International Journal of Future Generation Communication and Networking
Vol. 11, No. 5 (2018), pp.45-62
http://dx.doi.org/10.14257/ijfgcn.2018.11.5.05

Study of Security Mechanisms and Simulation Analysis of Packet Drop in RPL in Low Power Lossy Networks

Nikita Malik[1*], Prakash Rao Ragiri[2] and Aarti Jain[3]

[1]*Research Scholar, USIC&T, GGSIPU*
[2]*Assistant Professor, Dept. of CSE, AIACT&R, GGSIPU*
[3]*Assistant Professor, Dept. of ECE, AIACT&R, GGSIPU*
[1]*nikitamalik92@gmail.com*, [2]*prakashraoragiri@gmail.com*,
[3]*rtjain2001@gmail.com*

Abstract

A large number of small sensor nodes or motes can be randomly distributed in any environment. These nodes communicate with each other over a low power wireless communication medium since they are severely restricted in their resources. Owing to these constraints, nodes in low power and lossy networks (LLNs) need to collaborate in order to establish a multi-hop network in which data is transmitted over several nodes to reach the sink node(s). Such communications over the radio environment are prone to various attacks, such as the RPL (Routing Protocol for Low Power and Lossy Networks) Packet Drop attack, which participates in the routing process to accept packets from the neighboring motes, only to drop them instead of forwarding in the route to the destination. Such an attack is generally hard to detect and to provide defenses against. In this paper, through simulations on Contiki's network simulator COOJA, the impact of RPL Packet Drop attack on Contiki RPL is observed for performance based on average power consumption, received packet count, expected transmission count and hop count. Based on the results, several security schemes to tackle RPL in LLN have been studied.

Keywords: *Contiki Network Simulator, LLN, Packet Drop Attack, RPL, Security measures, Wireless Sensor Networks*

1. Introduction

LLNs consist of several devices that have constrained memory and power, limited processing resources and restricted filed of sensing. These embedded devices can be interconnected to each other through a number of links like wired links, low power Wi-Fi, IEEE 802.15.4, Bluetooth, or other low power line communication links [8]. Wireless Sensor Networks (WSN) are LLNs with a huge collection of autonomous devices that are spatially distributed to communicate wirelessly and used to monitor application specific physical or environmental conditions. WSNs form an important part of the Internet of Things (IoT). Some of the applications where wireless sensor nodes are deployed include environment monitoring, house automation, machine surveillance and preventive maintenance, disaster relief operations, medicine and healthcare, military applications etc. Sensor node, or 'mote', is a small, smart, and a self-organizing multi-functional device, which consists of a sensor, radio communication, microcontroller and a battery. Because of the tough deployment environments for WSN and the use of wireless mediums, security in WSNs poses more severe challenges as compared to that in traditional networks. Security issues in WSNs include processing, power and memory limitations, data loss due to unreliable transfer, collisions and latency, and physical attacks [4]. Any

Received (May 13, 2018), Review Result (July 1, 2018), Accepted (July 6, 2018)
* Corresponding Author

ISSN: 2233-7857 IJFGCN

system employing a network of these motes must be able to provide secure routing of data through the network. It is therefore required for the systems to be protected from the kind of security attacks which are capable of rendering the system useless by rejecting data/control message deliveries. These kinds of attacks are classified as Denial of Service (DoS) attacks. DoS attacks include wide-ranging generic or specialized attacks which can be categorized further as network-based or host-based. Packet drop attack is one such attack in which the node that is supposed to relay packets instead discards them, reducing the throughput of the network.

Because of the sensor nodes' constrained capabilities, conventional mechanisms for security that require huge computations and communication overhead are unsuitable in WSNs. After studying the related literature, it has been observed that researchers have proposed mechanisms to detect the packet dropping blackhole attack and mitigate its effect through monitoring, trust mechanism, multi hop routing and cryptography based methods, each with their own set of pros and cons. In this paper, malicious motes creating blackhole regions in the WSN have been simulated using Contiki OS's network simulator COOJA to observe the impact of the RPL packet drop attack on LLNs. The network performance evaluation metrics used are average power consumption, received packet count, expected transmission count (ETX), hop count.

The paper is organized as follows- Section 2 provides background information for IEEE 802.15.4 standard and RPL protocol, detailing its operation and the packet drop attack along with its algorithm for ContikiRPL. The simulation scenario along with the various protocols used, parameters and performance metrics applied is discussed in Section 3, followed by the analysis and discussion of the obtained results. Based on the results, a review of the security mechanisms against such attacks is presented in Section 4, and finally the conclusion and future work in Section 5.

2. Theoretical Background

This section gives an overview of the IEEE 802.15.4 standard used for WSN and the operation of RPL protocol and packet drop attack, along with its algorithm, as implemented on ContikiRPL.

2.1. IEEE 802.15.4

The IEEE 802.15.4 standard defines, for the networks with low power consumption, low data rate and lower cost applications, both the MAC and physical layer protocols. This technical standard provides the basis for other standards like Zigbee, which extend it by further developing the upper layers that are not defined. Using mechanisms of encapsulation and header compression defined by 6LowPan technology, sending and receiving of IPv6 packets can also be allowed by IEEE 802.15.4, which is an acronym for IPv6 over Low power Wireless Personal Area Networks (LoWPAN). IEEE standard 802.15.4 focuses primarily on providing low-cost, low-speed ad hoc communication, and hence offers a type of wireless personal area network. In comparison to other approaches like Wi-Fi, that require more power and offer more bandwidth, the emphasis in IEEE 802.15.4 standard is on nearby devices' communication without any underlying infrastructure, in low cost and lowest power consumption possible.

The physical layer defined by this standard is responsible for managing the physical radio frequency transceiver. It also performs channel section and management functions for energy and signals. The medium access control (MAC) layer defined by this standard is responsible for enabling the transmission of MAC frames through the physical channel. It also manages network beaconing and access to physical channels. Besides this, node associations can be handled by it, time slots can be guaranteed, validation of frames can be controlled and secure services be provided. Beacon-enabled and non-beacon enabled are the two operational modes supported. This work uses beacon-enabled coordinator that

periodically sends out beacon frames depending upon the value of Beacon Interval (BI), for enabling the nodes to associate and synchronize in the network. The BI refers to the time interval between two consecutive beacon frames, which is divided into an active and an inactive portion as shown in Figure 1, and is regulated by the two parameters of superframe order (SO) and beacon order (BO). The active portion of the BI is called as the superframe. This active portion is divided into sixteen equally-sized time slots during which transmission of frames is allowed. The first slot of this is allotted for transmission of beacons [22].

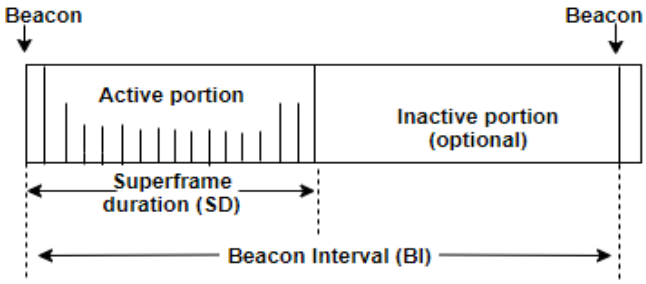

Figure 1. Beacon Interval *(Source: Zen et al. 2008)*

A node that receives the beacon frames can begin transmitting data in accordance with the mechanism of CSMA-CA. In case a node fails to receive beacon frames more than a preset number of times, it loses its synchronization and is then unable to receive or transmit any data.

This IEEE standard defines two kinds of network nodes- a full-function device (FFD) that can serve as a normal node or the coordinator of a PAN and can relay messages or communicate with any other device, and a reduced-function devices (RFD) that is meant to have simple communication and resource needs and can't act as coordinators, but only communicate with FFDs. IEEE 802.15.4 supports various topologies such as peer to peer networks with arbitrary patterns of connections between nodes, or cluster tree where a FFD forms tree root that is connected to multiple FFDs and RFDs as children in the tree structure, or star topology with a central FFD node as the coordinator. The one topology used in this work is a generic mesh network where the nodes form a cluster tree network with a global coordinator along with separate local coordinator for each cluster.

IEEE 802.15.4 serves as the preferred link layer protocol for IPv6 addressed LoWPAN. IEEE 802.15.4 cluster based networks have various security mechanisms. Although security enabled, these security services are at the behest of the higher layers of the network. The radio environment of IEEE 802.15.4 based networks leaves the information carried in the beacon frames vulnerable to misuse for exploiting the integrity and availability of the network.

2.2. RPL

RPL is an IPv6 routing protocol for LLN designed by IETF and used as the de-facto routing protocol in Contiki for WSN [8]. It is a distance vector routing protocol which does not require much memory and is hence suitable for the resource constrained networks. This proactive routing protocol functions through the creation of a tree like topology known as directed acyclic graph (DAG). Nodes send local control messages for sharing information with neighbors, and also broadcast network wide topology information. There is one root node and multiple child and leaf nodes in a RPLDAG, along with redundant links, as shown in Figure 2. A Destination Oriented DAG (DODAG) maintains all the topology information, consisting of paths from the leaves to the roots, facilitating both upward and downward movement of traffic in the network [5]. Route establishment and traffic movement using RPL in Contiki begins with the DAG's

root node or the LLN border router (LBR) sending out DIO (DODAG Information Object) messages to inform the neighbors about the network parameters like rank, DAG-ID, Objective function, routing metric etc. This LBR node is preset by the administrator and it is assigned rank 1. Objective Function is used for steering the traffic to different paths according to the requirement, *i.e.*, it describes how RPL protocol selects the routes and optimizes them, which in ContikiRPL is based on hop count and ETX. The child nodes receiving this message calculate their rank accordingly and cost of reaching the parent node and forward this message until all the nodes present in the network join the DAG. A node which doesn't receive DIO for 5 seconds or more issues out a DIS (DODAG Information Solicitation) message to promptly receive DIO from the receiving nodes. Once all nodes have selected their parents and upward traffic topology has been created, nodes start to send out DAO (DODAG Advertisement Object) to advertise their prefix to their parents so that they update their routing table and downward traffic can be enabled [2]. Kim *et al.*, [24] carried out an extensive survey on the RPL protocol, highlighting its research concerns and suggesting future directions for its evolution.

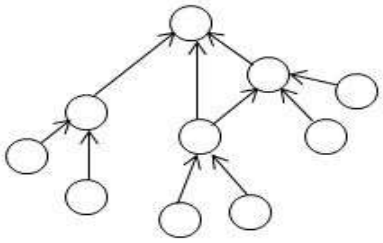

Figure 2. Sample RPL DAG Representation

2.3. Packet Drop Attack in RPL

A routing protocol's dynamicity can be used by an attacker to listen to the routing packets and that information can then be used by it to its own advantage. The attack aims at attempting to create a connection of the source node with the malicious node to enter into the original network by claiming to have path to the destination/sink node. Post this step, every packet's fate on that route is in the malicious node's hands. This malicious node can individually, or by colluding with other nodes in the network drop all the received packets that were meant to be forwarded in the route to the sink node [16]. In ContikiRPL, each node has a default upward route, consisting of all the preferred parents, leading up to the DODAG root, and so whenever a node has to forward a message towards the sink, it sends the message to the preferred parent. A malicious node forms a part of the DODAG in this process, such that when some other node selects this node as a parent in the path to reach the sink node, all the data packets that it is supposed to forward are dropped by it silently. This packet drop attack is among the gravest attacks in RPL as it may cause loss of a large part of the traffic, depletion of energy reserves because of DoS, and end-to-end packet delay issues. This attack can be more destructive when joined with other malicious nodes and can be the point of entry for a wide range of other sneaky attacks. Therefore, it can cause excessive vulnerabilities in WSNs [1]. Figure 3 shows how a malicious node accepts data packets to be routed to the root/sink node from its neighbors and drops them instead. The subsection of network on which this attack is fixated forms the blackhole region.

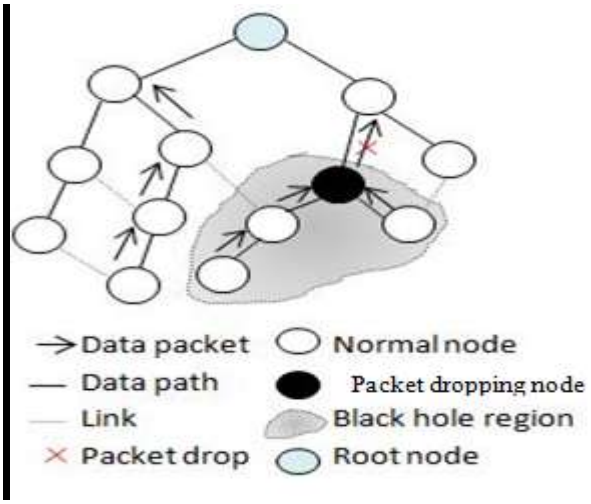

Figure 3. RPL Packet Drop Attack

The following algorithm outlines the operation of packet drop attack in ContikiRPL:

```
1.  Create N sensor nodes
2.  Select N1 as root node with rank=1
3.  RPL Route Establishment Process {
4.      N1 multicasts DIO messages consisting DAG-ID, OF, rank to its neighbors
5.      if (a node doesn't receive DIO for 5 seconds) {
6.          The node sends out DIS message
7.          Parent node to that node replies with DIO
8.          Goto Step 11
9.      }
10.     else {
11.       do {
12.          Neighboring nodes calculate their rank, cost to reach root node based on OF
13.          Neighbor node which has optimized path to root becomes a parent node and
    multicasts DIO message to its neighbors
14.       }
15.       until all nodes join the DODAG
16.     }                       //Upward traffic topology created
17.     do {
18.         for each leaf node
19.         Send DAO to its parent consisting prefix info
20.         Receiving parent node processes the prefix information and stores in its
    routing table
21.     }
22.     until prefix information reaches N1
23. }                       //Downward traffic topology is created.
24. RPL Traffic Movement {
25.   do {
26.       if (malicious node)
27.           Drop packet
28.       else
29.           Send packet to N1 by finding path through RPL route establishment process
30.   }
31.   until data packets to send
32. }
```

3. Simulation Analysis

This section discusses the simulator tool, topology and protocols of the LLN being simulated and analyzed. It explains the deployment methodology along with the various simulation parameters and performance metrics.

3.1. Contiki

Contiki is an open source OS developed above Ubuntu as base OS and Linux as kernel. This OS is developed in order to facilitate developments and simulations on IoT and WSN as discussed by Dunkels *et al.*, [7]. It connects tiny low-cost, low-power micro controllers to the Internet. It supports fully standard Ipv4 & IPv6 along with recent low power wireless standards of CoAP, RPL 6LowPan. Contiki is an event driven system, the processes in which run to completion employed as event handlers. Applications in Contiki are written in standard C and it provides not just network simulation and realizations, but all facilities of a typical Linux OS. Instant Contiki provides, in a single download, a complete environment for development- it comes in a complete package upon downloading with a virtual machine file and can be run using any virtual machine player. Using Contiki OS in comparison to other operating systems offers various advantages like implementing a sleep-controlling interface separately is not required, or using different MAC and RDC layers can enforce different radio sleep times, *etc*.

COOJA (COntiki Os Java) is the network simulator tool provided by Contiki OS. It allows all sorts of small and large networks of Contiki sensor nodes to be simulated. COOJA also allows for emulation of motes, both at the hardware and lesser detailed level, for accurate inspection of the system's behavior and for simulation of larger networks respectively. Although COOJA has been developed using Java platform, all the motes in the COOJA simulator are configured using C language codes and scripts for analysis. COOJA comes as an independent tool, preinstalled in the Contiki OS. Every time it is to be run using Contiki's command line interface, it needs to be compiled. COOJA allows the complete designing of the network, along with realization of virtual system as well as in the real world, by connecting motes in the USB ports of the system. COOJA comes preinstalled with some extensions like PowerTracker, Collect View etc. that re required to be configured as per the structures of Contiki, using the variable paths' specifications in COOJA. The simulations are stored in a .csc format and can be easily loaded from anywhere, whereas loading the individual mote programs requires a proper building of architecture.

3.2. Contiki Protocols

Figure 4 shows the four layers of the network protocol stack for Contiki, and the protocols used for the simulated WSN are shown on the right part of the figure, as explained below.

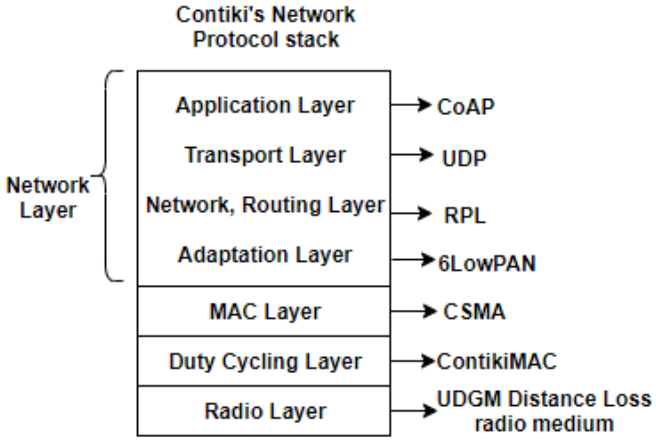

Figure 4. Protocol Stack for Contiki

UDGM Distance Loss

In COOJA, a radio medium acts as an observer of each mote's radio interface. Whenever the radio of a mote starts to transmit, the medium is notified of it. To decide that the transmitted message should be received by which all available radios in the simulation, the radio medium uses radio location of each node. Unit Disk Graph Medium (UDGM) radio propagation model is used in COOJA, which models the range of transmission ideally as a disk wherein motes lying outside the disk are not able to receive packets whereas the motes inside the disk region receive all the packets. UDGM Distance Loss is an extension of this basic model, used by default, in which interferences in transmissions are considered and the packets can be received and transmitted with a success ratio probability each. Two distance parameters are used: transmitting-range- that decides whether the nodes are within each other's transmission-range, and interference-range- that decides if there will be interference between one node's transmission and another node's reception. A sending node's packet can be received by a node which lies only within the defined transmitting-range radius of that node. Outside this range, but within the interference-range, the node can't receive the sender node's packet but will face interference by the sender node's transmission. However, outside the interference-range, the node is unaware of the sender's transmissions.

The UDGM radio model considers the antenna as omnidirectional. Inside the transmitting radius of a node, the strength of the receiver mote's signal is related to the distance from the sender mote by a factor only. This distance factor is defined as the ratio of the distance to the transmitting-range. The path loss is given in simple terms by the shown equation 1, where decibels is used to measure all the real life like observed quantities. This is the Friis equation. The real life path loss of signal strength can't be accurately described by the existing UDGM model.

$$\mathrm{Pr} = Pt + Gt + Gr - PL \tag{1}$$

where Pr is the signal power received at the receiving antenna, Pt is the signal power that the transmitting antenna delivers, Gt is the transmitting antenna's gain, Gr is the gain of the receiving antenna, and PL is the path loss in free-space [18].

ContikiMAC

Of all the components on a resource constrained wireless device, the wireless transceiver often has the highest power consumption. The low power motes mostly remain in sleep to extend their lifetime, and since at that time the transceiver is turned off and the node is unable to receive any data, it is necessary to use a mechanism of duty

cycling so as to turn on the transceiver every once in a while. ContikiMAC is the better and the default set radio duty cycling (RDC) mechanism in Contiki that makes use of periodic wake-ups for listening to any transmissions of packets from neighbors. That is, a node remains awake until the duration of successful receiving of packets when any transmission is detected during a wake-up. An acknowledgement is then sent by the receiver, until the reception of which a sender continues to repeatedly transmit its packet. In case of broadcasts, no acknowledgement is received, so the packet is sent repeatedly over the full wake-up interval to ensure its successful transmission to all neighbors. ContikiMAC therefore uses ordinary link layer packets that require no additional packet headers or signaling mechanism. Through a precise set of timing constraints, ContikiMAC offers a significantly more power-efficient wake-up mechanism than other duty cycle mechanisms, allowing the nodes to keep off their radios for most of the time while being able to relay multi-hop messages. Additionally, ContikiMAC allows quick detection of false-positive wake-ups to receivers using a fast sleep optimization, and run-time optimization of the energy-efficiency of transmissions using transmission phase-lock optimizations [6].

3.3. Methodology

Sky mote nodes have been arranged on a plane square and are considered as stationary, such that every node has a communication range of 100m and an interference range of 120m. The topology is constructed in a manner that each node has communication (multihop) with the sink, considering a single sink in the simulation. The sink receives data packets periodically from each node. The nodes are randomly distributed in a 10m x 10m area, following the Poisson probabilistic distribution of traffic, as supported by Contiki's random generator, assuming a real-time traffic flow from the nodes in the network. A number of malicious packet dropping nodes may exist in the network, and they initiate their malicious behavior after the initial graph is established. The duration for which simulation for each scenario is run is around 620 seconds, repeated five times, and each metric's average value is presented to account for the random nature of the protocols. The simulation parameters used and their values in Contiki's COOJA network simulator are displayed in Table 1.

To evaluate the performance of the network under standard RPL and RPL under packet drop attack, the performance metrics employed are received packet count, average power consumption, ETX and hop count.

• Energy Consumption: This allows the calculation of the total time that is spent by each mote in the various states of transmission and reception, listening, low power mode and CPU processing, as presented in equation 2.

$$Total\ Energy\ Consumed = \sum cp + lp + lt + lr \quad (2)$$

Where, CPU energy, cp = c*1.8/tm
Low power mode energy, lp = l*0.0545/tm
Transmission energy, lt = t*17.7/tm
Listening energy, lr = r*20/tm
and tm = c+l

total time is shown by tm, the time for which the mote used the CPU is denoted by c, l is the time for which the mote is in the low power mode (LPM), t represents the time for which mote is transmitting while r denotes the time for which mote is listening.

• Received Packet Count: This refers to the number of data packets successfully received at each mote that forms part of the RPLDAG. This count is helpful in

determining the impact of presence of malicious blackhole mote(s) which drops the packets and reduces the successful transmissions in the network.

• Expected Transmission Count: A probabilistic measure for path quality among nodes in a wireless packet data network. ETX for a link in the network refers to the expected number of transmissions that are needed for sending over a packet on that link, as shown in equation 3. The ETX of a network path is the summation of the ETX of all the network links along that path, as shown in equation 4.

$$ETX(link) = 1/(df \times dr) \quad (3)$$

$$ETX(path) = \sum ETX(link) \quad (4)$$

Where df is the measured probability that a transmitted packet is successfully received by the neighbor and dr is the measured probability that the acknowledgment packet is successfully received.

• Hop Count: This refers to the number of intermediary nodes through which data passes between the sending and receiving nodes. In a network, it is basically a measure of distance, establishing how long a path a sender mote needs to take for transmitting its packets to the sink mote.

Table 1. Simulation Parameters

Parameter	Value
Radio medium model	UDGM Distance Loss
Range of nodes	Rx and Tx: 100m, Interference: 120 m
Mote type	Sky Mote
Duty Cycle	ContikiMAC
No. of motes	15 to 25
No. of sinks	1
Simulation area	10 x 10m
Physical layer	IEEE 802.15.4
MAC layer	ContikiMAC, IPv6
Routing layer	ContikiRPL
Transport layer	UDP
Objective function	Hop count and ETX
Simulation Time	10 min

As shown in Figure 5, Node 4 acts maliciously to perform packet drop attack in the existing network of sensor nodes by discarding the packets routed to it.

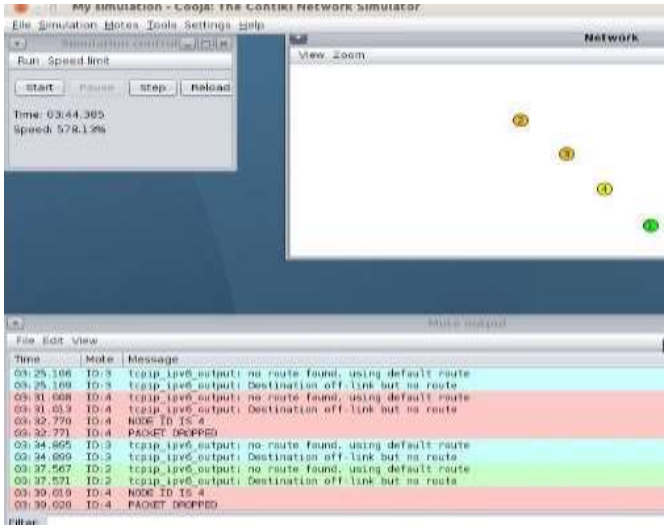

Figure 5. Sample Simulation of RPL Packet Drop Attack in COOJA

Taking a network of 25 motes, 20 motes and 15 motes, in each of which one mote is a udp-sink and the rest udp-senders, malicious packet dropping motes-1, 2, 3, 5 and 8, were introduced, and on running the simulation for a duration of over 10 minutes, the performance metrics of the network were observed to get the results.

3.4. Results and Analysis

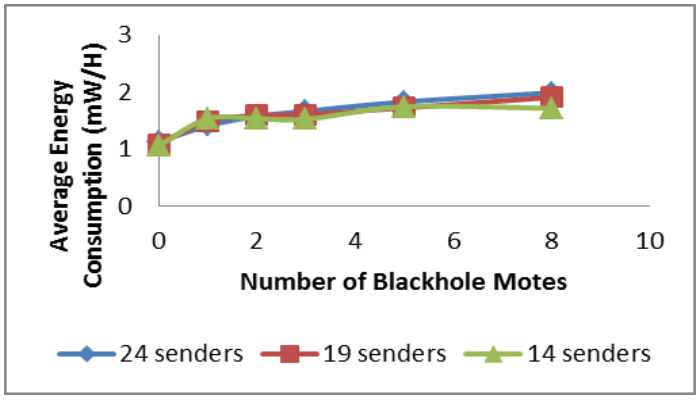

Figure 6. Effect of Increasing Malicious Motes on the Average Energy Consumption (in mW/H) over a WSN with varying Number of Senders

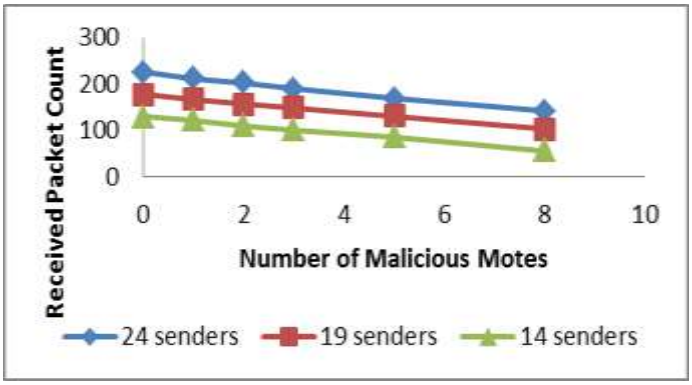

Figure 7. Effect of Increasing Malicious Motes on the Received Packet Count over a WSN with varying Number of Senders

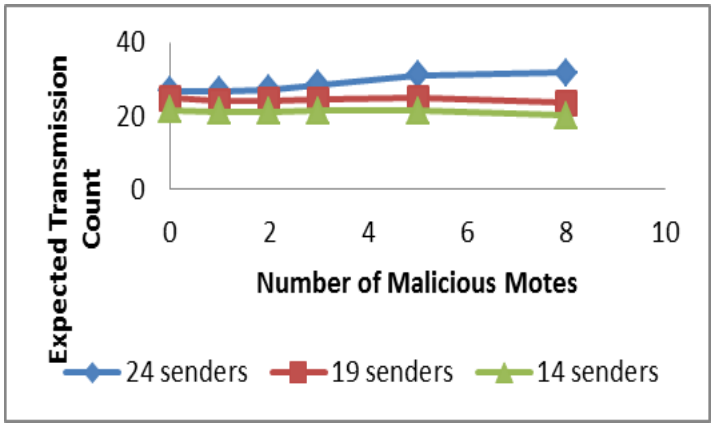

Figure 8. Effect of Increasing Malicious Motes on the Expected Transmission Count over a WSN with varying Number of Senders

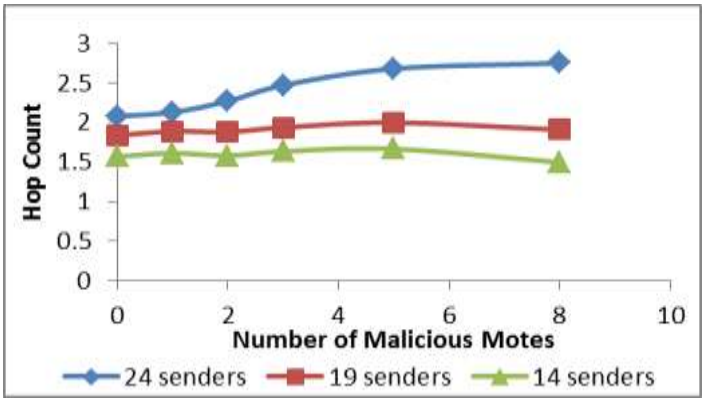

Figure 9. Effect of Increasing Malicious Motes on the Hop Count over a WSN with varying Number of Senders

Figure 6 shows that with the increase in the number of packet dropping motes in the network, the energy consumed, which is the average of energy involved in transmission, reception and processing activities, progressively rises. Considering a network with 15 motes with 1 sink and rest motes acting as senders, the total energy when there is no node acting maliciously is 1.1mW/H, close to the values when total motes are 20 and 25 with 1 sink mote and remaining senders each. But with the inclusion of a single node dropping packets, this value rises to 1.5mW/H and continues to gradually rise as more malicious nodes join in. This shows that as the route with malicious node starts dropping packets, the sending motes require to send out more packets for successful transmission to the sink, through alternate routes. Since energy is a crucial resource in sensor motes, this increased consumption of energy due to packet drop attack poses a negative impact on the lifetime of such a network.

Figure 7 shows that the count of packets received continuously falls as the number of malicious motes are increased, leading to more routes in the network where packets are dropped. This is an important indicator of how the RPL packet drop attack impacts the performance of a WSN. The successful transmission of packets declines almost linearly in case of successively rising packet dropping malicious motes in a network consisting of 20 motes. A similar decline in total received packet count is observed for 15 and 25 motes' network too. This shows that the malicious behavior of motes is able to successfully drop packets received on its route.

Figure 8 shows the expected transmission count metric variation with the count of malicious nodes in the network. The 25 mote network rightly indicates the packet drop

attack's impact on the path quality. The probabilistic number of transmissions required over a route for successful transmission rises due to the malicious node affected routes to the sink dropping packets in the network.

Figure 9 shows how the hop count changes in the network as more and more packet dropping nodes are introduced. The hop count effectively tells the number of intermediaries in the route to the sink, the count of which changes as alternate routes are selected for transmission by the sender. As depicted by the simulated network with 25 motes, introduction of malicious motes forces the nodes to choose a longer route to the sink with more intermediate nodes for forwarding its packets successfully. Therefore, the hop count rises. The count although remains invariably the same for the network with lesser motes.

Based on the observations, it is safe to say that the effect that packet drop attack has on WSN is severe, with time and as the network grows. It critically impacts the successfully received packet count and hence the quality of the path, and is responsible for effectively reducing the overall lifetime of the network by increasing the requirement of already constrained power resource of motes.

4. Security Mechanisms

This section highlights the various security measures against attacks on LLNs and the different approaches for countering packet drop attack in RPL have been presented, analyzes them for their advantages and limitations for the simulated WSN in this work.

The packets to be successfully delivered at the base station is imperative in WSN in relation to focusing on capturing of data by some adversary. Using an effective algorithm for data encryption such as AES (Advanced encryption standard) and using techniques for data anonymity can render the information captured by the adversaries as insignificant. Consequently, the basic important objective remains packet delivery to the base stations in the presence of packet dropping malicious nodes.

In [23], the impact of blackhole DoS attack on a cluster based network is witnessed using ns2 simulations. The Leach (low energy adaptive clustering hierarchy) protocol is modified to incorporate the attack. It was observed that the attack led to fall in the packets received at the base station However, the energy consumed reduced as the malicious node did not forward any packets. This increased the network's overall lifetime as well.

Jinwala *et al.*, [9] implemented encryption algorithms of AES and XXTEA for Mica2 as security mechanism for WSN. These algorithms were included into TinySec and performance was compared to the default Skipjack, TinySec cipher. Avrora simulator provides consumed energy, CPU cycles and throughput. Based on experiments performed using this simulator, it was concluded that XXTEA (Corrected Tiny encryption algorithm) with an OCB (Offset Codebook) mode of operation is the ideal arrangement for security of WSNs. Lee *et al.*, [13] further performed studies on a wide array of block ciphers and operation modes. In place of simulations, the experiments were carried out on actual sensor platforms and the results showed XXTEA and Skipjack having good performance in reference to energy consumption and memory usage, however, RC5 (Rivest Cipher) and AES offer a higher security level than XXTEA and Skipjack but have higher resource requirements, heavily dependent on the size of the key and the number of rounds. It was further observed that the block-cipher-based MACs (message authentication codes) require very less memory in comparison to hash-based MACs, which consume lesser energy due to a computation time that is lesser than that of block-cipher based MACs.

Wazid *et al.*, [21] proposed a cluster based technique for detection and prevention of blackhole attack. When a cluster of sensor nodes is created, a coordinator for the cluster is elected based upon fairness and efficiency, and all sensor nodes are in its supervision. It sends out Authentication packets, and on receiving Reply Packets from intermediate nodes, assigns them IDs and maintains a table. The routing intermediate nodes when reply with a Reply Packet but fail to forward the sensed data packets periodically, these are

detected by the coordinator as blackhole nodes and their id is identified to be removed from the cluster set and inform previous nodes through beacons. This mechanism for detecting and preventing blackhole attack, as shown through simulations in Ns2, resolves the affected throughput and end to end delay performance of the network. However, this work was limited to a cluster based WSN topology.

To mitigate the effect of black hole attack on RPL, Ahmed and Ko [1] used two progressive processes of local decision and global verification neighbors. In the former process, based on the collected information about the communication behavior of a node's neighbors, it is identified as whether a suspicious node or not. The latter process is instigated conditionally and the verification messages are forwarded through an alternate path in order to validate the suspicious node. This approach did not take into account rank-related issue but anyhow increased the data delivery rate and reduced end to end delivery. However, the black hole nodes were able to be identified more effectively and reliably. Karakehayov [11] proposed a mechanism REWARD (receive, watch, redirect) which is based on power control performed by a transmitting node to multiple nodes in the direction of the base station such that if a sensor node on the route doesn't forward packets, the forwarding route's next hop neighbor will detect this event and report that node as a black hole. This technique is appropriate for the nodes in the network which can adjust their power of transmission as the packets are routed according to geographic routing. Identification of malicious nodes is done with the help of MISS (material for intersection of suspicious sets) broadcast messages and the detected black hole attack's location is identified through another broadcast message SAMBA (suspicious area, mark a black-hole attack). Although a balance between lifetime performance and security capability can be struck using this scheme, for a network consisting n blackhole nodes, this scheme would require O(n) extra messages for each original message, hence proving to be very expensive.

Yu *et al.*, [25] provide a detailed review of the various methodologies of trust schemes for secure routing that can resist blackhole attacks by using the rules of trust ranking for eliminating the distrustful nodes. However, these are less suitable in WSN since the complexity of such schemes is high, which takes up resources, and with the complexity involved in the structure of trust system, it also needs varied roles for meeting the trust evaluation approaches' flexibility.

Misra *et al.*, [17] and Shu *et al.*, [19] proposed solutions that used the placement of multiple base stations and developing mechanisms that generated randomized multipath routes. This scheme ensured high success of packet delivery by improving the probability of sensor nodes' packets reaching to the networks' one root node/base station at least. Under this design, through the arrangement of multiple base stations, huge volumes of different kinds of data can be achieved, and the routes taken by these packets change with the course of time. So even if the attacker gets to know the routing algorithm, the routes that are traversed by each packet can still not be pinpointed. Also, extremely dispersive and energy proficient routes are generated, which makes them fairly capable of dodging black holes, and the use of multiple base stations, as examined through simulations, effectively improves data delivery in presence of blackhole attack.

Lou and Kwon [14] proposed a hybrid multipath scheme (H-SPREAD) that aims at improving the reliability and security in a potentially hostile and erratic WSN. The end-to-end delivery of data was enhanced using the mechanism of end-to-end multipath data dispersion, in combination with secret sharing. This ensured that in the face of adversarial nodes, even if a few paths are compromised, it will not lead to the data message being compromised. In the existence of unreliable sensor nodes or/and wireless links, the reliability of transmission of each packet is significantly improved through availability of the alternate path routing scheme at each sensor node.

Casado and Tsigas [3] presented ContikiSec, a configurable secure network layer designed and introduced in Contiki's architecture for providing security in three modes of confidentiality, integrity and authentication.

Vidhya and Sasilatha [20] introduced external batteries to increase the lifetime of sensor network and via public key encryption using Message Digest (MD5) algorithm, identified black hole attack in routing. Identity of each node is maintained by a trust manager and if a source node doesn't continuously receive any replies, that node is verified by employing the secure algorithm of MD5, and on identifying which node is making use of another node's signature, it is marked as malicious and the security design initiates the data packets' alternate routing to sink for allowing data transmission.

Use of cryptographic hashes as a solution to blackhole attack was implemented in medical based WSN by Mathur *et al.*, [15]. The nodes collectively pick a cluster head (CH) to transmit all their data to. This CH then aggregates the encrypted data and transmits it further to the nearest AP (access point). The AP then, using mesh routing's reformed version, routes the data to the BS (base station). A pre-deployment phase, wherein pseudorandom numbers generated by Contiki are assigned by the BS to the APs, followed by a routing phase where the senders of request and reply packets are reversed and a hash using SHA2 algorithm is included in the request packet to avoid duplication provide security from blackhole attack. The defense mechanism used provides an appropriate way for dealing with both the single and collaborative attacks in medical WSNs.

In [12], a lightweight one-way cryptographic hash algorithm (LOCHA) is proposed as a security mechanism in WSN. It produces a short fixed length digest of 96 bits by applying low weight operations such as modulus, swap. It has been theoretically proved to be lightweight in terms of communication, computation overhead, storage and more energy efficient than MD5 and SHA-1 cryptographic functions. This way, it proves to be suitable for energy starved sensor motes and can be used as a node-authentication and message-authentication scheme to prevent node capturing and malicious activities in the WSN.

The studied countermeasures for the disruptive effect of packet drop attack can be broadly recognized as:

• Authentication- as traditionally practiced in wired networks, data and nodes of a network can be authenticated using public-key cryptography and message authentication codes to avoid unauthorized activity [9] [10] [13]. This can be achieved in ContikiRPL by enabling AES encryption along with MAC or signature coding. This is a complex computation intensive task wherein preinstalled keys are used so that only authenticated nodes can join the network and for exchanging secure data.

• Monitoring- each node can monitor its neighboring nodes and links to ensure that proper routing behavior is observed [1] [11] [21]. A few parent nodes can also collect trust ranking from all the nodes to identify valid nodes/links [25]. Supporting this in ContikiRPL affects the sleep cycle and the energy of the motes, which takes a toll on the battery life of the motes.

• Redundancy- sending multiple copies of same packet along all alternate routes or have multiple sink nodes for collection of data, to be able to bypass any malign link/node of network [17] [19] [14]. Providing this in ContikiRPL improves the successful transmissions against packet dropping blackholes, but consumes up extra energy from the motes in carrying out multiple transmissions.

• Architectural adaptations- a separate additional configurable layer can be added in the network's protocol stack or existing protocols be modified for inclusion of schemes to maintain various aspects of security, example: ContikiSec [3].

• Cryptographic Hashing- confidentiality, integrity, authenticity against attacks in network can be better provided through cryptographic hash functions like SHA1, MD5 [20] [15]. However, inclusion of these algorithms is highly complex and computation intensive to be suitable for WSN. Lightweight versions can be incorporated in ContikiRPL [12].

Table 2 highlights the security mechanisms suitable for the simulated WSN, based on the simulation results.

Table 2. Security Mechanisms for Simulated WSN

Security Mechanism	Advantages	Limitations
▪ ContikiSec layer	➢ Complete and configurable solution providing three security modes of integrity, confidentiality, and authentication.	➢ High energy consumption.
Cryptographic Hashing ▪ MD5 ▪ SHA2 ▪ Lightweight one-way hash function	➢ Shorter computation time than encryption algorithms i.e. consume lesser energy. ➢ Deal with both single and collaborative attacks. ➢ Lightweight solution suitable for energy constrained motes.	➢ Require external batteries to increase lifetime of network motes. ➢ Computation intensive.

5. Conclusion and Future Work

The impact of RPL packet drop attack, that is responsible for dropping packets in the route to the sink, is observed in LLN. Through simulations of varying number of motes in Contiki, performance metrics of received packet count, total power consumption, ETX and hop count were noted to be able to conclude that the packet drop attack has a detrimental effect on the successful transmissions and path quality, which continues to

rise as the network grows and time lapses. This effect can however be countered using a number of security measures. The studied mechanisms range from multiple path routing, node monitoring, trust based scheme, encryption algorithms to proposed cryptographic hash based security methods. Though, some limitations were posed by these methods, such as high computational complexity, need for addressing rank related issue, inclusion of external battery, need of more memory, or topology limitations. The hash based cryptographic measure is considered to be a good countermeasure against packet drop attack for RPL in LLN. There is, however, vast scope for developing more resource efficient algorithms that ensure all security standards in WSN.

References

[1] F. Ahmed and Y. B. Ko, "Mitigation of black hole attacks in Routing Protocol for Low Power and Lossy Networks", Security and Communication Networks, vol. 9, no. 18, **(2016)**, pp. 5143-5154.
[2] H. Ali, "A performance evaluation of rpl in contiki: A cooja simulation based study", School of Computing, Blekinge Institute of Technology, Sweden, **(2012)**.
[3] L. Casado and P. Tsigas, "Contikisec: A secure network layer for wireless sensor networks under the contiki operating system", in Nordic Conference on Secure IT Systems, Springer, Berlin, Heidelberg, **(2009)**, pp. 133-147.
[4] K. Chelli, "Security Issues in Wireless Sensor Networks: Attacks and Countermeasures", Proceedings of the World Congress on Engineering, vol. 1, **(2015)**, pp. 1-3.
[5] K. Chugh, L. Aboubaker and J. Loo, "Case study of a black hole attack on LoWPAN-RPL", Proceedings of the 6th International Conference on Emerging Security Information, Systems and Technologies (SECURWARE), Rome, Italy, **(2012)**, pp. 157-162.
[6] A. Dunkels, "The contikimac radio duty cycling protocol", **(2011)**.
[7] A. Dunkels, B. Gronvall and T. Voigt, "Contiki-a lightweight and flexible operating system for tiny networked sensors", 29th Annual IEEE International Conference on Local Computer Networks, **(2004)**, pp. 455-462.
[8] T. Winter, "RPL: IPv6 routing protocol for low-power and lossy networks", RFC 6550, IETF document, **(2012)**.
[9] D. Jinwala, D. Patel and K. Dasgupta, "Optimizing the block cipher and modes of operations overhead at the link layer security framework in the wireless sensor networks", in International Conference on Information Systems Security, Springer, Berlin, Heidelberg, **(2008)**, pp. 258-272.
[10] S. Kalyoncu, "Wireless Solutions and Authentication Mechanisms for Contiki Based Internet of Things Networks", **(2013)**.
[11] Z. Karakehayov, "Using REWARD to detect team black-hole attacks in wireless sensor networks", Wksp. Real-World Wireless Sensor Networks, **(2005)**, pp. 20-21.
[12] A. R. Chowdhury, T. Chatterjee and S. DasBit, "LOCHA: A light-weight one-way cryptographic hash algorithm for wireless sensor network", Procedia Computer Science, vol. 32, **(2014)**, pp. 497-504.
[13] J. Lee, K. Kapitanova and S. H. Son, "The price of security in wireless sensor networks", Computer Networks, vol. 54, no. 17, **(2010)**, pp. 2967-2978.
[14] W. Lou and Y. Kwon, "H-SPREAD: a hybrid multipath scheme for secure and reliable data collection in wireless sensor networks", IEEE Transactions on Vehicular Technology, vol. 55, no. 4, **(2006)**, pp. 1320-1330.
[15] A. Mathur, T. Newe and M. Rao, "Defence against black hole and selective forwarding attacks for medical WSNs in the IoT", Sensors, vol. 16, no. 1, **(2016)**, pp. 118.
[16] B. K. Mishra, M. C. Nikam and P. Lakkadwala, "Security against black hole attack in wireless sensor network-a review", 4th International Conference on Communication Systems and Network Technologies (CSNT), IEEE, **(2014)**, pp. 615-620.
[17] S. Misra, K. Bhattarai and G. Xue, "BAMBi: Blackhole attacks mitigation with multiple base stations in wireless sensor networks", IEEE International Conference on Communications (ICC), **(2011)**, pp. 1-5.
[18] V. Rege, "Design and Implementation of an Antenna Model for the Cooja simulator", arXiv preprint arXiv:1610.06129, **(2015)**.
[19] T. Shu, M. Krunz and S. Liu, "Secure data collection in wireless sensor networks using randomized dispersive routes", IEEE transactions on mobile computing, vol. 9, no. 7, **(2010)**, pp. 941-954.
[20] S. Vidhya and T. Sasilatha, "Performance analysis of black hole attack detection scheme using MD5 algorithm in WSN", IEEE International Conference on Smart Structures and Systems (ICSSS), **(2014)**, pp. 51-54.
[21] M. Wazid, A. Katal, R. S. Sachan, R. H., Goudar and D. P. Singh, "Detection and prevention mechanism for blackhole attack in wireless sensor network", International Conference on Communications and Signal Processing (ICCSP), **(2013)**, pp. 576-581.

[22] K. Zen, D. Habibi, A. Rassau and I. Ahmad, "Performance evaluation of IEEE 802.15. 4 for mobile sensor networks", 5th IFIP International Conference on Wireless and Optical Communications Networks (WOCN'08), IEEE, **(2008)**, pp. 1-5.
[23] M. Tripathi, M. S. Gaur and V. Laxmi, "Comparing the impact of black hole and gray hole attack on LEACH in WSN", Procedia Computer Science, vol. 19, **(2013)**, pp. 1101-1107.
[24] H. S. Kim, J. Ko, D. E. Culler and J. Paek, "Challenging the IPv6 Routing Protocol for Low-Power and Lossy Networks (RPL): A Survey", IEEE Communications Surveys & Tutorials, vol. 19, no. 4, **(2017)**.
[25] Y. Yu, K. Li, W. Zhou and P. Li, "Trust mechanisms in wireless sensor networks: Attack analysis and countermeasures", Journal of network and computer applications, vol. 35, no. 3, **(2012)**, pp. 867-880.

Authors

Ms. Nikita Malik, completed her Masters in Technology (Information Security) from Ambedkar Institute of Advanced Communication Technologies and Research, GGSIP University, Delhi, India (Gold Medallist). She is currently pursuing Ph.D. from University School of Information, Communication and Technology, GGSIP University. She has published few research papers in IEEE/Springer international conferences/journals of repute. Her main research interest focuses on Wireless Sensor Networks, Mobile Ad hoc Networks and Network Security.

Mr. Prakash Rao Ragiri, completed his M. Tech in Computer Science and is currently working as an Assistant Professor in Ambedkar Institute of Advanced Communication Technologies and Research, GGSIP University. He has more than 10 years of teaching experience and 2 years of industry experience. His areas of research interest are Computer Networks, MANETs and Computer Forensics. He has guided over 25 B. Tech and M. Tech projects and has several research papers in international and national conferences and journals of repute.

Dr. Aarti Jain, completed her Ph.D. in the area of Networks from GGSIP University, Delhi in 2009. She is currently working as an Assistant Professor in Ambedkar Institute of Advanced Communication Technologies and Research, GGSIP University. She has more than 12 years of teaching experience and has guided over 35 B. Tech and M. Tech projects. Her areas of research interest are Wireless sensor networks, fuzzy logistics, and bio-inspired optimization. She has several research papers in international and national conferences and journals of repute.

