based Defence Scheme for Mitigating Blackhole and Selective Forwarding Attacks in the RPL Routing Protocol

David Airehrour
Nelson Marlborough Institute of Technology, Auckland, New Zealand

Jairo Gutierrez
Auckland University of Technology, Auckland, New Zealand

Sayan Kumar Ray
Manukau Institute of Technology, Auckland, New Zealand

Abstract: The routing protocol for low-power and lossy networks (RPL) has gained prominence as the standard IoT routing protocol. However, it faces like many other routing protocols diverse attacks. Many studies have been proposed to secure the RPL protocol, and simulation studies have been put forward as the main research method, while testbed experiments, though an authentic research and testing method, have been ignored. Although testbed experiments and simulation studies have their strengths and limitations, testbed techniques could be used as a verifiable validation method for simulation studies. This study is a follow up research work to validate our simulation study, which addressed Blackhole attacks in the RPL routing protocol. In addition, Selective Forwarding attacks are also addressed. It implements a testbed while embedding our Trust-based RPL protocol and the standard RPL protocol in a smart environment configuration. Based on the test experiments, we provide a proof-of-concept of the validity of our claim that our Trust-based RPL protocol provides a comprehensive defence (simulation and testbed) against Blackhole and Selective Forwarding attacks.

Keywords: Trust, RPL, Blackhole attack, Selective Forwarding attack, AS-XM1000

Copyright © 2018
http://doi.org/10.18080/ajtde.v6n1.138

Introduction

The Internet of Things (IoT) — the connectivity, communication and management of vast numbers of networked devices (machines and sensors) by means of the Internet — is a pervasive phenomenon that is creating a global technological disruption. From the production plant to the intensive care unit of a hospital to a smart home, IoT is rapidly making its presence felt. As the proliferation of these devices permeate our society, the progressive reliance on these intelligent, interconnected devices in our everyday life increases. This fact, coupled with the rising challenge of cyber threats and security attacks raises the question: how do we ensure that this massive number of online devices are protected from interference and malicious attacks that could compromise their security and hence create public safety concerns, which, in turn, could hinder the potential growth and benefits of this new technology wave?

Undoubtedly, for the safe and reliable operation of connected IoT devices the issue of security of these devices is paramount. However, identifying the ideal systemic security approach to adopt in order to have a secure and robust IoT ecosystem is not an easy task. Although enterprise networks, firewalls and protocol systems can manage a high level of Internet traffic, a study (Pongle, 2015b) shows, however, that the protection of resource-constrained and deeply embedded terminal sensor devices having specific functionalities is a challenge.

RPL (Routing Protocol for Low power and lossy networks) is considered the standard IoT routing protocol (Gaddour, 2015). An important characteristic of RPL is its design for a network of resource-constrained devices with lossy links and high Packet Error Rate (PER). The growing acceptance of RPL is due to its adaptability to diverse network topologies and its Quality of Service (QoS) features, amongst others. However, secure operation mode is not enabled in RPL, and this makes RPL vulnerable to various routing attacks. This has been reported in Djedjig, Tandjaoui, & Medjek (2015); Gaddour *et al.* (2015); Glissa, Rachedi, & Meddeb (2016) and in our work (Airehrour, Gutierrez, & Ray, 2016b).

In our work (Airehrour, 2016b), we proposed a Trust-based secure RPL routing protocol against Blackhole attacks. Subsequently, we improved this work to address Selective Forwarding attacks (Airehrour, Gutierrez, & Ray, 2017). In both studies, simulation results proved our secure Trust-based system for RPL protocol to be a promising solution to protect RPL from routing attacks. To take this further, this study, proposes a testbed experiment to investigate the authenticity of our simulation claims with respect to the work presented in Airehrour (2016b). In our testbed, we have embedded our Trust-based system in RPL protocol, deployed it and tested our secure protocol against the standard RPL implementation.

The remainder of the paper is organized as follows. The Related Work section discusses RPL protocol operations, related studies, and the need for testbed experiments to validate

Copyright © 2018
http://doi.org/10.18080/ajtde.v6n1.138

simulation studies in secure RPL protocols. In the Trust and Reputation Based RPL Objective Function section, our previous study (Airehrour, 2016b) on Trust-based RPL protocol and the validation process is discussed. The testbed setup and demonstration is shown in the Testbed Experiments section, which shows the efficacy of our proposed Trust-based system and its consistency with the simulations performed in Airehrour (2016b). We conclude with some thoughts in the Conclusion and Future Work section.

Related Work

Routing in RPL

RPL forms a tree-like topology with a root node at the top (commonly referred to as the sink node) and leaves at the edges (known as sender nodes). RPL, however, is not restricted to a tree topology because it can cope with redundant links that are required in Low-power and Lossy Networks (LLNs) (Winter, 2012). In RPL, the movement of traffic is described in terms of the "up" and "down" directions. Traffic moving from the sender nodes to the sink node is referred to as the “upward” traffic, while traffic moving from the sink node to the sender nodes is regarded as the “downward” traffic. During a RPL operation, links are required to be bidirectional to create both upward and downward routes to and from any node. For a node to be considered a parent, its reachability must be ascertained using an external mechanism that is being activated during the parent-node selection process. This is to ensure the link properties and neighbour reachability are defined.

RPL is considered a distance vector protocol, which performs routing either in a downward or upward fashion. All information regarding the topology of RPL is maintained as a graph called the Destination Oriented Directed Acyclic Graph (DODAG). The DODAG consists of paths from the sender nodes to the sink node. During routing, every node maintains its Rank relative to its position in the DODAG tree. A node’s Rank is a calculated 16-bit monotonic scalar value that is used for loop avoidance, and this value is calculated according to the specified Objective Function (OF).

Every DODAG is populated with parent information. The parent data is control and route information, which is used for routing and RPL network stability. The packets used by DODAG are: DODAG Information Object (DIO), Destination Advertisement Object (DAO), and DODAG Information Solicitation (DIS) for transmitting the DODAG information. A DODAG formation is administered using the following guidelines: Path metrics, OF, Rank of a node for loop avoidance in the DODAG tree, and any stipulated policies of a node (Winter, 2012). Figure 1 shows an illustration of the route-build process in RPL. From time to time, a node periodically re-evaluates the Rank of its parent to maintain a loop-free route topology.

Copyright © 2018
http://doi.org/10.18080/ajtde.v6n1.138

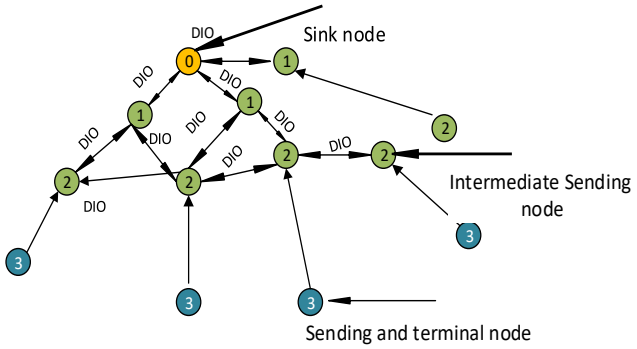

Figure 1. A RPL instance displaying DIO broadcast.

Routing Metrics and Objective Function in RPL

According to the IETF specification (Winter, 2012), different OFs could be specified for RPL. Traffic in a RPL network is transported and delivered based on the defined OF, which could be different for various traffic types. OFs are defined to optimize some particular metrics while also fulfilling specific constraint(s). Accordingly, the OF is used for effective routing path definition based on specific requirements. These requirements could be embedded in a series of programming logic in IoT motes and utilized by RPL for routing purposes. A fundamental reason for the adoption of RPL for LLNs is the separation of the OF from the central protocol specification (Winter, 2012), thus making it easy for different OF specifications to be built into RPL and which, in turn, makes it useful for a wide range of application scenarios.

Routing metrics are scalar values for determining the 'cost' of a route path. The values are used for making optimal routing decisions, especially when multiple routes are identified. A formal specification of how routes are defined, selected and optimized is regarded as the objective function (OF) of the RPL routing protocol. The network of resource-constrained sensor devices uses metrics defined in the OF to make optimal routing decisions. The use of a scalar value for route determination makes it particularly attractive for embedding trust as a metric for route computation, and the isolation of malicious nodes. Routing metrics are important to the successful creation and preservation of any network topology. Traditional networks employ the use of static metrics (hop count, bandwidth) for routing decisions. The IETF RFC 6550 specification of RPL (Winter, 2012) does not define specific forwarding metric policies. Furthermore, in the RPL draft from the IETF, constraints are also specified, which are used as filters for the specification of what should be included or excluded in the routing metric dynamics of RPL. Various literatures have discussed the RPL routing protocol and have proposed different metrics for LLNs, which have been presented in Djedjig *et al.* (2015), Gaddour *et al.* (2015) and Glissa *et al.* (2016).

Copyright © 2018
http://doi.org/10.18080/ajtde.v6n1.138

Security Vulnerabilities in RPL

Studies have been undertaken that bring to the fore the vulnerabilities in the RPL routing protocol. The authors in Pongle & Chavan (2015b) conducted a study on possible attacks that could be perpetrated against RPL. Similar studies have been conducted and are reported in Airehrour, Gutierrez & Ray (2016a) and Nawir, Amir, Yaakob & Lynn (2016), while the impact of attacks on the RPL protocol has been reported in Kumar, Matam & Shukla (2016). In RPL protocol, a Blackhole attacking node advertises itself by broadcasting a false and low DIO rank value to the sink node. This causes nodes within its reach to select it as their parent for a downward route transmission from the sink node. The Blackhole node immediately commences the discard of packets upon receipt from its neighbour nodes. Table 1 provides a summary of recent literature addressing RPL protocol attacks. The table provides the attacks addressed, attack detection strategy, and the method of validation. In nearly all the cases provided, simulation was used as the method of verification. This brings to bear, therefore, the need for a realistic live study, such as testbed experiments, that will validate the claims presented in the literature addressing the RPL protocol attacks.

In addition, a Selective Forwarding attacking node selectively or randomly forwards packets it has received. The aim of this type of attack is two-fold. The first is the desire to degrade network performance by increasing the packet loss rate. The second is to act as a 'man in the middle' in order to inhibit other nodes that are seeking to communicate through it (the attacker) with the sink node. This scenario creates a denial of service (DoS).

Table 1. A summary of RPL protocol research improvements and validation methods

Reference	Attack(s) Isolated	Attack Detection Strategy	Validation Method
Real Time Intrusion and Wormhole Attack Detection in Internet of Things (Pongle & Chavan, 2015a)	Wormhole attacks	Anomaly-based detection system	Simulation
A Specification-Based IDS for Detecting Attacks on RPL-Based Network Topology (Le, Loo, Chai, & Aiash, 2016)	RPL topology attacks	Specification based detection system	Simulation
Ultra-Lightweight Deep Packet Anomaly Detection for Internet of Things Devices (Summerville, Zach, & Chen, 2015)	General purpose IDS system	n-gram bit-pattern matching	Empirical
Enhancing RPL for Robust and Efficient Routing in Challenging Environments (Kantert *et al.*, 2015)	Sinkhole	Trust-based method	Simulation
A Distributed Monitoring Strategy for Detecting Version Number Attacks in RPL-Based Networks (Mayzaud, Badonnel, & Chrisment, 2017)	Version Number attacks	Distributed Monitoring Strategy	Simulation
A secure routing protocol based on RPL for Internet of Things (Glissa *et al.*, 2016)	Rank attacks	Hash chain authentication	Simulation

Copyright © 2018
http://doi.org/10.18080/ajtde.v6n1.138

Reference	Attack(s) Isolated	Attack Detection Strategy	Validation Method
Trust-based RPL for the Internet of Things (Djedjig *et al.*, 2015)	Rank attacks	Trust-based	Simulation
Strong Authentication Countermeasures Using Dynamic Keying for Sinkhole and Distance Spoofing Attacks in Smart Grid Networks (Taylor & Johnson, 2015)	Sinkhole and Distance Spoofing Attacks	Dynamic key Authentication	Simulation
Enhancing RPL Resilience Against Routing Layer Insider Attacks (Heurtefeux, Erdene-Ochir, Mohsin, & Menouar, 2015)	Selective Forwarding attacks	Duplication of packets for redundancy	Simulation
Addressing DODAG Inconsistency Attacks in RPL Networks (Sehgal, Mayzaud, Badonnel, Chrisment, & Schönwälder, 2014)	DODAG Inconsistencies		Simulation
Denial-of-service detection in 6LoWPAN based Internet of Things (Kasinathan, Pastrone, Spirito, & Vinkovits, 2013)	DoS attacks	Signature-based detection	Empirical

Validating Simulation via Testbed

Simulation has over the years proved to be a fundamental testing and diagnostic tool. This is especially true for network simulations, and this has become a global standard for wireless sensor network testing and evaluation. However, as sophisticated as a simulation may be, it is often inadequate as an investigation platform for real-world deployments (Fortier, 2002; Tan, 2010). Sensors, and indeed IoT sensors, have continued to improve in technological advancements; their form factors have become, and are continuing to be, smaller by the day while their processing capabilities have soared in recent times. In addition, some of the measuring devices on these sensors have not been adequately and accurately simulated (Fortier, 2002).

A testbed, on the other hand, is a collection of deployed hardware infrastructure, developed for physical network experimentation and integrated with software services, for controlling and managing hardware and experiments executed on it. Therefore, a physical testbed becomes imperative, as it is designed to support physical experimentation, which addresses the gaps that simulations are not able to fill. A fundamental feature of a testbed is its focus on a specific aspect of the total system. This helps in furthering a deeper understanding of the functional and operational requirements of the system while capturing specific behaviours under unique conditions, which otherwise would not have been captured during a simulation. Results gathered during testbed runs can be quantitatively measured and analysed, on which design decisions can be predicated from the theoretical and empirical findings.

Copyright © 2018
http://doi.org/10.18080/ajtde.v6n1.138

Trust and Reputation Based on RPL Objective Function

RPL uses routing metrics defined in its Objective Function to create the DODAG. Essentially, the routing metrics help in the creation of the network routes and hence result in optimal routes. The Contiki platform (Thingsquare, 2016) uses Minimum Rank with Hysteresis Objective Function (MRHOF) by default, which minimizes the expected transmission count (ETX) values.

This study compares the MRHOF implementation of RPL and our Trust-based implementation of RPL. Our previous work (Airehrour, 2016b) was compared with a MRHOF implementation of RPL and, based on that, testbed experiments were similarly conducted.

In our previous work (Airehrour, 2016b), a Trust-based system was proposed for RPL protocol, which provides security against Blackhole attacks. The Trust-based protocol provides a feedback-aware trust system for a RPL network. In this system, a node evaluates the trust value of its neighbour-node with respect to the good forwarding behaviour of the node. This study was further improved for the detection and isolation of Selective Forwarding attacks, and this was reported in Airehrour *et al.* (2017). We recap some fundamental trust computations in our previous study below.

Computing and Embedding Trust in RPL

Algorithm for the detection of Blackhole

Let N1 ← one unfilled node in the NeighborNodeList [ ]
Let N2 ← another node next to N1 in the NeighborNodeList [ ]

Compute $EP_{ij} = \frac{N_{dlv}}{N_{sent}}$

```
    If (N1.ETX<= ETX_Limit)  & (N2.ETX<=ETX_Limit)
    If (N1.Rank <= Rank_Self)  & (N2.RANK <= RANK_Self)
       Preferred_Parent = N1.EP > N2.EP ? N1 : N2;
    Else
        If (N1.Rank <= Self_Rank)  || (N2.Rank <= Self_Rank)
            Preferred_Parent = N1.Rank < N2.Rank ? N1: N2
        Else
            Preferred_Parent = NULL;
  Else
      If (N1.ETX <= ETX_Limit)  || (N2.ETX <= ETX_Limit)
        Preferred_Parent = N1.ETX <= N2.ETX ? N1 : N2;
      Else
         Preferred_Parent = NULL;
  Return Preferred_Parent
End program.
```

Figure 2. Trust algorithm for trusted parent selection and isolation of Blackhole and Selective Forwarding nodes (Airehrour et al., 2016b).

Copyright © 2018
http://doi.org/10.18080/ajtde.v6n1.138

The trusted node(s) are selected for routing decisions while maintaining the rank order of all nodes in the RPL network. Trust is computed based on Equation 1. while Figure 2 presents the algorithm for trusted parent selection and isolation of blackhole nodes.

$$EP_{ij} = \frac{N_{dlv}}{N_{sent}} \quad (1)$$

In Equation 1, N_{dlv} is the number of node i's packets delivered through node j, and N_{sent} is the total number of packets sent by node i to node j.

Blackhole and Selective Forwarding Detection and Isolation

This section describes the detection and isolation of Blackhole and Selective-Forwarding nodes. After the computation of the trust values of nodes, the nodes are ranked in the magnitude of their trust values while maintaining the rank order of nodes, as specified in RFC 6550 (Winter, 2012). The nodes with high trust values are used for secure routing decisions. To achieve the objective above, we assumed that the network operates in promiscuous mode and hence we modified the RPL protocol to achieve the functions stated below:

- Every child node keeps a record of the number of packets forwarded to its parent.
- A child-node assesses the number of packets forwarded by a parent-node on its behalf. This is much like the DAO and DAO-ACK in RPL.
- A node queues up its packets in its buffer for delivery. In coding the Blackhole behaviour, an attacking Blackhole node always keeps its buffer empty, since it discards packets sent to it and does not report packets forwarded to its child node, whereas a normal node reports its details to its child node.

Testbed Experiments

The testbed experiment undertaken in this study serves as a proxy for a smart home environment, which is vulnerable to attacks. In the testbed setup, fourteen AS-XM1000 motes (refer to Figure 3) based on the Telos-B system were deployed in a research laboratory (fourth floor, School of Engineering, Computer and Mathematical Sciences) at the Auckland University of Technology's City campus. The coverage area was approximately 30 metres by 30 metres. The InstantContiki 3.0 platform (Thingsquare, 2016) was used to carry out the experiment. Three mote types were deployed: one UDP sink mote; twelve UDP sender motes; and two Blackhole attacking motes. Although the sender and attacking motes deployed were stationary, they could still communicate with the UDP sink, since all of them were under the coverage area of the UDP sink mote. The sink mote was connected to a desktop PC running

Copyright © 2018
http://doi.org/10.18080/ajtde.v6n1.138

the Contiki/Cooja emulation program, while the sender and Blackhole motes were evenly distributed across the testbed location.

Figure 3. AS-XM1000 mote

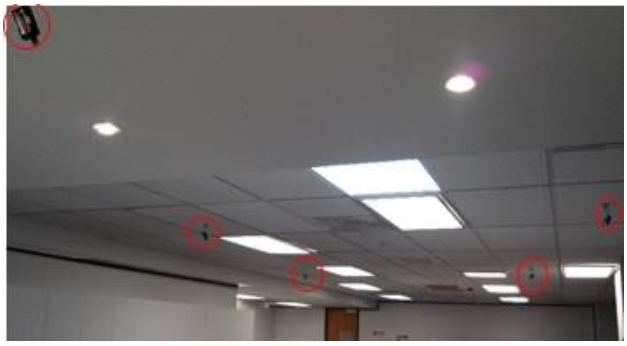

Figure 4. Physical deployment of 14 XM1000 motes in the research lab

Table 2 lists the deployment settings and configurations. To complete the testbed setup, the respective UDP_sink, UDP_sender and malicious codes were embedded into the XM1000 motes using ContikiRPL (MRHOF) and Trust-based RPL. Figure 4 shows a physical partial view of the motes deployment in the research laboratory. The motes are circled in red. In the accompanying sections, the testbed performance results between MRHOF-RPL and the proposed Trust-based RPL under Blackhole attacks are discussed. In the figures 5 and 6 the motes are depicted as y.y. Hence, mote 1 is shown as 1.1; mote 2 as 2.2. In addition, the child-parent relationship is indicated with a blue arrow along with the expected transmission count (ETX) value between them.

Table 2. Testbed Parameters

Testbed tool	Contiki/Cooja 3.0
Testbed coverage area	30m x 30m
Total number of XM1000 motes	14
Blackhole motes	2 (Motes 13 and 14)
Mote deployment environment	Smart building
RX Ratio	30-100%
TX Ratio	100%
TX Range	50m
Interference Range	55m
Routing Protocols	MRHOF-RPL and Trust-based RPL
Network protocol	IP based

Copyright © 2018
http://doi.org/10.18080/ajtde.v6n1.138

Isolation of Blackhole Attacks

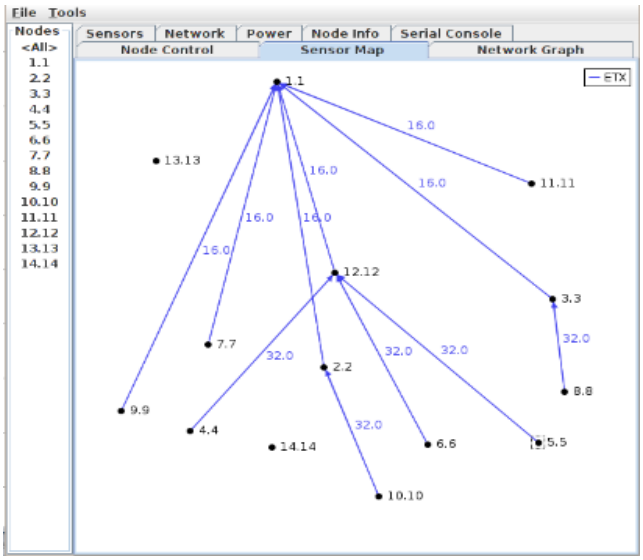

Figure 5. Blackhole mote isolation using Trust-based RPL protocol

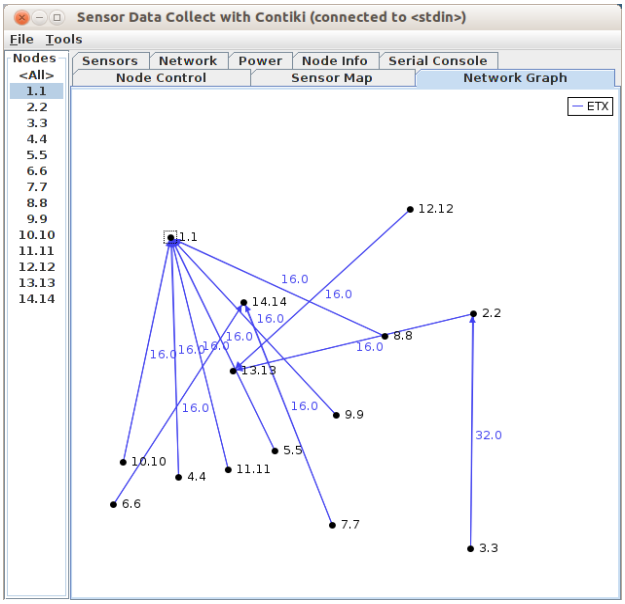

Figure 6 MRHOF-RPL route topology segmentation under Blackhole attacks during the testbed experiment with XM1000 motes

Figures 5 and 6 show snapshot captures of the testbed network topology formation of XM1000 motes under the Trust-based RPL and MRHOF-RPL protocols during Blackhole attacks. The Trust-based RPL could detect and isolate motes 13 and 14 from its route topology formation due to their malicious behaviour in the network. As observed from Figure 5, motes 13 and 14 were not considered for routing decisions in the network. However, the MRHOF-RPL protocol standard (Figure 6) could not mitigate the effect of the Blackhole activities of motes 13 and 14, respectively. Consequently, three disjointed network segments were formed, which resulted in unsuspecting motes 2, 3 and 12 selecting mote 13 as their parent, and motes 6 and 7 selecting mote 14 as their parent. The remaining motes were connected to the sink mote. Furthermore,

Copyright © 2018
http://doi.org/10.18080/ajtde.v6n1.138

as evident in Figure 7, the Trust-based RPL could detect and isolate Blackhole attacks during routing operations. The first five minutes of RPL operation witnessed the detection of a slightly higher level of initial Blackhole attacks among the malicious motes. Our Trust-based RPL could identify and isolate the Blackhole attack motes and thus the malicious motes were not considered for routing decisions in the network. The testbed result discussed above agrees with the simulation study presented in our paper (Airehrour, 2016b). In both cases, the testbed and simulation studies had similar detection pattern and detection rate of Blackhole attacks during RPL operation.

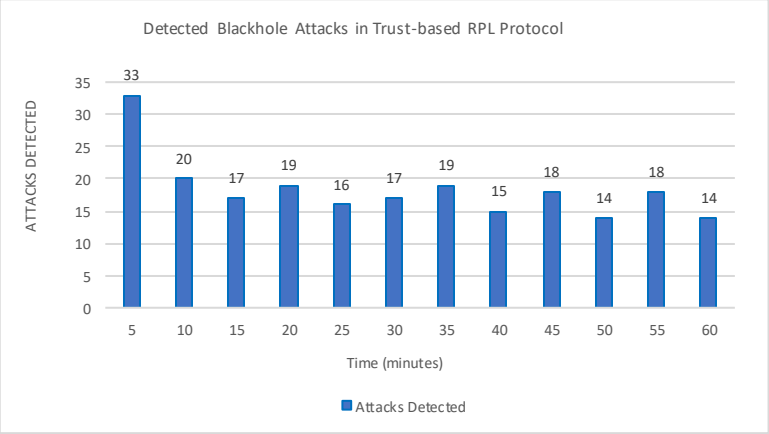

Figure 7. Blackhole attacks detection and isolation during the testbed experiment

Moreover, as MRHOF-RPL protocol was unable to detect any of the Blackhole attacks in the network, the protocol experienced a high frequency of mote Rank changes as a result of an incessant re-alignment of a child mote with new parent mote (see Figure 8). This destabilized the network topology and hence made the network inefficient. In addition, as evident from the results presented in Figure 8, the Trust-based RPL protocol maintained the number of its mote Rank changes within 15 – 55, while MRHOF-RPL had a range between 16 – 246 mote Rank changes. Also, it can be observed that MRHOF-RPL had a significant number of mote Rank changes compared to the Trust-based RPL protocol. This indicates that the activities of the Blackhole attack motes during RPL's operation had a significant impact on MRHOF-RPL protocol during the testbed experiments.

Copyright © 2018
http://doi.org/10.18080/ajtde.v6n1.138

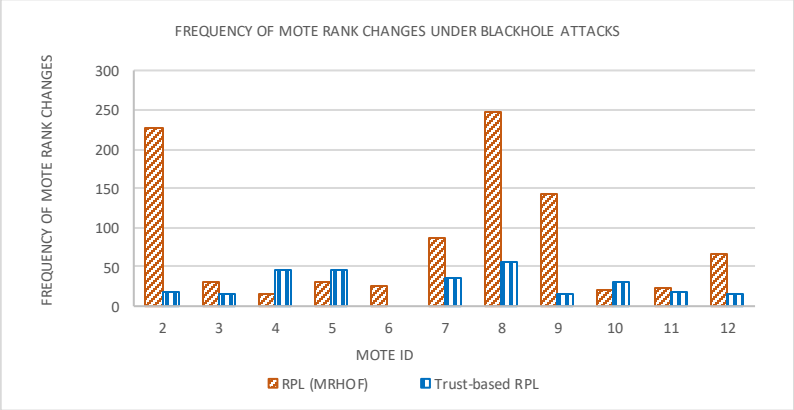

Figure 8. Comparison of frequency of mote Rank changes under Blackhole attacks during the testbed experiment

Network Performance Evaluation

In this section, we present the testbed analysis of the network throughput and the packet loss rates of MRHOF-RPL and our Trust-based RPL protocols while under Blackhole attacks. The network throughput (kilobits per second), which is the amount of data transmitted in each period over a given communications channel, is presented. A higher throughput shows a more stable network topology despite the presence of Blackhole attackers. As shown from the throughput comparison presented in Figure 9, the Trust-based RPL protocol maintained a significantly higher throughput measurement over and above MRHOF-RPL. Motes 7 and 8 achieved the highest and lowest throughputs of 3 kbps and 0.34 kbps under MRHOF RPL. Under the Trust-based RPL, motes 5 and 4 achieved the highest and lowest throughputs of 6.6 kbps and 2 kbps, respectively. This clearly implies that our Trust-based RPL protocol delivers better network performance than the MRHOF-RPL under Blackhole attacks. The testbed network throughput measurements reported here are similar to the simulation results reported by our simulation study in Airehrour *et al.* (2016b).

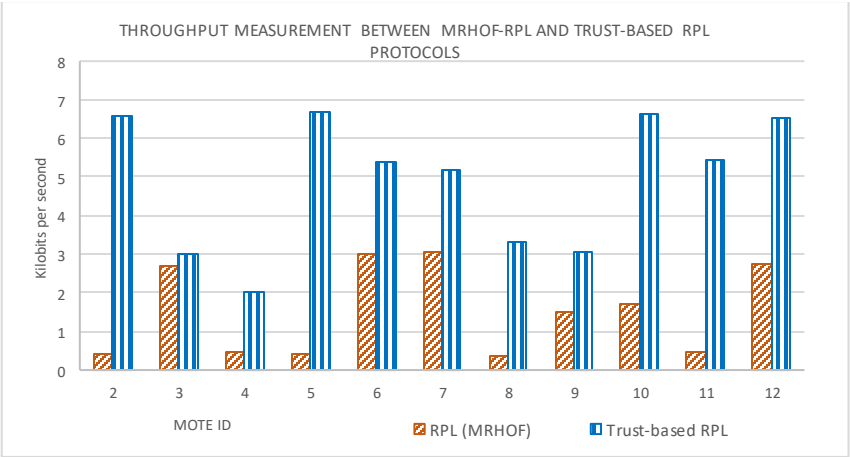

Figure 9. A throughput performance measurement between MRHOF-RPL and Trust-based RPL protocols

Copyright © 2018
http://doi.org/10.18080/ajtde.v6n1.138

Figure 10 compares the packet-loss percentage between the Trust-based RPL and MRHOF-RPL. Packet percentage loss is the ratio of the total packets lost to the total packets sent between a sender and a sink mote. A lower loss rate is indicative of better packet delivery and hence a more stable link between network nodes. From Figure 10, the Trust-based RPL protocol maintained a packet loss rate of less than 28%, but MRHOF-RPL had 60 to 75% packet loss rates. The testbed packet-loss-rate results presented in Figure 10 agree with the simulation study results reported in Airehrour *et al.* (2016b).

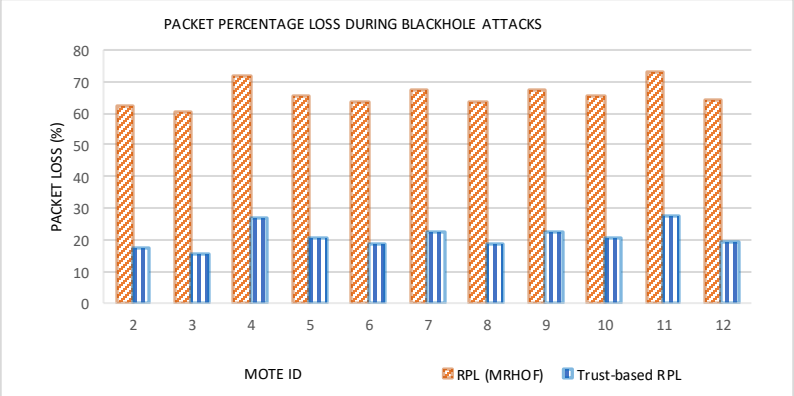

Figure 10. Percentage of packet loss comparison between Trust-based RPL and MRHOF-RPL under Blackhole attacks during the testbed experiment

Isolation of Selective Attacks

The testbed experiment was extended to test the performance of the Trust-based RPL protocol and MRHOF-RPL under Selective Forwarding attacks using the deployed XM1000 motes. When the test was conducted, an instance of the network topology was captured in the sensor data collection menu of Contiki/Cooja, and the topology instance is displayed in Figure 11. It reveals that the Trust-based RPL protocol could detect and isolate malicious motes 13 and 14 from its route topology formation. However, in Figure 12, which is the network topology formation of MRHOF-RPL, it could not mitigate the effect of malicious activities of the Selective Forwarding attacking motes (13 and 14) in the network. Motes 3, 6 and 8 were drawn to malicious mote 13 while motes 2, 7 and 12 were drawn to malicious mote 14. The rest of the motes, however, were connected to the sink mote. Figure 12 illustrates the situation whereby packets sent to mote 1 by motes 2, 7 and 12 cannot be delivered during the period they were connected to mote 13. Also, packets sent by motes 2, 7 and 12 cannot be received by mote 1 during the time they were connected to malicious mote 14, since the network is segmented and cannot connect to the central sink mote.

Copyright © 2018
http://doi.org/10.18080/ajtde.v6n1.138

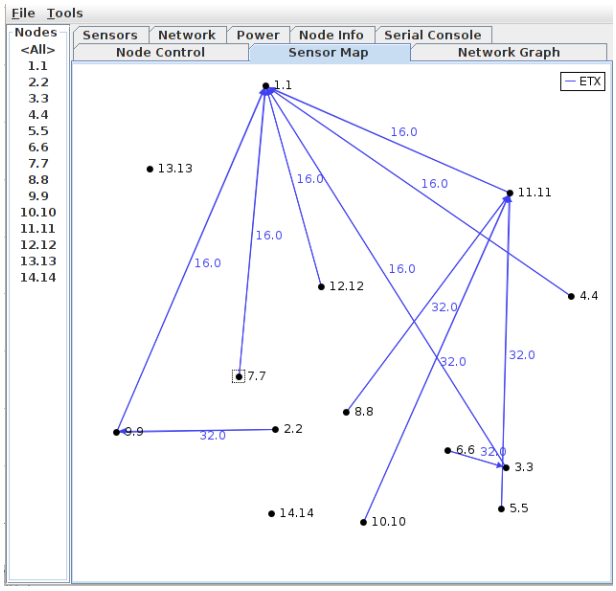

Figure 11. Isolation of Selective Forwarding attacks using the Trust-based RPL protocol

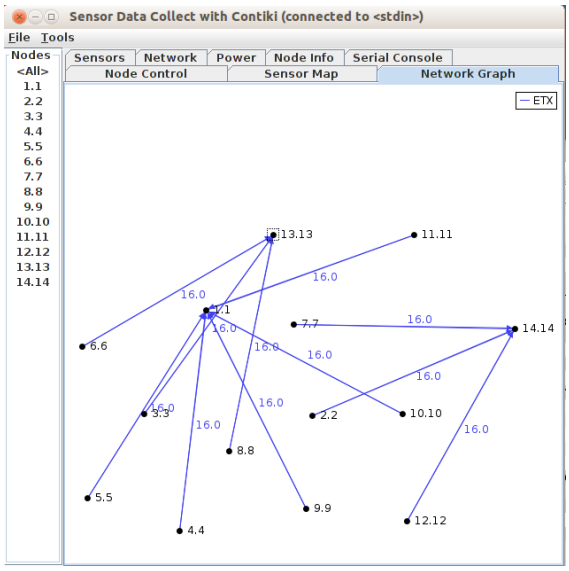

Figure 12. Route topology segmentation by Selective Forwarding attacking nodes under MRHOF-RPL

Detection and Isolation of Attack Nodes

The testbed experiment in Figure 13 shows the detection of attacks perpetrated by malicious motes 13 and 14 performing Selective Forwarding attacks. The first five minutes shows the detection of a high amount of attacks, while the remaining simulation period (10 – 60 minutes) shows a relatively stable number of attacks detected (50 – 75). The initial high flow of attacks and detection in the first five minutes is attributed to RPL's proactive routing nature, which floods the network with DIOs. Due to this, the Selective Forwarding attacking motes (13 and 14) rapidly, but selectively, intercept and forward packets as per their malicious behaviour. Conversely, MRHOF-RPL protocol has no mechanism for detecting Selective Forwarding attacks perpetrated by malicious motes 13 and 14 during the experimentation period.

Copyright © 2018
http://doi.org/10.18080/ajtde.v6n1.138

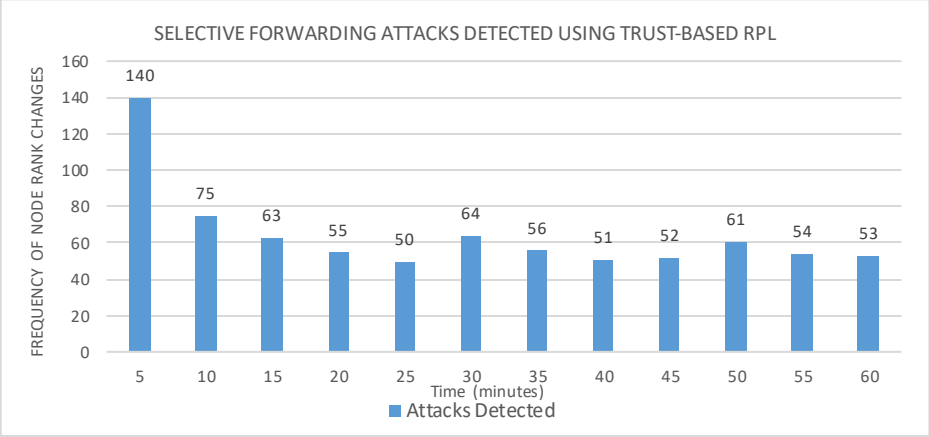

Figure 13. Selective Forwarding attacks detection and isolation during the testbed experiment

Figure 14 shows the frequency of mote Rank changes between MRHOF-RPL and the Trust-based RPL protocol under Selective Forwarding attacks during the testbed operation. MRHOF-RPL had a significant number of mote Rank frequency changes. The frequency of Rank changes for MRHOF-RPL ranged from 122 – 661, while Trust-based RPL had a range of 17 – 200. The MRHOF-RPL protocol under Selective Forwarding attacks reveals high malicious mote activity. Conversely, Trust-based RPL had much lower mote Rank changes, which could be considered moderate and consistent with RPL operations. This implies that the Trust-based RPL had better network performance and stability.

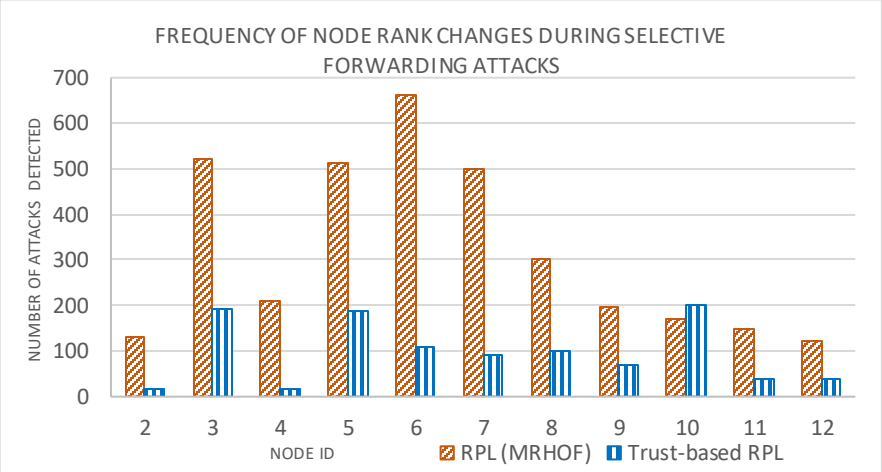

Figure 14. Comparison of frequency of node Rank changes under Selective Forwarding attacks during the testbed experiment

Network Performance Measures

In the throughput comparison between MRHOF-RPL and the Trust-based RPL shown in Figure 15, the Trust-based RPL protocol displayed a better throughput performance over MRHOF-RPL. MRHOF-RPL consistently lagged behind the Trust-based RPL in throughput performance during the testbed trials. Trust-based RPL maintained 4 – 6.5 kbps throughput range, while MRHOF-RPL had a range of 1 – 4 kbps.

Copyright © 2018
http://doi.org/10.18080/ajtde.v6n1.138

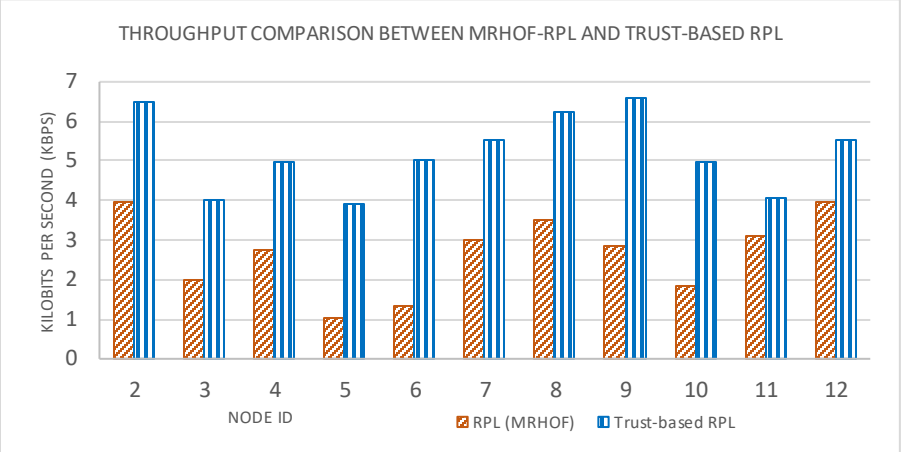

Figure 15. Network throughput performance comparison between Trust-based RPL and MRHOF-RPL during the testbed experiment

Figure 16 shows the packet loss rates between MRHOF-RPL and Trust-based RPL. The Trust-based RPL maintained packet loss rates between 15% – 27.7%; MRHOF-RPL on the other hand, had packet loss rates of 60% – 72.7%. It can be summarised, therefore, from Figure 16, that the Selective Forwarding attacks of malicious motes 13 and 14 had a more significant impact against the MRHOF-RPL network than is the case for the network using the Trust-based RPL protocol. This further shows Trust-based RPL as having better network performance over MRHOF-RPL under the Selective Forwarding attacks.

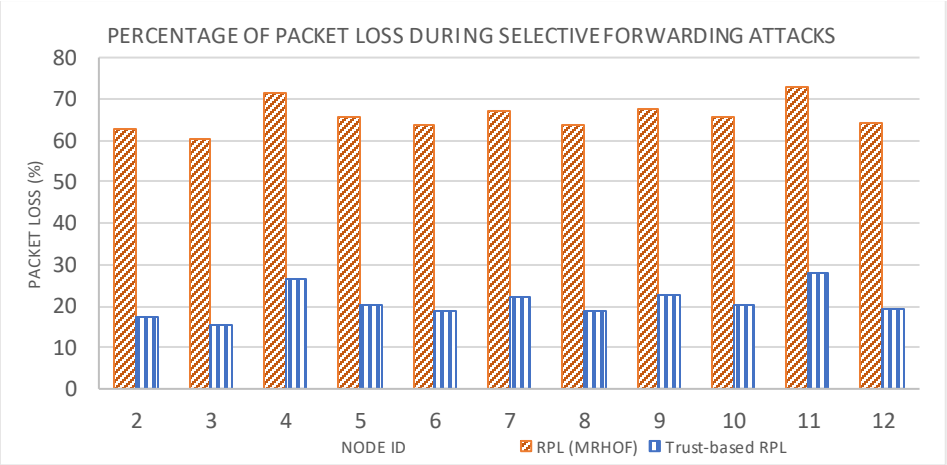

Figure 16. Percentage of packet loss comparison between Trust-based RPL and MRHOF-RPL under Selective Forwarding attacks during the testbed experiment

Conclusions and Future Work

Compromised sensor nodes can destabilize the integrity of data routing in IoT networks by intentionally dropping or sending incorrect control and route information. This study evaluated through testbed experiments the performance of our Trust-based RPL protocol against the standard RPL (MRHOF) protocol under Blackhole and Selective Forwarding attacks. The testbed data gathered were analysed to determine the efficacy of our Trust-based

Copyright © 2018
http://doi.org/10.18080/ajtde.v6n1.138

RPL protocol in mitigating Blackhole and Selective Forwarding attacks in comparison with the IETF standard presented in ContikiRPL. The results gathered through the testbed experiments are in agreement with our simulation study results in Airehrour et al. (2016b) and thus confirm the validity of our Trust-based RPL protocol in terms of providing better security against Blackhole and Selective Forwarding attacks in IoT networks. As part of our future work, we are conducting similar testbed experiments to examine ways of extending our trust-based protocol to address Rank and Sybil attacks, amongst others.

References

Airehrour, D; Gutierrez, J; Ray, SK. 2016a. 'Secure routing for internet of things'. *Journal of Network and Computer Applications*, vol. 66(C), pp. 198-213. doi:10.1016/j.jnca.2016.03.006

Airehrour, D; Gutierrez, J; Ray, SK. 2016b. 'Securing RPL routing protocol from blackhole attacks using a trust-based mechanism'. 2016 26th International Telecommunication Networks and Applications Conference (ITNAC), 7-9 Dec 2016.

Airehrour, D; Gutierrez, J; Ray, SK. 2017. 'A Trust-Aware RPL Routing Protocol to Detect Blackhole and Selective Forwarding Attacks'. *Australian Journal of Telecommunications and the Digital Economy*, vol. 5, no. 1, pp. 50-69. doi:http://dx.doi.org/10.18080/ajtde.v5n1.88

Djedjig, N; Tandjaoui, D; Medjek, F. 2015. 'Trust-based RPL for the Internet of Things'. 2015 IEEE Symposium on Computers and Communication (ISCC), 6-9 July 2015.

Fortier, PJ; Michel, H. 2002. *Computer Systems Performance Evaluation and Prediction*, Butterworth-Heinemann.

Gaddour, O; Koubâa, A; Abid, M. 2015. 'Quality-of-service aware routing for static and mobile IPv6-based low-power and lossy sensor networks using RPL'. Ad Hoc Networks, vol. 33, pp. 233-256. doi:http://dx.doi.org/10.1016/j.adhoc.2015.05.009

Glissa, G; Rachedi, A; Meddeb, A. 2016. 'A Secure Routing Protocol Based on RPL for Internet of Things'. 2016 IEEE Global Communications Conference (GLOBECOM), 4-8 Dec 2016.

Heurtefeux, K; Erdene-Ochir, O; Mohsin, N; Menouar, H. 2015. 'Enhancing RPL Resilience Against Routing Layer Insider Attacks'. 2015 IEEE 29th International Conference on Advanced Information Networking and Applications, 24-27 March 2015.

Kantert, J; Ringwald, C; Zengen, G. V; Tomforde, S; Wolf, L; Müller-Schloer, C. 2015. 'Enhancing RPL for Robust and Efficient Routing in Challenging Environments'. 2015 IEEE International Conference on Self-Adaptive and Self-Organizing Systems Workshops, 21-25 Sep 2015.

Copyright © 2018

Kasinathan, P; Pastrone, C; Spirito, MA; Vinkovits, M. 2013. 'Denial-of-Service detection in 6LoWPAN based Internet of Things'. 2013 IEEE 9th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), 7-9 Oct 2013.

Kumar, A; Matam, R; Shukla, S. 2016. 'Impact of packet dropping attacks on RPL'. 2016 Fourth International Conference on Parallel, Distributed and Grid Computing (PDGC), 22-24 Dec 2016.

Le, A; Loo, J; Chai, K; Aiash, M. 2016. 'A Specification-Based IDS for Detecting Attacks on RPL-Based Network Topology'. *Information*, vol. 7, no. 2, p. 25.

Mayzaud, A; Badonnel, R; Chrisment, I. 2017. 'A Distributed Monitoring Strategy for Detecting Version Number Attacks in RPL-Based Networks'. *IEEE Transactions on Network and Service Management*, vol. 14, no. 2, pp. 472-486. doi:10.1109/TNSM.2017.2705290

Nawir, M; Amir, A; Yaakob, N; Lynn, OB. 2016. 'Internet of Things (IoT): Taxonomy of security attacks'. 2016 3rd International Conference on Electronic Design (ICED), 11-12 Aug 2016.

Pongle, P; Chavan, G. 2015a. 'Real time intrusion and wormhole attack detection in internet of things'. *International Journal of Computer Applications*, vol. 121, no. 9.

Pongle, P; Chavan, G. 2015b. 'A survey: Attacks on RPL and 6LoWPAN in IoT'. 2015 International Conference on Pervasive Computing (ICPC), 8-10 Jan 2015.

Sehgal, A; Mayzaud, A; Badonnel, R; Chrisment, I; Schönwälder, J. 2014. 'Addressing DODAG inconsistency attacks in RPL networks'. 2014 Global Information Infrastructure and Networking Symposium (GIIS), 15-19 Sep 2014.

Summerville, DH; Zach, KM; Chen, Y. 2015. 'Ultra-lightweight deep packet anomaly detection for Internet of Things devices'. 2015 IEEE 34th International Performance Computing and Communications Conference (IPCCC), 14-16 Dec 2015.

Tan, K; Wu, D; Chan, A; Mohapatra, P. 2010. 'Comparing simulation tools and experimental testbeds for wireless mesh networks'. 2010 IEEE International Symposium on "A World of Wireless, Mobile and Multimedia Networks" (WoWMoM), 14-17 June 2010.

Taylor, C; Johnson, T. 2015. 'Strong authentication countermeasures using dynamic keying for sinkhole and distance spoofing attacks in smart grid networks'. 2015 IEEE Wireless Communications and Networking Conference (WCNC), 9-12 March 2015.

Thingsquare. 2016. 'Contiki: The Open Source OS for the Internet of Things'. Available from http://www.contiki-os.org/download.html

Copyright © 2018

Winter, T; Thubert, P (Eds). 2012. 'RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks'. Internet Engineering Task Force (IETF), RFC 6550. Available from https://tools.ietf.org/html/rfc6550 .

Copyright © 2018
http://doi.org/10.18080/ajtde.v6n1.138