Published on *Telsoc* (https://telsoc.org)

A Trust-Aware RPL Routing Protocol to Detect Blackhole and Selective Forwarding Attacks

David Airehrour [1]

Auckland University of Technology
Jairo Gutierrez [2]

Sayan Ray [3]

Manukau Institute of Technology

AJTDE - Vol 5, No 1 - February 2017 [4]

[5]

☆ 10 [6]

Abstract

This research addresses blackhole and selective forwarding routing attacks, which are fundamental security attacks on the routing of data in IoT networks. Most IoT devices today, from medical devices to connected vehicles and even smart buildings, have the capability of communicating wirelessly with one another. Although, consumers are progressively embracing the concept of connected devices, recent studies indicate that security is not high on the priority list of manufacturers, especially in the way these IoT devices route and communicate data amongst themselves. Thus, it leaves the door wide open to attacks and compromises. In this study, a trust-based routing Protocol for Low-Power and Lossy Networks, addressing blackhole and selective forwarding attacks is proposed. We show that our proposed protocol is not only secure from blackhole and selective

forwarding attacks, but also does not impose undue overheads on network traffic.

Keywords: IoT, RPL, Trust, Blackhole attacks, Selective Forwarding attacks

Introduction

The Internet of Things (IoT) can be described as a trend causing a global technological disruption today as a result of a melding of advances in computing and communication enterprises (Airehrour et al., 2016 [7]). IoT is set to transform, not only the user-to-machine interaction, but also the way machine-to-machine interacts. Already, we are witnessing the penetration of IoT devices in the market place. Various industrial sectors have begun witnessing the infiltration of IoT products into the fabric of several industries, including healthcare, energy, automotive and agriculture. Increasingly in these industries, users are witnessing the Industrial Internet of Things (IIoT), where devices such as sensors, exercise fit bits, robots and insulin pumps are progressively becoming more connected to one another (Chinn et al., 2014 [8]). It is perceived that Internet of Things will not only significantly change the future of the industrial sectors of the world but also will bring a positive transformation to how we live. A culmination of the full potential of the IoT vision will improve the standards of living of humanity because of the numerous value-creation opportunities while also improving the careers of many (Ericsson, 2011 [9]). It is expected that the wide adoption of IoT will lead to a plethora of novel smart paradigms like smart healthcare, smart agriculture and smart power, amongst others. This could eventually evolve into new ecosystems of IoT that are propelled by self-aware, autonomous machines.

However, the fact that these devices can communicate with one another and over the web, poses a security risk to the Industrial Control Systems (ICSs) and other connected online devices, and hence requires better security mechanisms. There is no doubt that IoT is creating a new epoch of innovation that connects the digital and machine ecosystems and brings better speed and effectiveness to many sectors as recounted above. Nevertheless, with sensitive information increasingly being made available online via the deployment of IoT, and more endpoints exposed to attackers, the research community ? and indeed the business world ? are swiftly recognising that security in IoT networks and IoT generally cannot be an afterthought.

A study by McKinsey (Chinn et al., 2014 [8]) projects that the cost of cybersecurity will increase to $3 trillion by 2020 and of this, many of the security technology measures are futile. Further to the projection by Ericsson (Ericsson, 2011 [9]) that the number of connected devices will reach 50 billion by 2020, there is a pressing need to profoundly rethink security for the always-connected, high-volume and distributed world of the Internet of Things. One typical area of exposure in IoT is the routing packets between different IoT devices. These packets move across heterogeneous networks and are thus susceptible to various security attacks common to both the digital and machine world. At this stage of the nascent development of IoT, the security challenges need to be addressed to engender confidence in the public and globally achieve success with IoT.

The objective of this research is to develop a lightweight trust-based Routing Protocol for low power and Lossy networks (RPL) that will address blackhole and selective forwarding attacks in IoT. A blackhole attack is a denial-of-service (DoS) class of attack in which a malicious node drops data packets rather than forwarding them towards the expected destination. In a selective forwarding attack, a malicious node examines the packets received and then decides on the class of packets to drop. "Class of packets" indicates either data packets or route packets but not both. The intention, in both attacks, is to destabilise the network and the flow of data in the network (DoS).

The rest of the paper is organised as follows: a discussion on the IoT routing protocols and the current industry standards is presented; this is followed by an introduction of the security features available in RPL with a highlight on the challenges in its implementation. A trust-based mechanism for RPL routing protocol is further introduced as a mitigation strategy against the RPL attacks. We show that our proposed protocol is both secure from blackhole and selective forwarding attacks, while not imposing undue overheads on network traffic. We present our simulation results using the Contiki/Cooja environment and we demonstrate the efficacy of our proposed trust-based RPL routing protocol. Finally, we present our conclusions and final notes on our future work.

Internet of Things: A Routing Protocol Perspective

Routing Protocols in IoT

A routing protocol is a communication process tasked with the responsibility of making intelligent routing decisions during the forwarding of routing data among nodes. Routing in sensor networks could be classified into two types, namely: reactive routing system (where a sender node triggers a route discovery to transmit data packets to a destination node) and proactive routing system (where a node constantly searches for path information to a destination network, so that the path is ready before it is required). Protocols developed are based on any of these two systems (Kute et al., 2012 [10]).

Routing Protocols for Low Power and Lossy Networks

The Routing protocol for low power and lossy networks (RPL) is an IPv6 routing protocol designed by the Routing Over Low power and Lossy networks (ROLL) of the Internet Engineering Task Group Force (IETF) (Winter et al., 2012 [11]). RPL was designed as a standard for low power and lossy networks, which includes all IoT sensor nodes. RPL is a protocol based on proactive routing, which operates by discovering routes after the RPL protocol commences. It forms a tree-like topology known as Destination Oriented Directed Acyclic Graph (DODAG). Every node in the RPL network selects a preferred parent based on some metrics (hop-count, expected transmission count, link reliability and link colour object) and this preferred parent acts like a gateway for that node. If a node seeks to forward a packet for which it does not have a path in its routing table, it simply forwards it to its preferred parent, which has a path either to the destination or to its own parent for onward transmission until it gets to the final destination in the tree. Path selection is an important factor for RPL, and hence the protocol uses multiple metrics for this purpose. Every node in the DODAG computes its rank from the perspective of the position of the DODAG root node (sink) and in relation to the position of the other nodes. The rank of a node decreases in the upward direction towards the DODAG root while it increases from the DODAG root towards the leaf nodes (sender nodes). RPL operates in two modes to perform downward routing: RPL non-storing mode (source routing) and RPL storing mode (stateful in-network routing). In storing mode, each packet holds the route path to the destination. This entails the DODAG root maintaining details about each node within the network. It is important to note that when operating in a non-storing mode, forwarding RPL nodes in the network need to retain their in-network routing tables to identify where to send their packets. However, in both modes discussed above, the RPL DODAG root still retains a database of all nodes for downward routing purposes (Winter et al., 2012 [11]).

RPL utilises three control message types for the creation and maintenance of its graph topology and route table. The control messages include: DODAG Information Object (DIO), DODAG Advertisement Object (DAO) and DODAG Information Solicitations (DIS). DIO is used for creation, maintenance and discovery of the DODAG topology. When an RPL network is started, nodes exchange DODAG information via the DIO. The DIO helps nodes to select their preferred parents. RPL uses DAO messages to transmit the prefix of a node to its ancestor nodes for downward routing purposes. The DIS message is used by any unattached node in the network to solicit for a potential parent node. DIS is triggered by a node in a situation when it cannot obtain a DIO after a certain time interval (Winter et al., 2012 [11]). The creation of a RPL network in a DODAG is referred to as a RPL instance. While many RPL instances can consist within a DODAG, these RPL instances can have their own unique object functions (OF) for routing purposes.

Security in RPL

Security has been identified as being critical in sensor networks that are resource constrained (Le et al., 2012 [12]). In addition, the complexity of deployment and size is also a core concern for these resource-constrained networks, such that it may not be cost effective, if not practically unrealistic, to embed sophisticated security mechanisms in an implementation of a RPL system. Further to that, several RPL deployments can resort to link-layer security or

other security systems to achieve their security goals while bypassing the security features that RPL may provide. Consequently, RPL security features could then be mere optional and non-obligatory extensions. RPL nodes can operate in three predefined security options.

The first is referred to as the "unsecured" option. In this option, the control messages in RPL are forwarded with no security primitives. The unsecured status implies that the RPL network could as well have adopted other security mechanisms (such as a link-layer security) to achieve application-specific requirements.

The second option is referred to as "pre-installed". In this option, nodes entering an RPL instance come embedded with pre-installed keys, which grants them processing and generation permission to safeguard RPL messages.

The third option is referred to as "authenticated". This option permits nodes to enter a network as leaf nodes using the embedded pre-installed keys while operating in a pre-installed mode, or nodes operate as multicasting nodes by getting a key from a central authentication authority.

In the last two options, there is a secure variant for every RPL message. The security features of 32-bit and 64-bit message authentication code (MAC) and encrypted message authentication code (ENC-MAC) options are well supported, while the algorithms (CCM and AES-128-bit encryption) have become new supported extensions in RPL as specified in the protocol messages (Winter et al., 2012 [11]). The safe variants of the RPL messages are meant to provide confidentiality, integrity, delay protection and replay protection as an added option.

However, the bad news is they all rely on past encryption solutions that have failed ? and which continue to fail (Nordrum, 2016 [13]). Public Key Infrastructure (PKI) was developed about four decades ago to safeguard the communications between two human parties. It was at no time designed to handle the complications of managing industrial-scale networks of 50 billion devices that IoT promises to usher in. The very thought of having a central authentication authority for billions of devices makes it extremely awkward and inefficient.

Attacks in RPL

The RPL protocol, like any other wireless sensor network protocol, has been shown to be vulnerable to routing attacks. These attacks have been researched and covered in (Chugh et al., 2012; [14] Tsao et al., 2014 [15]; Wallgren et al., 2013 [16]) among other papers; Table 1 shows a summary of attacks in RPL and some proposed solutions.

In (Weekly & Pister, 2012 [17]) the authors assume the use of cryptography and they specifically use the Secure Hash Algorithm 1 (SHA-1) as the hash function to protect the route messages being transmitted. The researchers also assume that the cryptographic system utilised is guaranteed hence, it will not be tampered with by any malicious nodes. As discussed under the section ?Security in RPL?, the use of cryptography (SHA-1) will certainly deplete the battery energy of the nodes and hence degrade network performance.

The assumption that the attacking nodes will not tamper with the cryptographic system makes the proposed solution impracticable in a real-world scenario. Of equal importance is the mobility of the nodes, when these nodes join and leave the network at will, implementing encryption becomes difficult as a specific node with certain network details required by other nodes suddenly becomes unavailable. The authors of (Raza et al., 2013 [18]) revealed the weaknesses in the implementation of the ContikiRPL viz-a-viz malicious attacks, and thus gave helpful insight into design issues that could help in the implementation of a better ContikiRPL. Raza et al. (2013 [18]) implemented an IDS system to defend against sinkhole and selective forwarding attacks and opined that it could also detect blackhole attacks; however, they assumed that key IDS nodes must be strategically placed. With a deluge of IoT devices randomly and remotely located, this may not be the case, and thus may not provide optimal defence against attacks.

Selective forwarding attacks work much like blackhole attacks; however in this type of attack, the malicious node selectively drops route or data packets so that it is almost imperceptible to the system that the loss was intentional. Most Selective attacks choose between dropping data packets or route packets. When a Selective forwarding attacker decides to drop only data packets, it does not intercept route packets. In this way, testing the end-to-end connectivity in a network will show no network problems, but packets still are not delivered to their destinations.

Selective forwarding attacks have been discussed in several works and we present some references for further reading (Bysani & Turuk, 2011 [19]; Hu et al., 2014 [20]; Mathur et al., 2016 [21]; Ren et al., 2016 [22]).

A summary of various attacks and proposed solutions is presented in Table 1. In addition, Table 1 highlights the impact of the proposed solutions on network performance. In a later section, we present an algorithmic trust-based approach to secure the RPL routing protocol. This proposed protocol, when implemented in RPL, counters blackhole and selective forwarding attacks.

A Trust-Based Mechanism for RPL Protocol

Blackhole and selective forwarding attacks perform malicious activities like causing high packet drops and high route and control packet overhead, which depletes the limited resources of the IoT nodes. When malicious nodes propagate blackhole and selective forwarding attacks, network latency increases and the ranks of the nodes are altered, which causes a disruption to the RPL network topology and to its stability. Additionally, the rank alteration causes the nodes to re-compute their ranks. The rank alteration triggers a local repair ? a self-healing mechanism that RPL uses to eliminate local routing loops. However, with the increase in these (blackhole and selective forwarding) attacks, the local repair eventually becomes inefficient, prompting a global repair by the DODAG root. A continuous initiation of these repair messages causes inefficiencies and disruption to the RPL network.

The section ?Security in RPL? asserts that the security-related solutions to prevent malicious activities in RPL, which include cryptography and authentication operations, are unable to cope with the billions of IoT devices. Besides, the encryption technology could be considered complex and energy consuming in the context of the limited available resources of the IoT sensor nodes. Therefore, a trust-based mechanism which employs a lightweight solution with respect to the limited resources of the nodes, presents an interesting solution for the security of RPL routing.

Table 1 Summary of RPL Attacks and Countermeasures

Type of attack	**Consequence on performance of network**	**Some proposed solutions**
Rank	Minimal packet delivery and high packet loss; high-cost path selection and routing loop	IDS centred solutions (Raza et al., 2013) [18], (Amin et al., 2009 [23]), VeRA (Dvir et al., 2011 [24]), TRAIL (Perreyet al., 2013 [25])
Selective forwarding	Destabilisation of route topology	Heartbeat protocol (Wallgren et al., 2013 [16])
Sinkhole	Transmitting network traffic via attacker node	IDS centred solutions (Raza et al., 2013 [18]), Parent fail-over, rank authentication technique (Weekly & Pister, 2012 [17])
Hello flooding	Degrading of sensor energy	The initiation of RPL?s local and global repair system addresses this attack
Wormhole	Destabilisation of route topology and network traffic	A Markle tree authentication solution system (Zhang et al., 2014 [26])
Sybil and Clone ID	Route traffic truncation and node traffic isolation	Routing attacks and countermeasures in RPL-Based IoT (Wallgren et al., 2013 [16])
Denial of Service	Unavailability of network resources	User centred IDS based system (Kasinathan et al., 2013 [27])
Blackhole	High packet drop-rate and high control and route traffic overhead	SVELTE (Raza et al., 2013 [18]), A packet traffic counter monitoring system (Chugh et al., 2012 [14]), A parent system fail-over mechanism (Weekly & Pister, 2012 [28]),
Version number	High traffic latency and high control overhead with minimal packet delivery ratio.	VeRA (Dvir et al., 2011 [24])

Local repair and Control overhead	Route and control traffic destabilisation	IDS system for intrusion detection (Le et al., 2012 [12])
Neighbour attack	Falsification of route and network resource depletion	TRAIL (Perrey et al., 2013 [25])
DIS attack	Network resource depletion	TRAIL (Perrey et al., 2013 [25])

Embedding Trust in RPL

We describe below our proposed trust-based mechanism, which is embedded into RPL protocol. The aim of the mechanism is to compute a trust value for each node in the RPL network while embedding computed trust values for routing decisions. In this way, our proposed mechanism will deliver the combined values of providing an optimal routing decision while also isolating malicious nodes that may seek to drop control and route packets. The trust mechanism also computes the effective feedback values between nodes. In our model, we make two basic assumptions:

< >that every node operates in promiscuous mode hence, they can overhear neighbour packet transmissions; and that every blackhole attacking node will over time begin to drop all route packets thus, the effective feedback communications between nodes (i.e. the number of packets a node could satisfactorily forward on behalf of the requesting node) will certainly reflect the blackhole nature of any node. In our new protocol, a trust-based mechanism is embedded into RPL to enhance its capability to isolate blackhole attacks and selective forwarding.

When RPL is initially started, a comparison is made between nodes based on the expected transmission count and the rank of the nodes. These are normal RPL operations to determine preferred parents and routing decisions. Further to that, our computed trust values, as depicted in equation 1, are sorted in descending order of magnitude of trust. The corresponding trusted node(s) are selected for routing decisions while still maintaining the rank order of all nodes in the RPL network. The trust is computed as:

Equation to compute trust EPij = Ndiv/Nsent [29]

Where 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. Our trust-based algorithm is shown in Figure 1.

RPL uses routing metrics defined in its Objective Function to create the DODAG. Essentially, the routing metrics defined in the objective function help in the creation of the network routes and hence, resulting in an optimal route. In the Contiki implementation of RPL, there are two objective functions, namely: Minimum Rank with Hysteresis Objective Function (MRHOF) based on RFC 6719 (Gnawali, 2012 [30]) and Objective Function zero (OF0). Contiki uses MRHOF by default, which minimises the expected transmission count (ETX) values. This research work compares the MRHOF?s implementation of RPL with our trust-based implementation of RPL.

Algorithm for blackhole and selective forwarding attacks detection

Let N1 ? one available item in the NeighbourList[ ]

Let N2 ? another item next to N1 in the NeighbourList[ ]

Compute

[29]

```
  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 1 A trust-based algorithm for the isolation of malicious nodes in RPL

Simulation and Results

In the simulation, we have assumed that the IoT sensors are deployed in a smart building with one level. The InstantContiki 3.0 platform (Thingsquare, 2016 [31]) is used to perform the simulation. The various simulation parameters are listed in Table 2. During simulation, the system considers the interference from its surroundings, such as other devices or technologies that may be in use. We have also used the TMote Sky mote (Cooja simulator) for simulation and have defined the IEEE 802.15.4 broadcast range to be 50 metres and the interference range as 100 metres.

Table 2 Simulation parameters of a 30-node network

Simulation Parameters	
Simulation tool	Contiki/Cooja 3.0
Mote type	Tmote Sky
Simulation run time	3600 seconds
Simulation coverage area	70m x 70m
Interference range	100m

Total number of nodes	30
Root node (sink)	1
Blackhole attack nodes	3
Legitimate nodes	26
Deployment environment	Smart building
Wireless transmission range	50 metres
Network protocol	IP based
Routing protocol	RPL

Figure 2 shows the deployment of sensor nodes. The blackhole attacking nodes are coloured pink and were allowed to run as good behaving nodes for a while before being manually activated, after a certain time has elapsed, to act maliciously. The same topology was also used for the deployment and simulation of the selective forwarding attacks. As shown in Figure 2, nodes 28, 29 and 30 were used for blackhole and selective forwarding attacks during RPL operations. In the simulation study, we have assumed that the attack nodes behave as good nodes from the start and commence their malicious activities over time (when activated). Figure 3 shows the activation of the blackhole attacker node (node 28) after a set threshold timer while Figure 10 shows the activation of the selective forwarding attacker node (node 30). The set threshold timer is set to 5 seconds, by which time, the network is assumed to have converged based on the specifications of RPL routing operations.

Blackhole attacks

The section following presents the simulation results of the blackhole attacks? detection and the associated network performance measurements.

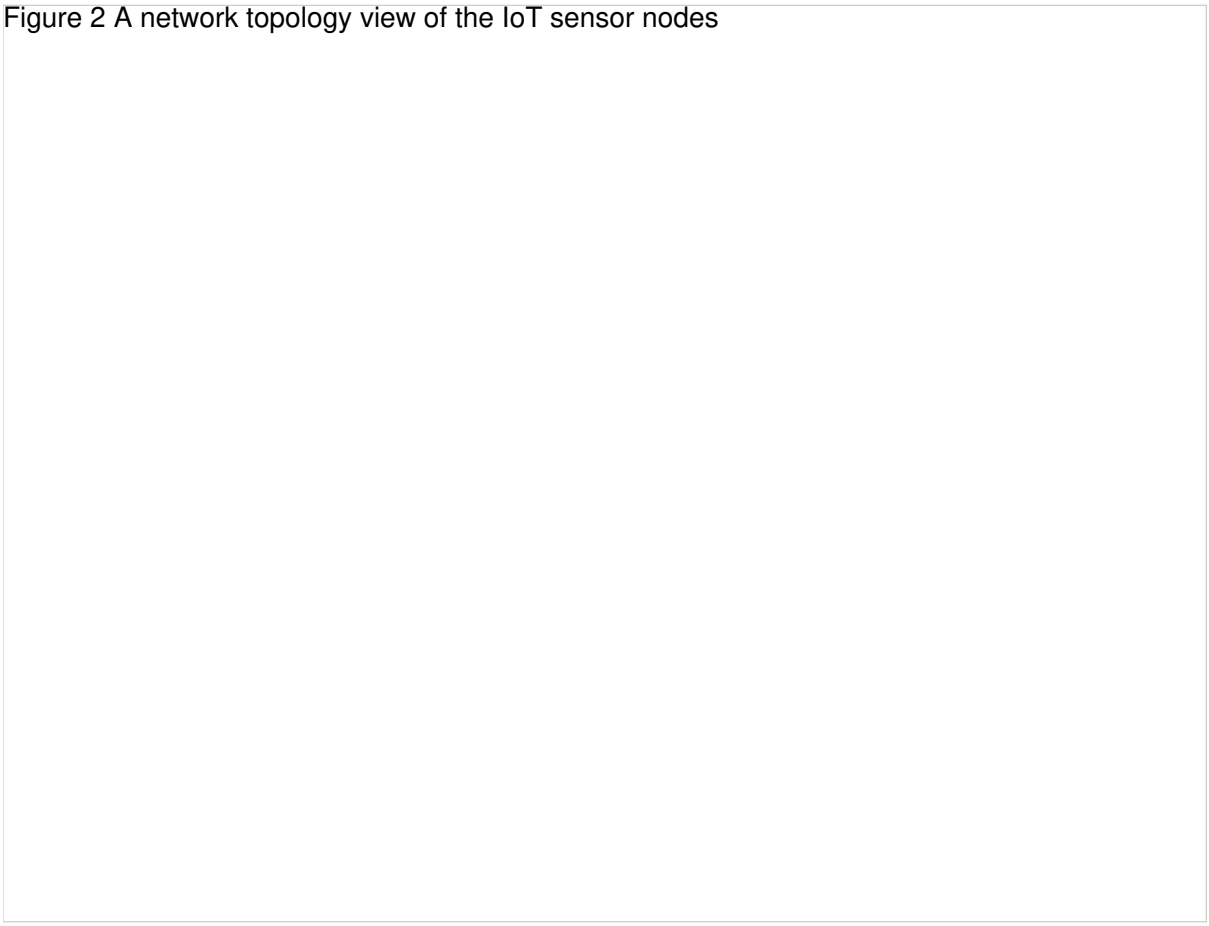
Detection and Isolation

In the simulation, sender nodes transmit packets to the sink node with the following stamp on each packet sent: time, source ID, packet type (sent or received), destination ID, sequence number and data size. This is shown in Figure 4. Packet sequence IDs are matched to ensure that packets sent are received by the sink node. Any sent packet sequence ID that is not matched with a corresponding received sequence ID by the sink node has either been black holed by the malicious node or affected by the lossy network link. However, the simulations showed strong reachability from the sender nodes to their neighbours. Furthermore, we have examined the packets dropped by the malicious nodes and they corresponded to the packets that have failed to reach the sink node. A complete log of the sent and received packets was analysed and the results presented in Figure 6. In Figure 5, the trust-based RPL protocol could detect and isolate the blackhole attacks during routing operations. A highlight of the attacks detected can be seen from the encircling blue pen-mark. In addition, Figure 5 displays a graph summary of

attacks detected and isolated during RPL operation using the trust-based RPL protocol over a 60-minute simulation period at an interval of 5 minutes. As many as 600 attacks were detected between the 40th and 45th minute of the RPL operation. Conversely, in MRHOF's RPL implementation these attacks could not be detected, as there was no mechanism to detect nor isolate blackhole attacks.

It is of note that in RPL routing, a node rank change shows a re-alignment of a child-node to another preferred parent-node. Blackhole attack nodes advertise themselves to their neighbour nodes as better routes in a guise to attract these unsuspecting nodes while eventually dropping their packets. In Figure 7, a comparison of the frequency of node rank changes between the two routing protocols is made. RPL with MRHOF showed high frequency in rank changes reflecting its high level of susceptibility to blackhole attacks while our trust-based RPL protocol showed a very marginal level of susceptibility.

Figure 2 A network topology view of the IoT sensor nodes



[32]

Figure 2 A network topology view of the IoT sensor nodes

Network Performance

Even though we have a protocol in place which could detect and isolate blackhole attacks during RPL operations, it becomes imperative that the new protocol should not impose undue overhead on the network performance. We present below a measurement of network throughput and packet loss rates to determine if our proposed protocol can deliver reasonable levels of network performance while isolating blackhole attacks when compared to MRHOF?s RPL.

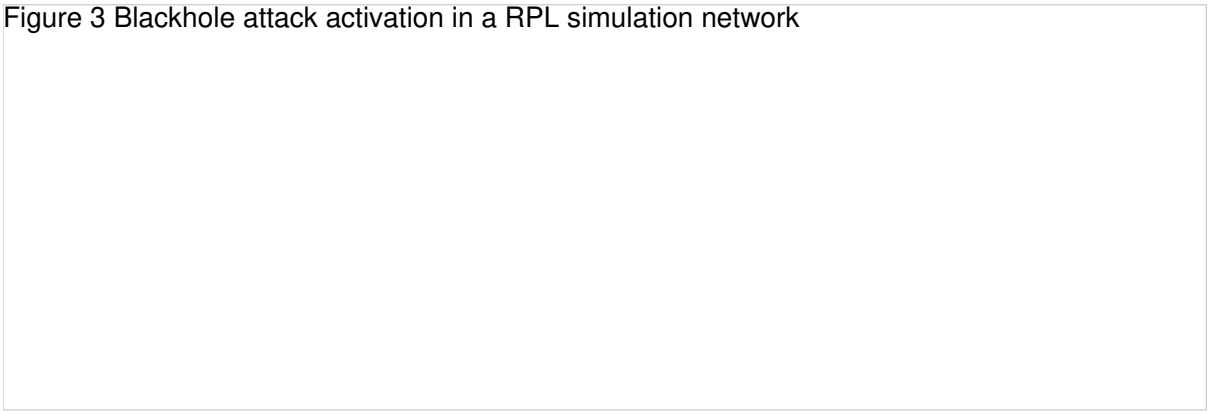
In Figure 8, the trust-based RPL showed significant improvement in throughput over the standard RPL (MRHOF). In fact, the throughput measurement of nodes 2-9, 15, 18, 19, 20, 22 and 25 was 0 kbps under MRHOF?s RPL because of the blackhole attacks on the network.

This indicates that these nodes were child-nodes to a blackhole parent-node. Meanwhile, with the trust-based RPL protocol, none of the nodes had a throughput of 0 kbps, which implies that no child node had a blackhole parent node. This indicates that these nodes were child-nodes to a blackhole parent-node. Meanwhile, with the trust-based RPL protocol, none of the nodes had a throughput of 0 kbps which implies that no child node had a blackhole parent node.

Figure 9 displays a graphical representation of the percentage of packet losses in RPL routing operation under blackhole attacks. While the trust-based RPL protocol's packet loss stayed below 40%, the standard RPL (MRHOF) recorded a staggering 60 to 100% packet loss rate.

Thus, the two network performance measurements presented above justify the trust-based RPL routing protocol as a better performing protocol over the standard RPL (MRHOF) under blackhole attacks.

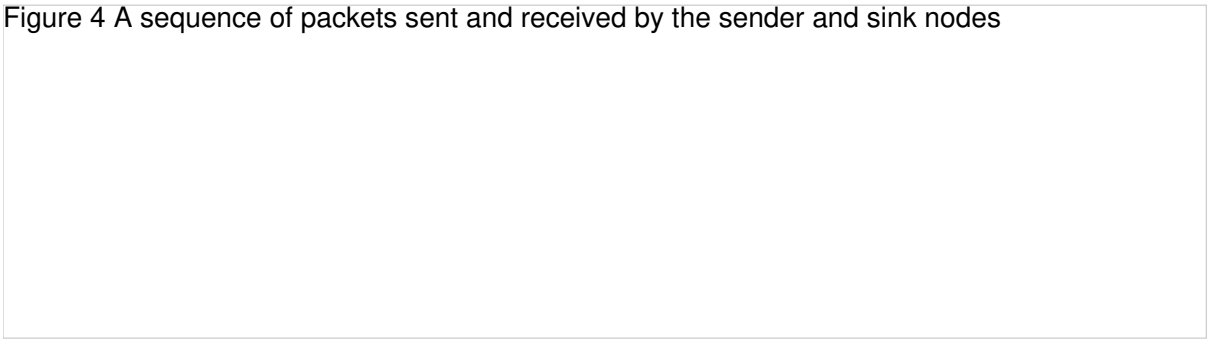
Figure 3 Blackhole attack activation in a RPL simulation network



[33]

Figure 3 Blackhole attack activation in a RPL simulation network

Figure 4 A sequence of packets sent and received by the sender and sink nodes



[34]

Figure 4 A sequence of packets sent and received by the sender and sink nodes

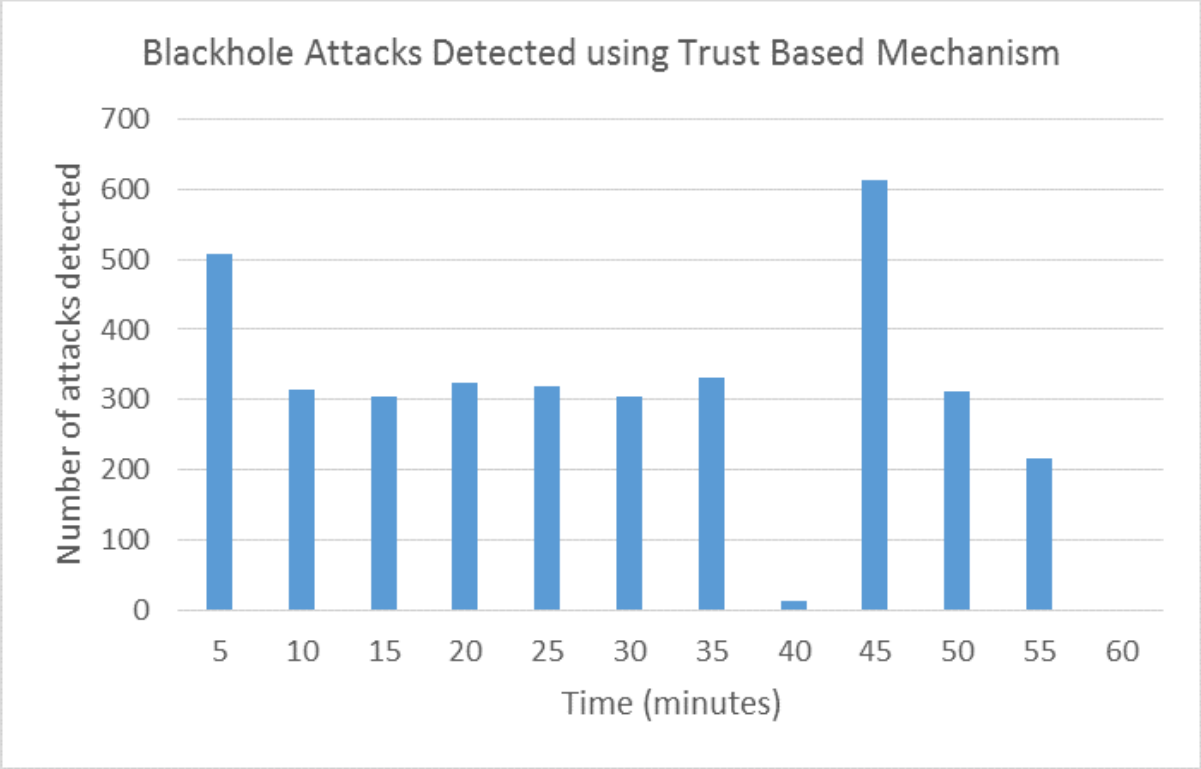
File Edit View

Time	Mote	Message
00:05.200	ID:21	RPL: parent node is changed and its rank is 512
00:05.201	ID:21	found the attacker
00:05.238	ID:23	RPL: parent node is changed and its rank is 512
00:05.239	ID:23	found the attacker
00:05.328	ID:24	RPL: parent node is changed and its rank is 512
00:05.329	ID:24	found the attacker
00:05.366	ID:8	RPL: parent node is changed and its rank is 512
00:05.367	ID:8	found the attacker
00:05.619	ID:18	RPL: parent node is changed and its rank is 512
00:05.621	ID:18	found the attacker
00:05.630	ID:14	RPL: parent node is changed and its rank is 768
00:05.641	ID:4	RPL: parent node is changed and its rank is 512
00:05.642	ID:5	RPL: parent node is changed and its rank is 768
00:05.643	ID:4	found the attacker
00:05.646	ID:19	RPL: parent node is changed and its rank is 768
00:05.646	ID:12	RPL: parent node is changed and its rank is 768
00:05.680	ID:27	RPL: parent node is changed and its rank is 512
00:05.681	ID:27	found the attacker
00:05.695	ID:7	RPL: parent node is changed and its rank is 512
00:05.697	ID:7	found the attacker
00:05.756	ID:15	RPL: parent node is changed and its rank is 512
00:05.757	ID:15	found the attacker
00:05.761	ID:25	RPL: select the best parent 1 and its rank is 512
00:05.765	ID:20	RPL: parent node is changed and its rank is 512
00:05.767	ID:20	found the attacker
00:05.894	ID:12	RPL: select the best parent 1 and its rank is 512

Filter:

[35]

Figure 5 Detection of Blackhole attacking nodes during RPL operation

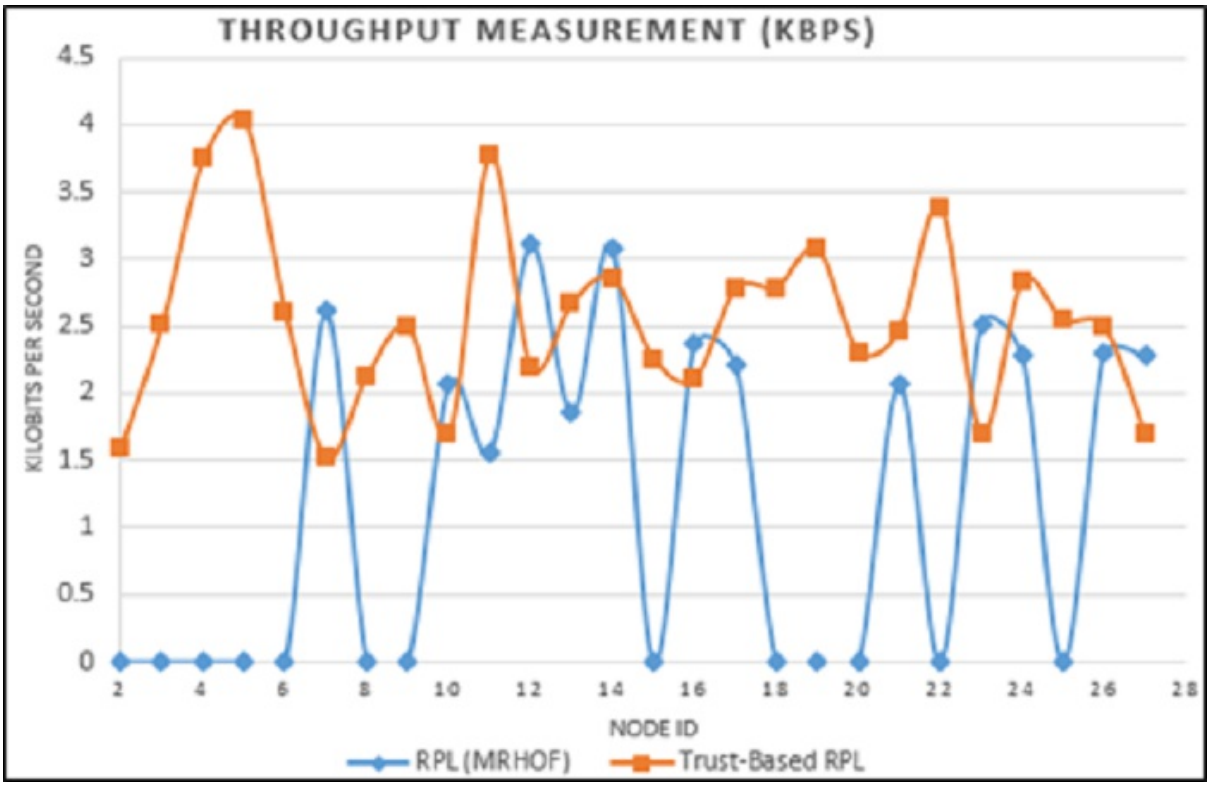


[36]

Figure 6 Trust-based detection and isolation of blackhole attacks in RPL

[37]

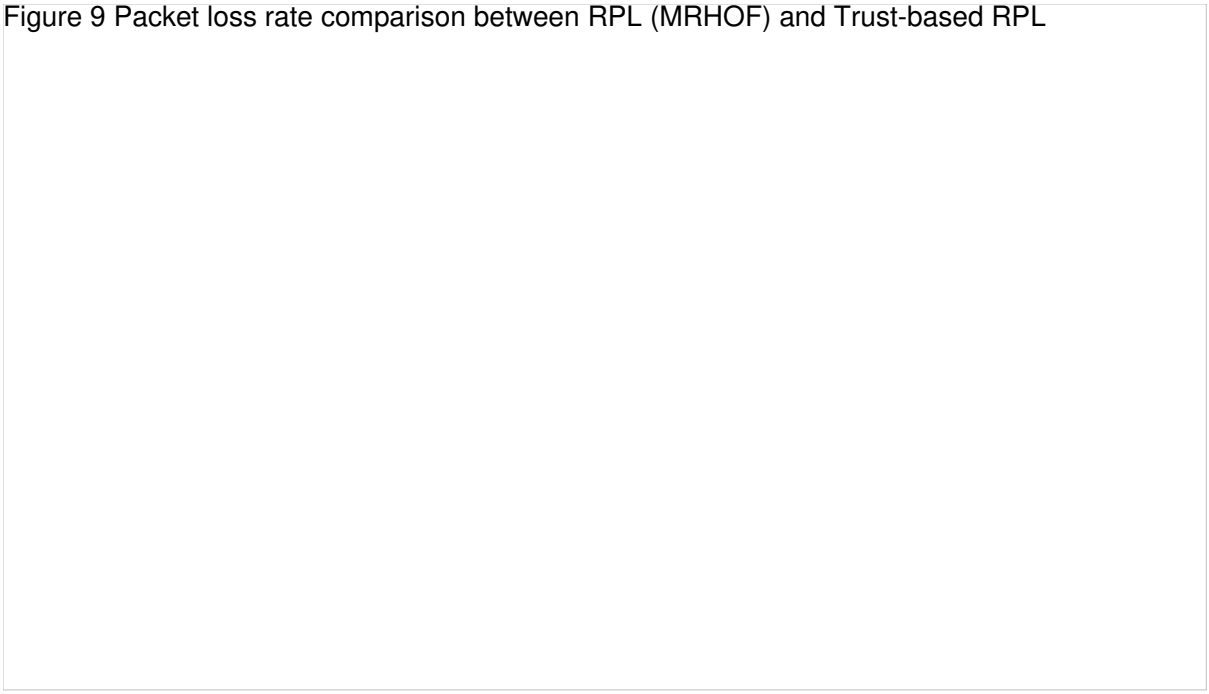
Figure 7 Comparison of frequency of node rank changes during blackhole attacks in RPL network during simulation



[38]

Figure 8 Comparison of throughput measurements between RPL (MRHOF) and Trust-based RPL

Figure 9 Packet loss rate comparison between RPL (MRHOF) and Trust-based RPL



[39]

Figure 9 Packet loss rate comparison between RPL (MRHOF) and Trust-based RPL

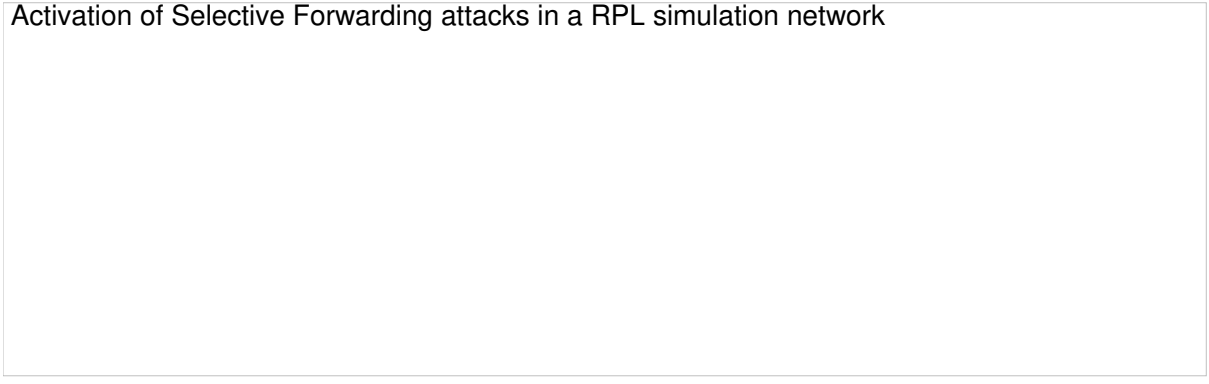
Selective Forwarding Attacks

A summary of the simulation results of the selective forwarding attacks detection, isolation and network performance measurement are presented below.

Detection and Isolation

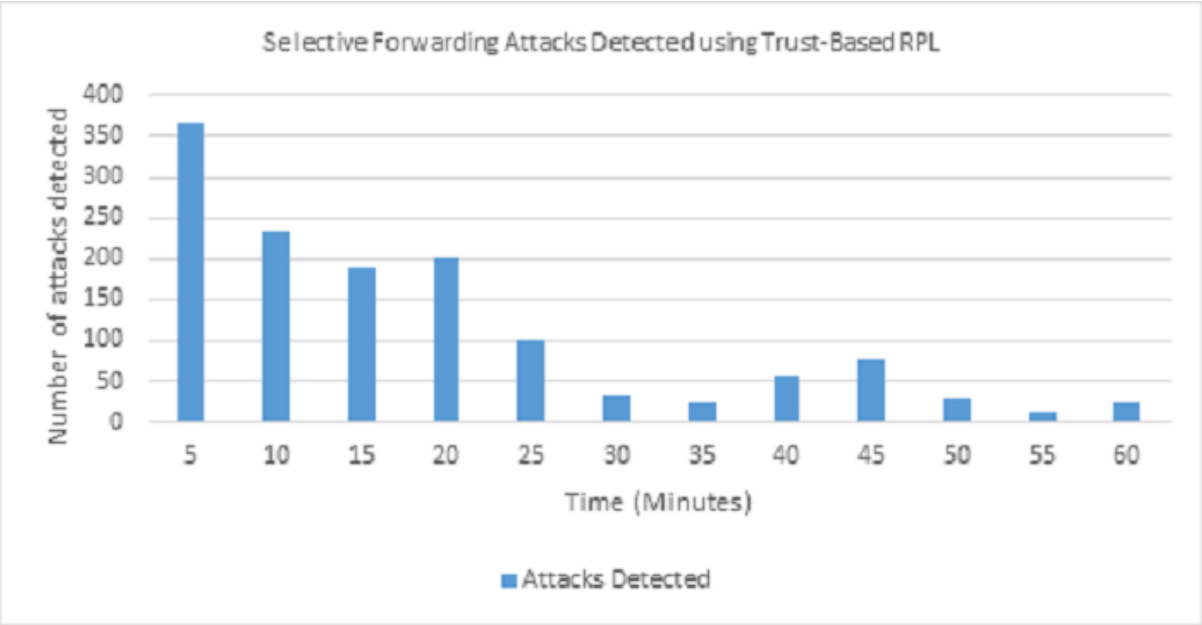
This section discusses the results of the simulation study of MRHOF-RPL and Trust-based RPL under selective forwarding attacks. As shown in Figure 10, node 30 was manually activated for selective forwarding attacks during RPL simulation. Similarly, other attack nodes (28 and 29) were also activated. As explained in the sub-section under ?Attacks in RPL?, a selective forwarding attack is a subtle variation of a blackhole attack where malicious nodes selectively drop packets during routing communications. From the results shown in Figure 11, Trust-based RPL could detect and isolate selective forwarding attacks during routing operations. In the simulation, the first 25 minutes of RPL operation witnessed a flooding of selective forwarding attacks. However, starting from the 30^{th} minute, the attacks were progressively and significantly reduced because Trust-Based RPL protocol could identify and isolate the malicious nodes. Hence, those malicious nodes were not subsequently considered for future routing decisions. On the other hand, MRHOF-RPL was not able to identify any of the selective forwarding attacks being perpetrated in the RPL network as evident from the high frequency of node rank changes shown in Figure 12. MRHOF-RPL showed significantly higher frequency node rank changes over our proposed trust-based RPL.

Activation of Selective Forwarding attacks in a RPL simulation network



[40]

Figure 10: Activation of Selective Forwarding attacks in a RPL simulation network

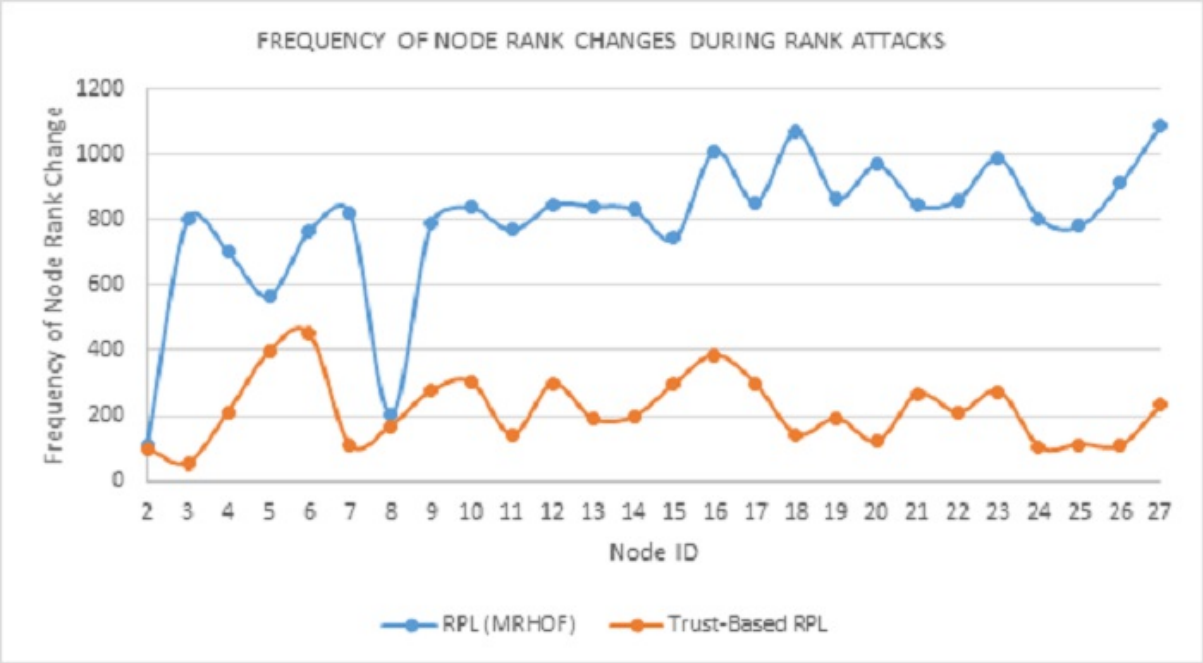


[41]

Figure 11: Detection and isolation of Selective Forwarding Attacks in a RPL simulation network

A RPL network with a stable topology will send route and control information based on the DIO trickle timer while the timer value increases with a stable network. However, an RPL network environment with high network topology changes will cause frequent transmission of control and route information. The topology changes could be due to the mobility of nodes or to suspicious activities of some malicious nodes in the network. This makes it necessary to have node re-alignment with new parents and that, in turn, results in a high frequency of rank changes among the nodes. Since the nodes are not mobile, we can conclude that changes in the rank of the nodes are purely because of the suspicious activities of the malicious nodes in the RPL network.

Figure 12 below provides a comparison of the frequency of changes in the node rank between the MRHOF-RPL and the Trust-based-RPL. MRHOF-RPL showed significantly higher node rank changes over our Trust-based RPL protocol reflecting a higher level of vulnerability to Rank attacks. As shown in the Figure, node 3 of the MRHOF-RPL had an initial spike of 800 node rank changes while that frequency in most other nodes ranges from 800 to 1,100. This range clearly reflects a high destabilisation of the network topology. As mentioned earlier in the paper, the high frequency of node rank changes not only destabilises the RPL network, but also affects both the efficiency and performance of any RPL network. Except for the spike experienced on node 6 with a node rank change of about 450 (refer to Figure 12), the Trust-based RPL protocol maintained a fairly consistent value of less than 400 node rank changes throughout the simulation time of 60 minutes.



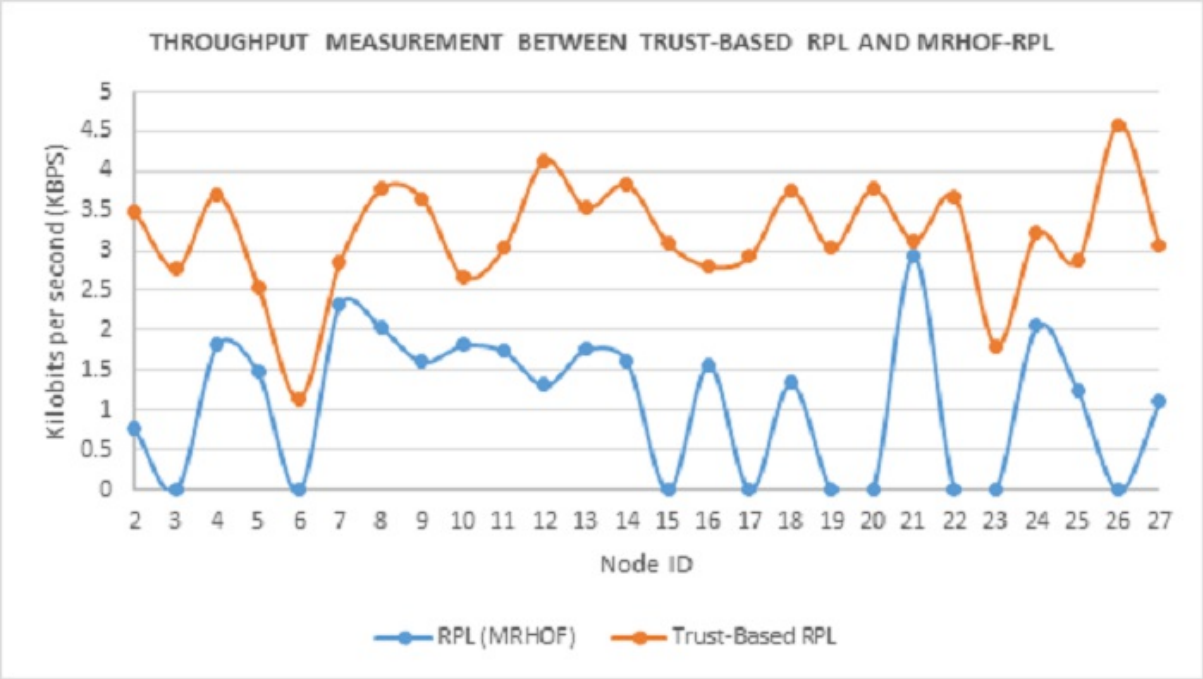
[42]

Figure 12: Comparison of frequency of node rank changes during Selective Forwarding attacks in RPL network simulation

Network Performance

Here we present a comparison of the MRHOF-RPL and the proposed Trust-based RPL during selective forwarding attacks based on network throughout and packet loss. As shown in Figure 13, in MRHOF-RPL, seven nodes, namely, 6, 15, 17, 19, 20, 22, and 26, have zero kbps throughput indicating that they are aligned to malicious parents that have selectively blackholed their packets. For example, following are the number of packets transmitted by each of these nodes that are not delivered to the sink node: Node 6 (packet sent, 52), Node 15 (packet sent, 52), Node 17 (packet sent, 52), Node 19 (packet sent, 52), Node 20 (packet sent, 52), Node 22 (packet sent, 52) and Node 26 (packet sent, 52). The remaining nodes, although they had some packets delivered to the sink node however, by observing their disproportionate packet delivery rates, we can conclude that they were affected by the activities of the malicious nodes in the network.

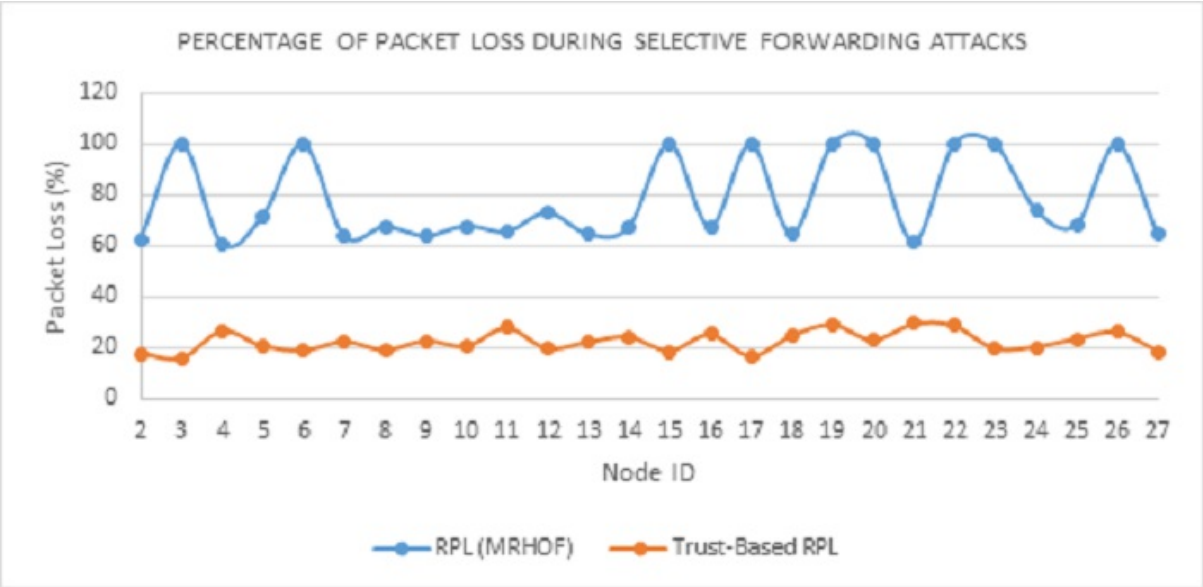
On the contrary, Trust-based-RPL has shown significant improvement in throughput over MRHOF-RPL and has maintained a much higher throughput range overall, except for nodes 2 and 23 that record less than 2 kbps in throughput due to malicious activities. Thus, we can conclude that, as evident from Figure 13, our Trust-based RPL protocol provides much better network throughput than the MRHOF-RPL protocol during selective forwarding attacks.



[43]

Figure 13: Comparison of network throughput between Trust-based-RPL and MRHOF-RPL during Selective Forwarding attacks

Figure 14 presents a comparison of the two protocols with regards to the percentage of packet losses in each node. From the Figure, it is evident that under selective forward attacks, while MRHOF-RPL had 60-70% lost packets during RPL operation, in the case of Trust-based RPL it was only 30%. This proves the efficacy of our Trust-based RPL protocol in delivering an acceptable network performance while isolating selective forwarding attack nodes in the network.



[44]

Figure 14 Percentage of packet loss in Trust-based-RPL and MRHOF-RPL protocols during selective forwarding attacks

Conclusions

In IoT networks, compromised sensor nodes can destabilise the integrity of data routing by intentionally (a) transmitting incorrect control and route information, (b) dropping all packets, (c) injecting false routing information during data aggregation, and (d) hampering the forwarding of composite data. Since cryptographic methods have proved to be inadequate in the prevention of these attacks, especially on a massive scale of billions of IoT nodes, a trust-based RPL protocol has been presented in this paper. The proposed novel reliable routing protocol provides a

feedback-back based trust-aware security protocol for IoT networks. The protocol computes a trust value for any node in the IoT network based on the good packet forwarding behaviour of neighbouring network nodes. The trust value is dependent on the positive feedbacks observed about the packet forwarding behaviour among nodes. From results presented in the simulation, we therefore conclude that our proposed trust-based RPL protocol can provide comprehensive security against blackhole and selective forwarding attacks.

Our future work intends to incorporate energy metrics into the protocol to isolate the nodes with depleting energy levels from routing decisions, while providing them with the opportunity to recoup their battery power.

References

Airehrour, D; Gutierrez, J; Ray, S. K. 2016. Secure routing for internet of things. *J. Netw. Comput. Appl., 66*(C), 198-213. doi: 10.1016/j.jnca.2016.03.006

Amin, S. O; Siddiqui, M. S; Hong, C. S; Choe, J. 2009. *A novel coding scheme to implement signature based IDS in IP based Sensor Networks.* Paper presented at the Integrated Network Management-Workshops, 2009. IM'09. IFIP/IEEE International Symposium on.

Bysani, L. K; Turuk, A. K. 2011. *A survey on selective forwarding attack in wireless sensor networks.* Paper presented at the Devices and Communications (ICDeCom), 2011 International Conference on.

Chinn, D; Kaplan, J; Weinberg, A. 2014. Risk and responsibility in a hyperconnected world: Implications for enterprises: McKinsey Global Institute.

Chugh, K; Aboubaker, L; Loo, J. 2012. *Case Study of a Black Hole Attack on LoWPAN-RPL.* Paper presented at the Proc. of the Sixth International Conference on Emerging Security Information, Systems and Technologies (SECURWARE), Rome, Italy (August 2012).

Dvir, A; Holczer, T; Buttyan, L. 2011. *VeRA-version number and rank authentication in rpl.* Paper presented at the Mobile Adhoc and Sensor Systems (MASS), 2011 IEEE 8th International Conference on.

Ericsson. 2011. More than 50 billion connected devices: Driving forces. http://www.akos-rs.si/files/Telekomunikacije/Digitalna_agenda/Internetni_protokol_Ipv6/More-than-50-billion-connected-devices.pdf [45]

Gnawali, O. 2012. The minimum rank with hysteresis objective function. https://tools.ietf.org/html/rfc6719 [46]

Hu, Y; Wu, Y; Wang, H. 2014. Detection of insider selective forwarding attack based on monitor node and trust mechanism in wsn. *Wireless Sensor Network, 6*(11), 237.

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

Kute, D. S; Patil, A. S; Pardakhe, N. V; Kathole, A. B. 2012. A Review: Manet Routing Protocols And Different Types of Attacks In Manet. *International Journal of Wireless Communication, 2*(1), 26-28.

Le, A; Loo, J; Lasebae, A; Aiash, M; Luo, Y. 2012. 6LoWPAN: a study on QoS security threats and countermeasures using intrusion detection system approach. *International Journal of Communication Systems, 25*(9), 1189-1212. doi: 10.1002/dac.2356

Mathur, A; Newe, T; Rao, M. 2016. Defence against black hole and selective forwarding attacks for medical WSNs in the IoT. *Sensors, 16*(1), 118.

Nordrum, A. 2016. Quantum Computer Comes Closer to Cracking RSA Encryption. *IEEE Spectrum*.

Perrey, H; Landsmann, M; Ugus, O; Schmidt, T. C; W?hlisch, M. 2013. TRAIL: Topology Authentication in RPL. *arXiv preprint arXiv:1312.0984*.

Raza, S; Wallgren, L; Voigt, T. 2013. SVELTE: Real-time intrusion detection in the Internet of Things. *Ad Hoc*

Netw., 11(8), 2661-2674. doi: 10.1016/j.adhoc.2013.04.014

Ren, J; Zhang, Y; Zhang, K; Shen, X. 2016. Adaptive and channel-aware detection of selective forwarding attacks in wireless sensor networks. *IEEE Transactions on Wireless Communications, 15*(5), 3718-3731.

Thingsquare. 2016. Contiki: The Open Source OS for the Internet of Things,. Retrieved June, 2016, from http://www.contiki-os.org/download.html [47]

Tsao, T; Alexander, R; Dohler, M; Daza, V; Lozano, A; Richardson, M. 2014. A Security Threat Analysis for Routing Protocol for Low-power and lossy networks (RPL).

Wallgren, L; Raza, S; Voigt, T. 2013. Routing Attacks and Countermeasures in the RPL-Based Internet of Things. *International Journal of Distributed Sensor Networks, 2013*, 11. doi: 10.1155/2013/794326

Weekly, K; Pister, K. 2012. *Evaluating sinkhole defense techniques in RPL networks.* Paper presented at the Network Protocols (ICNP), 2012 20th IEEE International Conference on.

Winter, T; Thubert, P; Brandt, A; Hui, J; Kelsey, R; Levis, P; . . . Alexander, R. 2012. RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks. https://tools.ietf.org/html/rfc6550 [48]

Zhang, K; Liang, X; Lu, R; Shen, X. 2014. Sybil Attacks and Their Defenses in the Internet of Things. *Internet of Things Journal, IEEE, 1*(5), 372-383.

Cite this article as:

David Airehrour, Jairo Gutierrez, Sayan Ray. 2017. *A Trust-Aware RPL Routing Protocol to Detect Blackhole and Selective Forwarding Attacks*. ajtde, Vol 5, No 1, Article 2. http://doi.org/10.18080/ajtde.v5n1.2 [50]. Published by Telecommunications Association Inc. ABN 34 732 327 053. https://telsoc.org [51]

RPL [52]
blackhole attacks [53]
Selective Forwarding attacks [54]
Trust [55]
Internet of Things [56]
Cyber security [57]
IoT [58]

Links
[1] https://telsoc.org/journal/author/david-airehrour
[2] https://telsoc.org/journal/author/jairo-gutierrez
[3] https://telsoc.org/journal/author/sayan-ray
[4] https://telsoc.org/journal/ajtde-v5-n1

[5] https://www.addtoany.com/share#url=https%3A%2F%2Ftelsoc.org%2Fjournal%2Fajtde-v5-n1%2Fa2-0&title=A%20Trust-Aware%20RPL%20Routing%20Protocol%20to%20Detect%20Blackhole%20and%20Selective%20Forwarding%20Attacks
[6] https://telsoc.org/printpdf/1744?rate=yipEHwixdtZgwp9ArFbOqV7RMiSp6VBez-JGnzLcY9g
[7] https://telsoc.org/journal/ajtde-v5-n1/a2-0#Airehrour_2016
[8] https://telsoc.org/journal/ajtde-v5-n1/a2-0#Chinn_2014
[9] https://telsoc.org/journal/ajtde-v5-n1/a2-0#Ericsson_2011
[10] https://telsoc.org/journal/ajtde-v5-n1/a2-0#Kute_2012
[11] https://telsoc.org/journal/ajtde-v5-n1/a2-0#Winter_2012
[12] https://telsoc.org/journal/ajtde-v5-n1/a2-0#Le_2012
[13] https://telsoc.org/journal/ajtde-v5-n1/a2-0#Nordrum_2016
[14] https://telsoc.org/journal/ajtde-v5-n1/a2-0#Chugh_2012
[15] https://telsoc.org/journal/ajtde-v5-n1/a2-0#Tsao_2014
[16] https://telsoc.org/journal/ajtde-v5-n1/a2-0#Wallgren_2013
[17] https://telsoc.org/journal/ajtde-v5-n1/a2-0#Weekly_2012
[18] https://telsoc.org/journal/ajtde-v5-n1/a2-0#Raza_2013
[19] https://telsoc.org/journal/ajtde-v5-n1/a2-0#Bysani_2011
[20] https://telsoc.org/journal/ajtde-v5-n1/a2-0#Hu_2014
[21] https://telsoc.org/journal/ajtde-v5-n1/a2-0#Mathur_2016
[22] https://telsoc.org/journal/ajtde-v5-n1/a2-0#Ren_2016
[23] https://telsoc.org/journal/ajtde-v5-n1/a2-0#Amin_2009
[24] https://telsoc.org/journal/ajtde-v5-n1/a2-0#Dvir_2011
[25] https://telsoc.org/journal/ajtde-v5-n1/a2-0#Perrey_2013
[26] https://telsoc.org/journal/ajtde-v5-n1/a2-0#Zhang_2014
[27] https://telsoc.org/journal/ajtde-v5-n1/a2-0#Kasinathan_2013
[28] https://telsoc.org/journal/ajtde-v5-n1/a2-0#_ENREF_21
[29] https://telsoc.org/sites/default/files/images/tja/equation_1.png
[30] https://telsoc.org/journal/ajtde-v5-n1/a2-0#_ENREF_8
[31] https://telsoc.org/journal/ajtde-v5-n1/a2-0#Thingsquare_2016
[32] https://telsoc.org/sites/default/files/images/tja/figure_2.png
[33] https://telsoc.org/sites/default/files/images/tja/2017032figure_3.png
[34] https://telsoc.org/sites/default/files/images/tja/2017032figure_4.png
[35] https://telsoc.org/sites/default/files/images/tja/2017032figure_5.png
[36] https://telsoc.org/sites/default/files/images/tja/2017032figure_6.png
[37] https://telsoc.org/sites/default/files/images/tja/2017032figure_7.png
[38] https://telsoc.org/sites/default/files/images/tja/2017032figure_8.png
[39] https://telsoc.org/sites/default/files/images/tja/2017032figure_9.png
[40] https://telsoc.org/sites/default/files/images/tja/2017032figure_10.png
[41] https://telsoc.org/sites/default/files/images/tja/2017032figure_11.png
[42] https://telsoc.org/sites/default/files/images/tja/2017032figure_12.png
[43] https://telsoc.org/sites/default/files/images/tja/2017032figure_13.png
[44] https://telsoc.org/sites/default/files/images/tja/2017032figure_14.png
[45] http://www.akos-rs.si/files/Telekomunikacije/Digitalna_agenda/Internetni_protokol_Ipv6/More-than-50-billion-connected-devices.pdf
[46] https://tools.ietf.org/html/rfc6719
[47] http://www.contiki-os.org/download.html
[48] https://tools.ietf.org/html/rfc6550
[49] https://telsoc.org/copyright
[50] http://doi.org/10.18080/ajtde.v5n1.2
[51] https://telsoc.org
[52] https://telsoc.org/topics/rpl
[53] https://telsoc.org/topics/blackhole-attacks
[54] https://telsoc.org/topics/selective-forwarding-attacks
[55] https://telsoc.org/topics/trust
[56] https://telsoc.org/topics/internet-things
[57] https://telsoc.org/topics/cyber-security
[58] https://telsoc.org/topics/iot