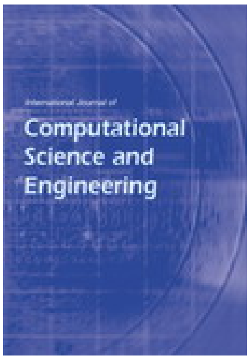


International Journal of Computational Science and Engineering

ISSN online: 1742-7193 - ISSN print: 1742-7185
https://www.inderscience.com/ijcse

Robust link-assessment-based approach for detection and isolation of blackhole attacker in resource constraint internet of things

Himanshu B. Patel, Devesh C. Jinwala

DOI: 10.1504/IJCSE.2024.10063354

Article History:

Received:	17 July 2023
Last revised:	08 December 2023
Accepted:	31 January 2024
Published online:	21 December 2024

Robust link-assessment-based approach for detection and isolation of blackhole attacker in resource constraint internet of things

Himanshu B. Patel* and Devesh C. Jinwala

Department of Computer Science and Engineering,
SVNIT-Surat,
Surat, Gujarat, India
Email: hims247@gmail.com
Email: dcj@svnit.ac.in
*Corresponding author

Abstract: Blackhole is one of the crucial packet-dropping attacks that can be launched on routing protocol for low-power lossy networks (RPL) protocol. In this paper, we propose an improved specification-based approach for *integrating trust* value in specification-based approach to detect and isolate blackhole attackers, based on a *tangible value* of packet-forwarding behaviour of the nodes in the network. To our knowledge, this is the first attempt to integrate packet-forwarding trust with the specification-based approach. In our proposed approach, lightweight-specification data are maintained at each device and shared periodically with the resource-rich edge device. Resource-insensitive computations are carried out at the edge device. The proposed approach uses a robust data collaboration mechanism that ensures detection-data delivery between nodes and edge devices, even in the presence of 10% of attacker nodes. Our simulations on Cooja simulator show that in an environment with 20% data loss, the proposed approach yields more than 80% true-positive rate.

Keywords: internet of things; IoT; routing protocol for low-power lossy networks; RPL; blackhole attack; trust.

Reference to this paper should be made as follows: Patel, H.B. and Jinwala, D.C. (2025) ‘Robust link-assessment-based approach for detection and isolation of blackhole attacker in resource constraint internet of things’, *Int. J. Computational Science and Engineering*, Vol. 28, No. 1, pp.100–113.

Biographical notes: Himanshu B. Patel received his PhD in Computer Engineering at Sardar Vallabhbhai National Institute of Technology-Surat. He is an Assistant Professor at the School of Information Technology, Artificial Intelligence and Cyber Security, Rashtriya Raksha University, Gandhinagar, Gujarat, India. His research interests include security and privacy issues in the internet of things, blockchain and security issues related to IP communication over resource constraint networks.

Devesh C. Jinwala is a Professor (HAG) at the Department of Computer Science and Engineering (DoCSE), Sardar Vallabhbhai National Institute of Technology and an Adjunct Professor in the DoCSE at the Indian Institute of Technology Jammu (IIT Jammu), India. In the past, he has also served as a Professor and Department Chair of the DoCSE, IIT Jammu. In the past, he also served as a Visiting Professor at the Daniel Felix Ritchie School of Computer Science and Engineering, University of Denver, USA. His research interests lie in the security and privacy issues in resource-constrained environments, machine learning applications in security, software security, and software engineering.

1 Introduction

The recent advancements in wireless communication and embedded system technologies have provided seamless communication between embedded devices. The network formed by such devices has enabled the real-world deployment of the internet of things (IoT). The IoT has eased the prediction and real-time management of different use-cases in modern-day medical, agriculture, military and transport systems (Yasser et al., 2020; Atzori et al., 2010). Internet Engineering Task Force (IETF) has defined the IPv6 over low-power wireless personal area network (6LoWPAN) standard, to enable internet protocol version 6 (IPv6) communicate over resource-constraint wireless personal area network devices (Hui et al., 2011).

Figure 1 6LoWPAN-based internet of things architecture (see online version for colours)

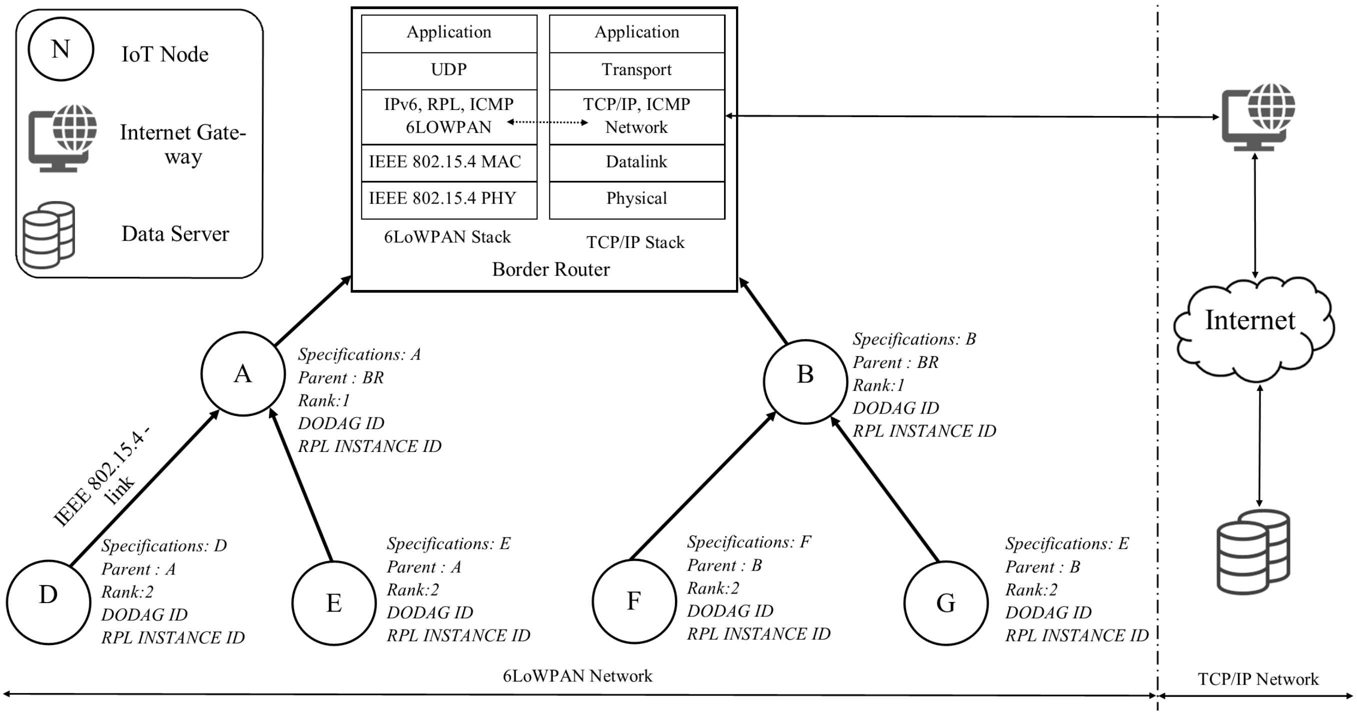


Figure 2 Taxonomy of blackhole mitigation approaches

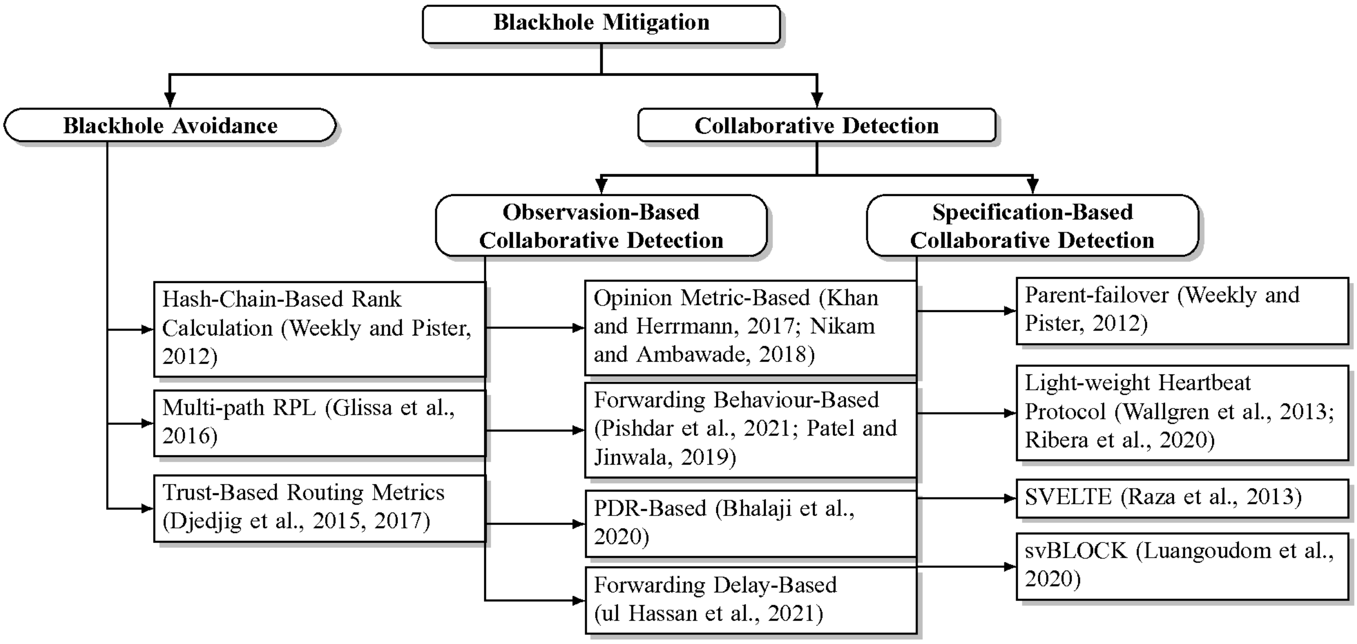

Blackhole Mitigation
Blackhole Avoidance
Collaborative Detection
Observasion-Based Collaborative Detection
Specification-Based Collaborative Detection
Hash-Chain-Based Rank Calculation (Weekly and Pister, 2012)
Multi-path RPL (Glissa et al., 2016)
Trust-Based Routing Metrics (Djedjig et al., 2015, 2017)
Opinion Metric-Based (Khan and Herrmann, 2017; Nikam and Ambawade, 2018)
Forwarding Behaviour-Based (Pishdar et al., 2021; Patel and Jinwala, 2019)
PDR-Based (Bhalaji et al., 2020)
Forwarding Delay-Based (ul Hassan et al., 2021)
Parent-failover (Weekly and Pister, 2012)
Light-weight Heartbeat Protocol (Wallgren et al., 2013; Ribera et al., 2020)
SVELTE (Raza et al., 2013)
svBLOCK (Luangoudom et al., 2020)

Figure 1 shows a typical 6LoWPAN-based IoT architecture consisting of IoT nodes and a border router (BR). An IoT node is a device capable of sensing computation and communication with limited computational power, storage, energy, and bandwidth. In contrast, BR is a comparatively resource-rich device having two communication stacks, viz., an IEEE 802.15.4 physical layer-based 6LoWPAN communication stack to communicate with sensing nodes and a TCP/IP communication stack to communicate with the internet (da Silva et al., 2021). In 6LoWPAN network, nodes are generally deployed in a large number with a common goal, in typical applications like military surveillance, environmental, medical and critical systems monitoring, smart-home, smart-grid and agriculture automation (Atzori et al., 2010; Lokhande and Patil, 2022; Niranjan et al., 2021; Lu et al., 2023; Chowdhury, 2022; Silva et al., 2022).

The routing protocol for low power and lossy network (RPL) is used as the *de-facto* standard for route management at the network layer in 6LoWPAN protocol stack. As compared to, mesh topology used in low power lossy network (LLN), RPL forms a destination oriented directed acyclic graph (DODAG) topology rooted at the BR. Regardless of their actual destination all the packets are forwarded by each nodes to its parent with BR node as the target. That is, nodes that are not in the range of BR forward a packet via their respective parent nodes to the BR, subsequently the packets are forwarded to their actual destination by BR. To find a route to the actual destination of incoming packets, a separate routing table containing a list of all links in the network is maintained at the BR. The parent selection process is optimised-based on routing metrics, viz., *hop-count, energy, link-quality* (Vasseur et al., 2012). An objective function is defined at each node to convert a routing metric value to the rank value. The rank of a node logically represents the node's relative distance from BR. It can also be seen from Figure 1, that rank value strictly increases as we move away from the BR. To optimise the routing process, the parent node is selected based on the lowest rank value (Winter et al., 2012).

Routing security was not considered as a primary concern while designing RPL (Winter et al., 2012). Hence the RPL is susceptible to many service-oriented attacks (Janani and Ramamoorthy, 2022; Verma and Bhardwaj, 2021). In the RPL a parent node is selected based on rank and routing metric values. A blackhole attacker manipulates those values to gain better position and control a large sub-tree in the DODAG. The literature also shows that by manipulating the rank value, an attacker can increase its chances of getting selected as a parent node by 30% compared to its sibling nodes (Patel and Jinwala, 2019). Once the attacker gains control over large sub-tree in the DODAG, it can drop the packets from all of its child nodes.

Blackhole mitigation approaches are mainly classified into two main categories, blackhole avoidance and blackhole detection. Blackhole avoidance approaches mainly restrict rank manipulation. Cryptographic hash-chain (Weekly and Pister, 2012) is used to restrict an attacker node to decrease a rank value by one only. As compared, in an alternative trust value-based approach a tangible value of packet-forwarding is used as a metric, to select the parent node with higher packet-forwarding trust value (Djedjig et al., 2015, 2017). The use of cryptographic hash and incorporating trust value for parent selection causes latency in route setup and requires additional hardware to perform complex computations. One of the ways to maintain packet delivery in the presence of the attacker is to drop optimised route formation and create multiple routes within the network (Glissa et al., 2016).

Due to the limited communication range of involved devices, a comprehensive view of the whole network, at a single node is infeasible to achieve in 6LoWPAN. Hence, collaboration-based approaches are used as alternative to detect a blackhole attack (Patel et al., 2016; Shi et al., 2023; Gebremariam et al., 2023). Based on their underlying mechanism, collaborative blackhole detection approaches are further classified as *observation-based collaborative approaches* and *specification-based collaborative approaches*. *Observation-based approaches* set all or partial nodes in *promiscuous mode* to dynamically observe their surrounding nodes' behaviour. Nodes running in promiscuous mode monitor all the neighbouring nodes for a specific behaviour, like packet-forwarding (Khan and Herrmann, 2017; Nikam and Ambawade, 2018; Patel and Jinwala, 2019; Pishdar et al., 2021), packet delivery ratio (Bhalaji et al., 2020), and forwarding delay (ul Hassan et al., 2021). The observed data from all the nodes are then processed by the BR node to calculate the individual node's trust value. Detection accuracy in the observation-based approaches is achieved by observing a single node by multiple surrounding nodes. Accuracy here is achieved by additional communication overhead. To assist routing and self-healing processes, RPL maintains some specification data at all the nodes in the network (Figure 1). From the literature it is observed that inconsistency in such data indicates the presence of an attacker in the network (Raza et al., 2013). The continuous communication-based approach shown in the literature puts compulsion on all nodes in the network to send either control or data packets at predefined time intervals to verify their liveliness in the network (Weekly and Pister, 2012; Wallgren et al., 2013; Ribera et al., 2020). Neighbour table information shared by individual node assists BR in finding rank value inconsistency imposed by a blackhole attacker (Raza et al., 2013; Luangoudom et al., 2020).

Due to the packet dropping nature of an attacker, packet-forwarding behaviour is the most suitable metric for blackhole attacker detection. From the literature we observe that observation-based approaches verify packet-forwarding behaviour by setting all the nodes in the promiscuous mode. Collaboration itself is a resource-intensive process. In observation-based approaches, promiscuous mode of operation burdens a node with extra computational overhead. A single node's trust value is obtained by aggregating the observation from its neighbouring nodes. Thereby accuracy of trust value is achieved at the cost of communication overhead. In contrast, specification-based collaborative approaches cause lesser communication overhead as nodes are communicating either specification data or control packets to the BR. The comparison is shown in Table 1.

Specification-based collaborative approaches do not verify the packet-forwarding behaviour of all the nodes. Instead, they emphasise which node is trying to manipulate the routing metric to gain a better position in the 6LoWPAN. Rank manipulation does not guarantee an attacker's presence, and an attacker with the knowledge of the surrounding node's routing metric value can bypass the detection mechanism. Apart from that, in the specification-based approaches, single node's claim has a comparatively higher impact on the final decision. In an environment like IoT, the accuracy of such approaches cannot be guaranteed.

This paper proposes an improved specification-based approach, *integrating trust* value in specification-based approach to detect and isolate blackhole attackers, based on a *tangible value* of packet-forwarding behaviour of the nodes in the network. A fixed-length specification data structure is designed to hold the numbers of packets received and forwarded at each node in the network. The specification data is then shared with BR, periodically to calculate trust values for nodes in the network. The trust value of a single node depends on specification data shared by itself, its parent, and all the child nodes. Hence, no single node can overpower the trust calculation mechanism by sharing false data. To the best of our knowledge this is the first attempt to integrate packet-forwarding trust with the specification-based approaches.

Table 1 Comparison between observation and specification-based blackhole detection approaches

Observation-based approaches	*Specification-based approaches*
Set nodes in promiscuous mode	No promiscuous mode operation is required
Overhear and process all the communication between neighbouring nodes	Share specification data or verify liveliness by high data rate
Verify packet forwarding behaviour of the nodes	Detect anomalies in specification data

The main contributions proposed approach are as follows:

a *Low memory and less computation* are required to hold and maintain lightweight specification data containing numbers of packets sent and received by a node with their destination and source nodes. Section 6.1 shows further analysis on memory efficiency of the proposed approach.

b *Robustness* in the presence of attackers is achieved by broadcasting specification data towards BR. Section 6.3 further discuss the energy efficiency of the broadcast mechanism. BR node collects specification data from all nodes and processes them to calculate packet forwarding trust value of individual node in the network.

c *Assembled trust value* for single node is calculated at the BR, by aggregating individual claims of that node with its parent and child node's claims. A node is sending partial information about how many packets it has received from and sent to, child and parent nodes respectively. That information from the different nodes are then combined by the BR to calculate individual node's trust value. Trust value calculation mechanism employed is so efficient that no single node cannot overpower the detection process. Sections 4 and 6.5 present further description and analysis of trust value computation.

The proposed approach is simulated using Cooja simulator with Contiki OS, using emulated Sky motes (Dunkels et al., 2004; Österlind et al., 2006). We use profiling tools provided by the Cooja simulator for analysis and comparison purposes.

Further in this paper, Section 2 presents efforts made in literature to counter blackhole attack. Section 3 describes basic characteristics of network over which approach is presented. Proposed blackhole detection approach is described in detail in Section 4 and formally verified in Section 5. Section 6 presents evaluation methodology and outcome analysis. Section 7 finally concludes our proposal.

2 Related work

As discussed in Section 1 an attacker can fabricate better rank value to attract one-hop neighbours. Weekly and Pister (2012) proposed a hash-chain-based rank generation mechanism that restricts nodes from manipulating the rank value and avoids blackhole formation. Multipath or multiparty RPL (MRPL) proposed by Glissa et al. (2016) ensures packet delivery by providing more than one routing path for a single packet. New trust routing metrics RPL node trustworthiness (RNT) and extended RNT (ERNT) are proposed in literature which consider routing trust of a nodes for parent node selection procedure during DODAG formation (Djedjig et al., 2015, 2017). Computations of both RNT and ERNT are complex heavy and therefore are offloaded to trusted platform module (TPM) chip embedded on devices.

Blackhole avoidance approaches discussed above resist the blackhole formation in an early phase of DODAG formation. Still, at the same time, they increase the latency in topology formation and contradict some of the optimisation criteria of RPL specified by RFC6560 (Winter et al., 2012). Also, an attacker can bypass them by following legit behaviour during initial phase of topology formation. Owing to the characteristics of IoT network, collaboration-based approaches where nodes share either their observations or specification data with BR have shown promising results for blackhole detection in IoT networks (Patel et al., 2016).

In the observation-based collaborative approaches routing behaviour of all the nodes in the network is dynamically observed by setting their one-hop neighbours in promiscuous mode. Observed behaviour is then used to calculate the trust values for the nodes. Opinion triangle-based approaches are shown by Khan and Herrmann (2017) and Nikam and Ambawade (2018), in which belief, disbelief and uncertainty about a node are calculated based on routing and packet forwarding behaviour by all the neighbouring nodes. SIEWE proposed by Patel and Jinwala (2019) uses the packet-forwarding behaviour of node to calculate trust value. A PDR-based trust calculation is shown by Bhalaji et al. (2020) calculates PDR-based trust value at two different levels intra-DODAG and inter-DODAG level. Ctrust-RPL uses forwarding delay along with packet forwarding behaviour to calculate individual node's trust value (ul Hassan et al., 2021).

Running a resource-constraint node in promiscuous mode and processing all captured packets impose extra computational overhead, whereas sending all observed trust values to BR causes extra communication overhead, which has direct impact on energy consumption. Khan and Herrmann (2017), in their proposed approach, use three different trust dissemination mechanisms to reduce communication overhead. SIEWE limits the number of nodes running into promiscuous mode by applying filtering criteria during DODAG formation (Patel and Jinwala, 2019). Ctrust-RPL delegates the complex trust-related computations to cloud layer and reduces the burden on IoT devices (ul Hassan et al., 2021). Pishdar et al. propose the parent change control RPL (PCC-RPL) in which parent nodes only observe their child node's routing behaviour to reduce packet and computation overhead. Still, in order to achieve an accuracy all nodes are sending redundant information (i.e., for a single node all of its neighbouring nodes are sending trust values) Pishdar et al. (2021). One option to avoid promiscuous mode operation and redundant dataflow, is to share RPL specification data with BR. In RPL, each node maintains some specification data to assist routing operations (Winter et al., 2012). It is being shown that anomaly or inconstancy in such specification data can be used to detect blackhole attack (Raza et al., 2013).

The parent-failover mechanism proposed by Weekly and Pister (2012) imposes a compulsion over devices to prove their liveliness by sending a data packet to a BR every 30 seconds. BR periodically broadcasts an unheard node list (UNL) containing a list of nodes that failed to send data packets in that interval. The nodes upon receiving their ID in UNL nodes in the network, consider that their route has a blackhole node somewhere and performs a local repair to generate a new route. A lightweight heartbeat protocol (LHP) proposed by Wallgren et al. (2013) uses a periodic ICMP echo-response exchange between nodes and the BR. On receiving fewer numbers of responses from a particular device or set of devices, BR triggers an alarm. Ribera et al. (2020) enhances LHP by replacing ICMP echo request packets with UDP packets to make it robust against a greyhole attack. A novel distributed IDS, viz., SVELTE is proposed by Raza et al. (2013), in which it is assumed that the blackhole attacker manipulates the rank value to gain a large sub-tree in DODAG. BR collects one of the specification data, viz., neighbour table from all the nodes via mapping packets and find inconstancy in rank value for individual node to detect an attacker node. In contrast to other proposed approaches where a black-list is generated to isolate attackers, SVELTE uses a while-list containing a list of nodes allowed to take p2art in the communication process. Detected attackers are removed from the whitelist of the network. svBLOCK proposed by Luangoudom et al. (2020), extends SVELTE with authenticated encryption (AE) using pre-shared key. In svBLOCK, BR uses secure messages and an optional route to inform nodes that have an attacker as their parent. Upon receiving that message, a node performs local repair and changes its default route.

Observation-based approaches discussed above, detect blackhole accurately as the trust value of a single node calculated at BR is an aggregation of multiple observation from multiple nodes. The accuracy here is achieved on the cost of promiscuous mode operation and extra communication cost. In contrast to that, specification-based approaches are comparatively energy-efficient as they do not require nodes to be set in promiscuous mode, and they need relatively less amount of data transfer between nodes and the BR. Manipulation of trust value in observation-based approaches requires more effort as the final result depends on aggregated values from multiple nodes. In specification-based approaches, a single node can easily manipulate the outcome. In an environment where there is no trusted third party to ensure nodes' genuineness, relying on a single node's opinion is not a feasible solution for detecting an attacker.

3 Network model and assumptions

The proposed approach is designed for 6LoWPAN network. This section presents the characteristics of the assumed network and attacker.

3.1 Physical devices

The network consists of IEEE 802.15.4 base resource-constraint (in terms of memory, bandwidth, computation power and communication range) sensing devices and a comparatively resource-rich edge device. BR is an edge device that performs topology formations and management. BR also works as a tunnel to connect 6LoWPAN with the internet backbone.

3.2 Network topology and protocol

RPL is used as a routing protocol for managing topology and routes in the network. In an assumed lossy environment RPL is the best candidate as it generates an optimised DODAG topology that can handle one-to-many, many-to-many and many-to-one traffic flow. For proposed approach RPL is assumed to be working in the non-storing mode in which routing table is only maintained at the BR. A node communicating with another node within or outside the 6LoWPAN network has to send that packet first to the BR, which is then forwarded to its actual destination. To manage route properly RPL at every node in the network maintains some specification data like neighbour table, default route list, topology specification. To generate, manage and repair topology, the modified internet control message protocol (ICMP) packets are used (Lamaazi et al., 2018). To maintain specification data and routing table, those packets continuously flows between nodes and the BR. The off-line node list is also maintained at the BR, which contains a list of nodes that fails to send control packets at BR. RPL also has a repairing mechanism by which it can perform a local and global repair if any anomaly is detected.

3.3 Benign node's behaviour

A legitimate node in the network works as a sensing device and sends sensed data periodically to the BR, and if that node is at a non-leaf position, it will work as a router and forward all the packets received from its child nodes.

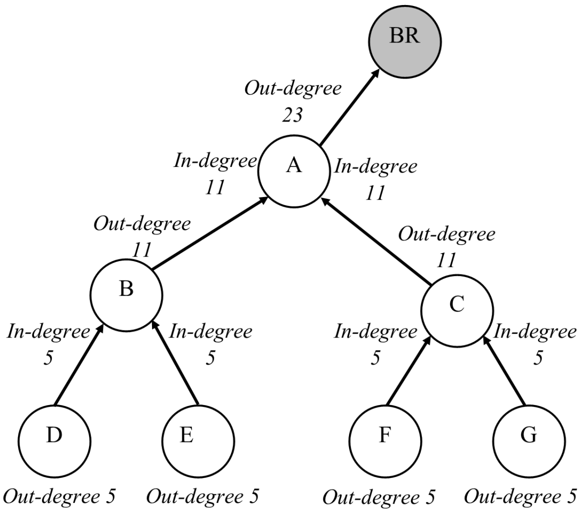
3.4 Attacker node's behaviour

As per the RPL specifications, all nodes have to take part in topology formation actively; otherwise, they will be removed from the DODAG or their malicious behaviour will get noticed. To provide stability, control packets continuously flow between nodes and the BR. Hence in assumed network and attacker node only drops all data packets whilst actively take part in RPL topology formation and forwards all control packets. As underlying IEEE 102.15.4 data link layer security is assumed, an attacker cannot modify a packet's content while forwarding it. An attacker only can send false or manipulated data. Also, an attacker cannot perform an impersonation attack, i.e., it cannot send a packet on behalf of other legitimate nodes.

4 Proposed approach

Collaborative approaches work by periodically sharing some pieces of information with BR. The collected information is then combined and used to categorise each node's behaviour. The imposed overhead of an approach depends on additional computational and communication requirements of the underlying mechanism.

Figure 3 DODAG

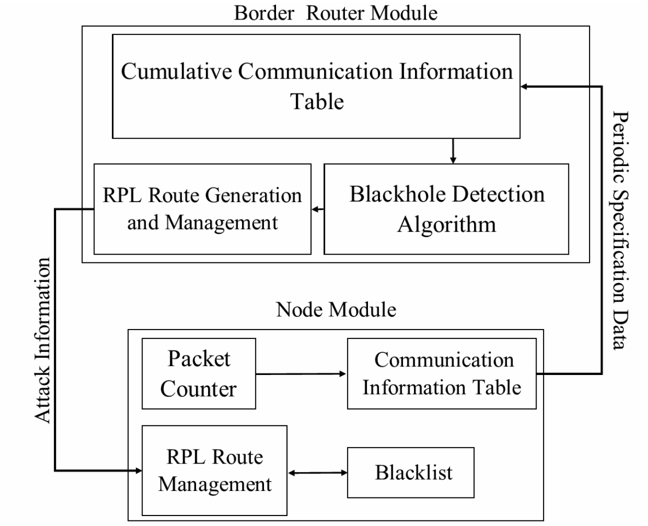


As discussed before here an improved specification-based blackhole detection approach is proposed that calculates the packet forwarding trust of a node by assembling specification values shared by that node and its associated (child and parent) nodes, without running them in promiscuous mode.

Consider a DODAG shown by Figure 3 containing six nodes and a BR. Except for leaf nodes and BR, all the nodes in a network also serve as a router to forward packets towards BR. Some observations from Figure 3 are as follows:

- *Observation 1:* For each node, *in-degree* and *out-degree* are specified, which represent numbers of packets received and sent by the node during a particular time interval, respectively.
- *Observation 2:* For an individual edge, ratio of *in-degree* to *out-degree*, at associated nodes shows the PDR of that link. For example, consider an edge DB, *out-degree* of node D is 5 and at another end *in-degree* of node B is also 5 which makes PDR of that link 100%.
- *Observation 3: Out-degree* at any intermediate node is always more than the addition of all incoming link's *in-degree* which supports the fact that all intermediate nodes are serving dual functionalities of a router and sensing device.
- *Observation 4:* Individual nodes routing behaviour can be verified using its parent and child node's claims (e.g., node B's claim that it has received a total of ten packets from child nodes and forwarded 11 packets to the parent node, can be supported by node D, E, and A's claims)

Figure 4 Proposed IDS architecture


Border Router Module
Cumulative Communication Information Table
RPL Route Generation and Management
Blackhole Detection Algorithm
Periodic Specification Data
Attack Information
Node Module
Packet Counter
Communication Information Table
RPL Route Management
Blacklist

Proposed approach leverages the observed characteristics of DODAG in a *cost-effective* way to detect a blackhole attack. Figure 4 shows basic architecture of proposed blackhole detection approach. The architecture is divided into two components. *Light-weight* component resides in each nodes and its *counter-part* which is capable of handling more data and perform complex computations, resides in the BR.

At each individual node, packet counter module keeps count of all incoming and outgoing packets along with their source and destination ID respectively and logs the details in communication information table (CIT). For a IoT device, keeping a count of incoming and outgoing packets imposes a slight overhead in terms of memory, while energy and computational overheads are negligible. Table 2 shows structure of CIT at node B from Figure 3.

Each node periodically (at δ_t interval) shares contents of its CIT with BR in a form of CIP. Section 6.3 present further analysis about selection of δ_t value for proposed approach. Figure 5 shows basic 8-byte structure of CIP and Table 3 shows size and significance of each field from CIP.

Table 2 Communication information table for node B

Node Id	*Direction*	*Count*
D	Received	5
E	Received	5
A	Forwarded	11

Figure 5 Communication information packet

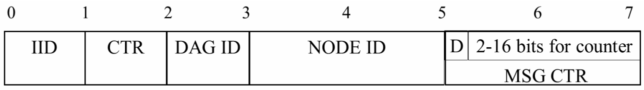


Table 3 Fields in CIP

Field	*Size (in bytes)*	*Usage and significance*
IID	1	Current RPL instance ID
DAGID	2	Current DODAG version number
CTR	1	Iteration counter value
NODE ID	2	Child/parent node ID
MSG CTR	2	Numbers of packets (sent/received)

RPL instance ID (IID) and *DODAG ID (DAGID)* are defined in RPL specifications and uniquely identify current version of RPL and DODAG respectively (Winter et al., 2012). The CTR represents the period/iteration for which CIP is generated. Value of CTR is basically used to provide synchronisation between nodes and BR. *IID*, *DAGID* and *CTR* along with source ID are used to represent CIP uniquely for a given source for a particular period/iteration. Algorithm 1 shows pseudocode, which uses all three field form CIP to provide replay protection. *NODE ID* contains the ID of a device with whom the source node has communicated (either sent or received packets).

Algorithm 1 CIP replay protection

```
procedure IS_REPLAYED($pkt$)
    $last\_cnt \leftarrow comm\_tbl[pkt.source].last\_count$
    if $last\_cnt \leq pkt.cnt$ then
        if $pkt.IID = current.IID$ and $pkt.IID = current.IID$ then
            return 0
        end if
    else
        return 1
    end if
end procedure
```

MSG CTR field represents the numbers of packets communicated with the node having ID represented by the NODE ID field. *MSG CTR* is 2-bytes long field. A byte can be used to store *MSG CTR* value, but it will limit the maximum count value that CIP can carry to 255. It makes compulsion that after every 255 transmissions, a node must have to share CIP with BR, and in highly responsive network, count value will frequently reach to its maximum and overburden network with the unnecessary transmission of CIP. Keeping *MSG CTR* 2-bytes long will waste some bits in the counter as it will not reach its maximum during execution. To provide space and communication efficiency, we combine *MSG CTR*, and a *Direction* fields in the 2-bytes, the most significant bit (MSB) here is used to hold the communication direction (1-sent/0-received). The remaining bits represent the numbers of transmissions in that direction.

Though DODAG provides optimised routing of packets, in the presence of a blackhole attack cannot guarantee the reception of all generated CIPs at BR. Hence for our proposed approach, each node periodically broadcast CIPs in the network until it reaches the BR. Section 6.3 presents further analysis on broadcasting mechanism. Each CIP is handled separately at the BR. Algorithm 2 shows pseudocode for CIP verification.

Algorithm 2 Communication information verification

```
procedure COMMUNICATION INFORMATION VERIFICATION
    $i \leftarrow 0$
    $d \leftarrow 0$
    $pkt\_cnt \leftarrow 0$
    for every $ci\_pkt\_rcv$ do
        if $ci\_pkt\_rcv$ is legitimate then
            $d = ci\_pkt\_rcv.msg\_ctr \wedge 0X80$
            $pkt\_cnt = ci\_pkt\_rcv.msg\_ctr \wedge 0X7F$
            if (is_replayed($ci\_pkt\_rcv$)=0) then
                if CIP has matcing pair then
                    remove matching pair from CCIT and mark its entry in routing table.
                else
                    Add CIP to CCIT for future use.
                end if
            else
                Drop packet and return
            end if
        else
            Mark source node of $ci\_pkt\_rcv$ for false-claim in routing table
        end if
    end for
end procedure
```

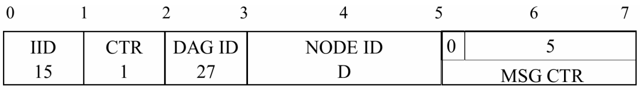
Table 4 Cumulative communication information table

Node 1	*Node 2*	*Direction*	*Msg count*	*CTR*
D	B	Forwarded	5	1
E	B	Forwarded	5	1
F	C	Forwarded	5	1
C	G	Received	5	1

BR first verifies the freshness of incoming CIP and then verify it for false-claim which assures that node only claims communication with its actual child or parent node which can easily be done by consulting the routing table, and node can send packets only for current or next iteration. A node sending a false claim will be marked in the routing table for further verification. Algorithm checks for matching pair in cumulative communication information table (CCIT) for each legitimate CIT. Table 4 shows basic structure of CCIT. In case CCIT is empty or CIP do not have matching pair in CCIT, incoming CIP is stored in CCIT for future use.

To understand the notion of a matching pair, consider Figure 6 as an incoming CIP sent by node B. The CIP is interpreted as node B is claiming that it has received five packets from node D during time interval 1. To verify node B's claim, we have to consult CCIT mentioned in Table 4; the first tuple in Table 4 shows that node D had already claimed that it had sent five packets to node B; hence, incoming CIP is said to be verified. In case of inconsistency in count value between two claiming nodes, lesser value of count is considered the final transmission count between them, and remaining packets are deemed lost or dropped.

Figure 6 Communication information packet



0	1	2	3	4	5	6	7
IID 15	CTR 1	DAG ID 27	NODE ID D		0	5 MSG CTR	

The integrity of transmission does not carry any weight in observation-based approaches as nodes running into promiscuous mode observe only source and destination fields from the header part of other nodes' sniffed transmissions. An attacker can temper the packet contains to make them dropped at another end of the link and remain undetected. In CIP verification mechanism employed in our approach, BR node verifies claims from both end devices to reach consensus about packet transmission count. As per the RPL specifications, BR maintains a routing table to store all the routes in the network; we add an extra column to the routing table that holds a successful transmission count. At the end of the verification procedure, the precise transmission count value for the corresponding link is logged in the extended routing table.

Table 5 Extended routing table entries at border router

Node Id	*Next-Hop*	*Transmissions*	*False-claims*
A	A	23	0
B	A	11	0
C	A	11	0
D	B	5	0
E	B	5	0
F	C	5	0
G	C	5	0

Table 5 shows an extended routing table with corresponding entries. The routing table contains a list of all edges, and corresponding successful transmission count values, added by CIP handling algorithm. Algorithm 3 shows pseudocode for blackhole detection, which runs over an extended routing table periodically (at Δ_t interval) and perform three primary tasks list generation, communication count, and attacker-detection. Brief detail about tasks are as follows:

Task 1: List generation

In Algorithm 3, L_i is a non-primitive data structure and can hold a list of nodes along with their associated *in-degree*, *out-degree* and *false-claim* values. The next-hop column of the extended routing table contains a list of all intermediate nodes. Their malevolent behaviour leads to a blackhole attack; hence, L_i is filled by all the distinct values from the next-hop column of the extended routing table.

Algorithm 3 Blackhole detection algorithm

```
procedure BLACKHOLE DETECTION
    if $L_i$[i] = next-hop[j] then
        Make list $L_i$ for all distinct nodes from next-hop column of routing table.
    end if
    for every entry i in CCIT do
        if entry i is from previous iteration and destination node is not in offline list then
            increase false-claim value of destination node of that entry in routing table
        end if
    end for
    for every $i$ in $L_i$ do
        for every $j$ in Routing table do
            if $L_i$[i].nodeID = tbl[j].nodeID and $L_i$[i].nodeID = tbl[j].next-hop then
                $L_i$[i].out-degree=$L_i$[i].out-degree+Tr[j]
            else
                if $L_i$[i] = tbl[j].nodeID then
                    $L_i$[i].out-degree=$L_i$[i].out-degree+Tr[j]
                end if
                if $L_i$[i] = tbl[j].next-hop then
                    $L_i$[i].in-degree=$L_i$[i].in-degree+Tr[j]
                end if
            end if
        end for
    end for
    for every $i$ in $L_i$ do
        $Tr_i = L_i[i].\textit{out-degree}/L_i[i].\textit{in-degree}$
        if $Tr_i < \delta_{loss}$ or $Tr_i > \delta_{rate}$ or $L_i[i].false-claim > \delta_{false}$ then
            $L_i$.[i] is added to Black-list.
            New-entry = True
        end if
    end for
    for every $i$ in Routing table do
        if $tbl[i].false-claim > \delta_{false}$ then
            $tbl[i].NodeID$ is added to Black-list.
            New-entry = True
        end if
    end for
    Broadcast Blacklist if it has any new entry.
end procedure
```

Task 2: Total communication count

Once a list containing IDs of intermediate nodes is generated, their associated *in-degree* and *out-degree* is calculated form the extended routing table. Each tuple in the routing table consists of a node and its immediate parent's

IDs. We combine those two columns for our proposed approach and consider it an edge and transmissions column as numbers of successful transmission over it. To calculate individual node's *in* and *out* degree from available transmission count value of edges, following cases are considered:

$$out\text{-}degree_{id} = \begin{cases} +tr, & \text{if } id \in NodeId \; \& \; NextHop \\ +tr, & \text{if } id \in NodeId \\ +0, & \text{otherwise} \end{cases}$$

$$in\text{-}degree_{id} = \begin{cases} +tr, & \text{if } id \in NextHop \\ +0, & \text{otherwise} \end{cases}$$

tr represents corresponding value of transmissions column from extended routing table.

- *Case 1:* If node's ID is in node ID and next-hop columns of routing table then node is connected to the BR and has sent packets to the BR corresponding transmission value is added to the *out-degree*.
- *Case 2:* If node's ID is in node ID column, implies that the node has acted as a child node and corresponding transmissions value is added to the *out-degree*.
- *Case 3:* If node's ID is in next-hop column, implies that node has acted as a parent and corresponding transmissions value is added to the *in-degree*.

Task 3: Attacker-detection

After completion of task 1 and task 2, L_i is having list of all intermediate nodes along with their *in* and *out degrees*. To detect an attacker, packet forwarding trust value Tr_{it} for node i during time interval t is calculated as shown by equation (1).

$$Tr_{it} = \frac{out\text{-}degree_{it}}{in\text{-}degree_{it}} \tag{1}$$

Values of *out-degree*$_{it}$ and *in-degree*$_{it}$ represents numbers on incoming and outgoing packets for a node i during time interval t. Trust value Tr for any node must remain between specified threshold value δ_{loss} and δ_{rate} threshold. Nodes that fail to maintain Tr between this range is then added to the black-list at the BR. Thus, the algorithm assures that node's packet forwarding behaviour and restricts them from forwarding extra packets to manipulate trust calculation value. After completion of an iteration, if there are still some entries from the previous iteration in CCIT then those entries are considered as false claims, and destination node in those claims are, if not in offline list, then will be marked for *false-claim* in extended routing table. Nodes with a *false-claim* count value more than a predefined threshold are considered an attacker and added to the black-list. When black-list at the BR gets updated, BR also broadcast new entries to synchronise black-list at individual node in the network.

When a node receives a black-list update packet from the BR, it adds updated entries in its local black-list. When the parent node gets black-listed by a detection process, a node invokes the local repair mechanism of RPL protocol to generate a new legitimate route towards a BR. In our proposed approach, black-list remains persistent for network lifetime while extended routing table, CIT and CCIT are regenerated for each new version of DODAG.

5 Formal verification of the proposed approach

To verify the claim that no single node can manipulate trust value calculation by sending false information or fake CIP formal verification is carried out. This section presents lemmas and theorem which proves the proposed claim.

Lemma 1: No single node can send false values in their CIP to manipulate *in-degree* and *out-degree* values.

Proof: Assume a node submits a false send or receive count values to the BR. CIP is a claim about the numbers of transmissions it has carried out with another device. As per Algorithm 2 each CIP is checked for an opposite claim in CCIT and if any found lowest value of the claim out of two, is considered as a final transmission count and remaining packets are considered as a lost or dropped. Hence, a false claim by a single node will not have any effect on the final transmission count value. □

Lemma 2: No node can send fake CIP to manipulate trust value of a node which is not connected to it.

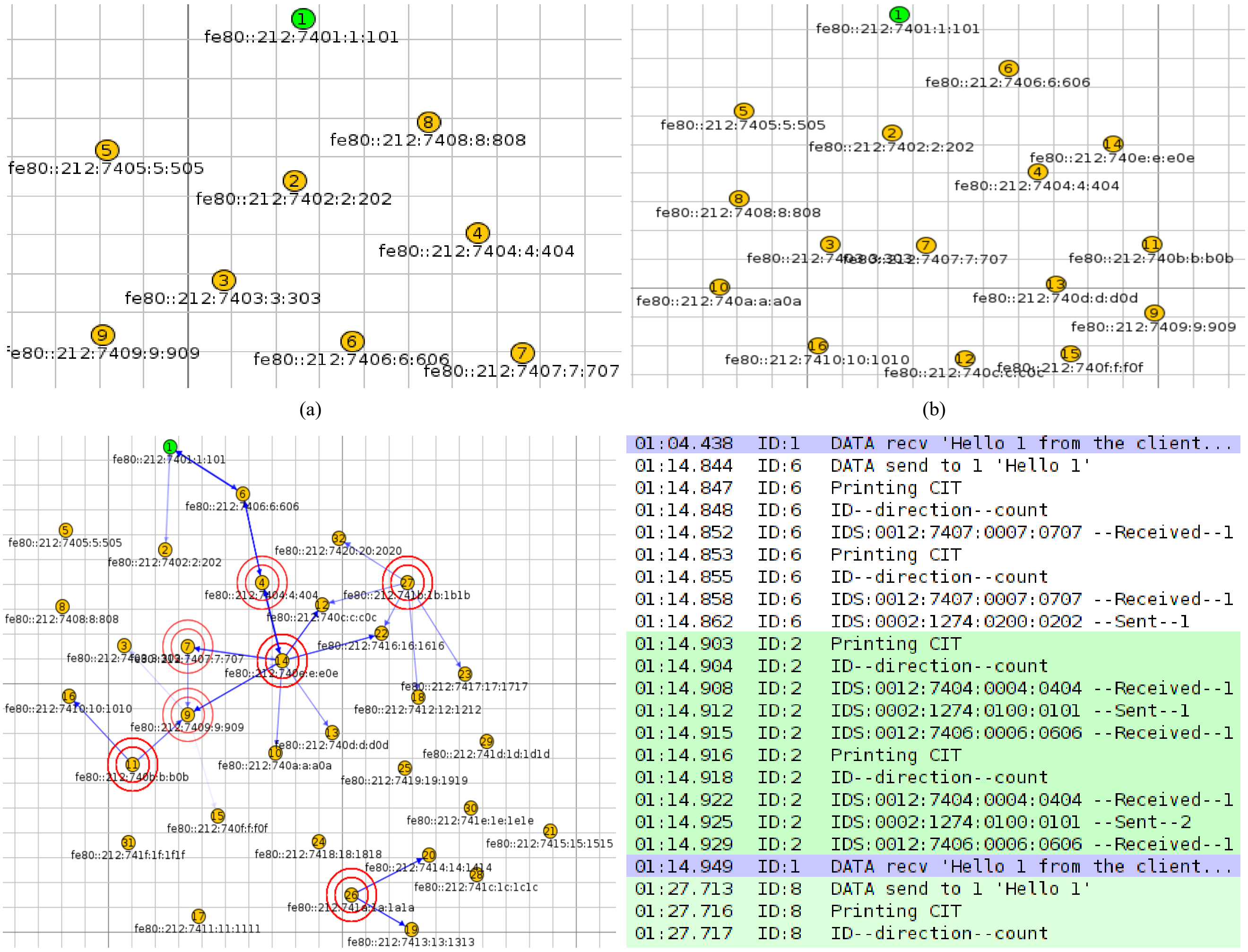
Proof: Assume a node submits a fake CIP for a node which are not in its range. At BR node, CIP is first verified for its legitimacy by consulting the routing table. If a node is claiming transmission with another node that is not its parent or child node, then the node is marked for false-claim, and incoming CIP is dropped. Hence, a false claim by a node for another node that is not in its range does not affect the final transmission count. Also, a node sending a false value will have its trust value decrease. □

Lemma 3: No node can increase its trust value by sending packets at higher rate.

Proof: Assume a node sends packets at a higher data rate compared to its child and sibling nodes and claims same via CIP. The claim by that node get verified by its parent node. Still, the blackhole detection algorithm at the time of trust value calculation also confirms that the node's data rate must not be higher than the predefined data. If any node exhibits such behaviour, it will get marked for false-claim in the routing table and increase the possibility of being blacklisted. □

Lemma 4: No node can decrease trust of other nodes by not sending the CIP packets.

Figure 7 Network setup and CIT, (a) network with 8 nodes (b) network with 16 nodes (c) network with 32 nodes (d) CIT maintained at node (see online version for colours)



(a)

(b)

(c)

```
01:04.438   ID:1   DATA recv 'Hello 1 from the client...
01:14.844   ID:6   DATA send to 1 'Hello 1'
01:14.847   ID:6   Printing CIT
01:14.848   ID:6   ID--direction--count
01:14.852   ID:6   IDS:0012:7407:0007:0707 --Received--1
01:14.853   ID:6   Printing CIT
01:14.855   ID:6   ID--direction--count
01:14.858   ID:6   IDS:0012:7407:0007:0707 --Received--1
01:14.862   ID:6   IDS:0002:1274:0200:0202 --Sent--1
01:14.903   ID:2   Printing CIT
01:14.904   ID:2   ID--direction--count
01:14.908   ID:2   IDS:0012:7404:0004:0404 --Received--1
01:14.912   ID:2   IDS:0002:1274:0100:0101 --Sent--1
01:14.915   ID:2   IDS:0012:7406:0006:0606 --Received--1
01:14.916   ID:2   Printing CIT
01:14.918   ID:2   ID--direction--count
01:14.922   ID:2   IDS:0012:7404:0004:0404 --Received--1
01:14.925   ID:2   IDS:0002:1274:0100:0101 --Sent--2
01:14.929   ID:2   IDS:0012:7406:0006:0606 --Received--1
01:14.949   ID:1   DATA recv 'Hello 1 from the client...
01:27.713   ID:8   DATA send to 1 'Hello 1'
01:27.716   ID:8   Printing CIT
01:27.717   ID:8   ID--direction--count
```

(d)

Proof: Assume a node avoids sending CIP to the BR node, then CIPs sent by its parent and child nodes will remain unverified in CCIT. BR executes the blackhole detection periodically scans CCIT for unverified entries from previous time intervals. If during scan any such entry is found, and if destination or second address mentioned in the CIP, not in the offline node list, then that address will be marked as false-claim in the routing table. Hence, by not sending the CIP and the node will make its parent and child nodes claim unverified and eventually increase its probability to get into the backlist. □

Theorem 5: No single node in the network, by manipulating a CIP can affect other node's trust value.

Proof: Assume Lemma 1, Lemma 2, Lemma 3 and Lemma 4 are true. By Lemma 1 and Lemma 2, no node can manipulate trust value of other nodes by manipulating or faking CIP. Also, proposed approach can detect such activity and can blacklist such nodes. By Lemma 3, no node can increase its trust value by sending packets at higher rate, and by Lemma 4 if a node chooses not to send CIP will get its trust value decreased and eventually will get into blacklist. □

6 Simulation and results analysis

To verify execution, the proposed approach is implemented using a real-time Contiki operating system. Libraries for 6LoWPAN and RPL implementation are designed in Contiki OS (Dunkels et al., 2004). For simulation purposes, Cooja simulator is used, which has inbuilt profiling tools that can evaluate different parameters like energy, PDR, throughput, CPU cycle (Österlind et al., 2006). Emulated sky mote platform is used to deploy proposed algorithms in unit disk graph medium (UDGM). To connect emulated BR with outer network *tunslip6* utility provided by Contiki OS is used. Tunslip works as a virtual network interface on the host machine, which provides IP tunnelling to emulate BR with the use of serial line internet protocol (SLIP). Table 6 shows list of basic simulation parameters.

6.1 Packet counter setup

As shown by Figure 1, BR nodes work as an edge device to connect 6LoWPAN network to the internet. IPv6 packets generated at the sensor nodes are tunnelled via BR over the internet. RPL provides routing of those IPv6 packets over resource constraint sensing devices. At IEEE 802.15.4 medium access control layer (MAC-Layer) each node forwards a packet to one-hop default parent node until it reaches BR. The packet counter is designed over MAC-Layer and logs an entry of each packet along with the relevant address and count values, in CIT. Each tuple in CIT contains 64-bit IP prefix, 8-bit counter value and 8-bit to store the direction of communication.

Table 6 Simulation environment

Parameter	*Value*
Simulator	Cooja
Radio model	UDGM
Node radio range	Rx and Tx 50 m
Mote type	sky
TX/RX success rate	80%
Size of deployment region	100 $*$ 100 m
Number of nodes	8 to 32
Types of nodes	3
Physical layer	IEEE 802.15.4
Routing protocol	RPL
Additional tools used	Collect View, tunslip
Simulation time	Variable

Figure 7 shows network setup and CIT generated at intermediate nodes. Simulations are carried out over varying size networks (8, 16 and 32 nodes). Leaf nodes are end devices and have a single tuple in their CIT whereas intermediate nodes have more than one tuple.

Table 7 shows memory overhead imposed by CIT at different nodes in the simulated network. For our analysis, we divide nodes into leaf and non-leaf categories. Leaf nodes contain a single entry in their CIT, i.e., for their parent node. Non-leaf nodes, as per their position in the network and number of associated child nodes, have varying numbers of tuples in CIT. Depending on node density, all intermediate nodes have an average of 3–5 tuples. Hence memory required to store packet counter varies between 80 to 400 bits depending upon the node's position in the network and is negligible.

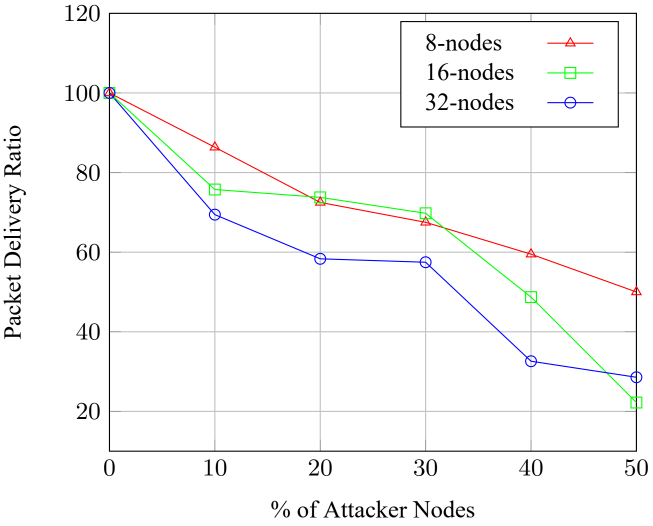
Table 7 Size of CIT (bits) at different nodes

Node-type		*Size of CIT (in bits)*		
		Figure 7(a)	*Figure 7(b)*	*Figure 7(c)*
Leaf nodes		80	80	80
Non-leaf nodes	Min	160	240	240
	Max	320	400	400

6.2 Blackhole setup

To create an attacker node, 6LoWPAN protocol stack is modified to drop all data packets. Attacking scenarios are simulated over varying size networks represented by Figures 7(a), 7(b) and 7(c). PDR of the whole network is calculated by taking a ratio of a total number of packets received by BR to a total number of packets sent by nodes in the network. Simulation scripts are used to calculate PDR value from the output log.

Figure 8 Packet delivery ratio during attacking scenarios (see online version for colours)



To analyse the effect of the blackhole attack on PDR, three different non-lossy network scenarios containing 8, 16 and 32 nodes have been simulated and the effect of the attack has been thoroughly analysed by deploying attackers in proportion with network size (0, 10, 20, 30, 40, and 50 percentage). For each scenario, simulations have been carried out ten times each for 30 minutes, and precise results were generated by calculating the average value of all intermediate results. Figure 8 present comparison between PDR values from all scenarios. It is clear from the figure that in the absence of an attacker, all the packets are received successfully at the BR and when more attackers are added to the network PDR decreases drastically.

To make the attacking scenario more realistic, attackers in the simulation were programmed to stop working as a router. Still, they were generating packets and were forwarding them to the BR. Hence in the presence of 50% of attackers, still some packets were received. In a small network, all 50% of attackers have a small probability of spanning over different levels. Still, in a large network, they can have positions at different levels and drop more packets. Figure 8 shows that a network with 8 noes and 50% of attackers has better PDR than the large networks because it might be possible that an attacker can have other attackers in its sub-tree.

6.3 Robustness of broadcast transmissions

Though RPL provides energy-efficient routing, it cannot guarantee packet delivery in the presence of blackhole attackers. To achieve accuracy in the presence of attackers, the proposed approach uses a broadcast mechanism for sending fixed size CIP packets to the BR node. The broadcast mechanism guarantees packet delivery but also increases energy consumption at each node in the network. This section presents an analysis of the used broadcast mechanism, from the PDR and, packet delay perspective.

Figure 9 Packet delivery ratio for broadcast scenario (see online version for colours)

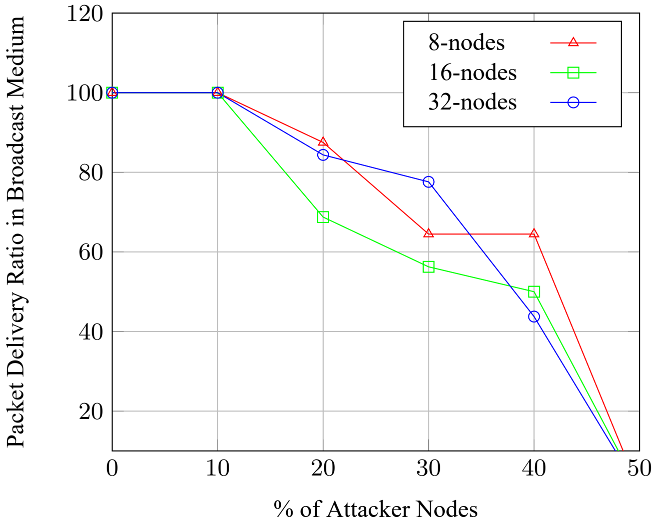
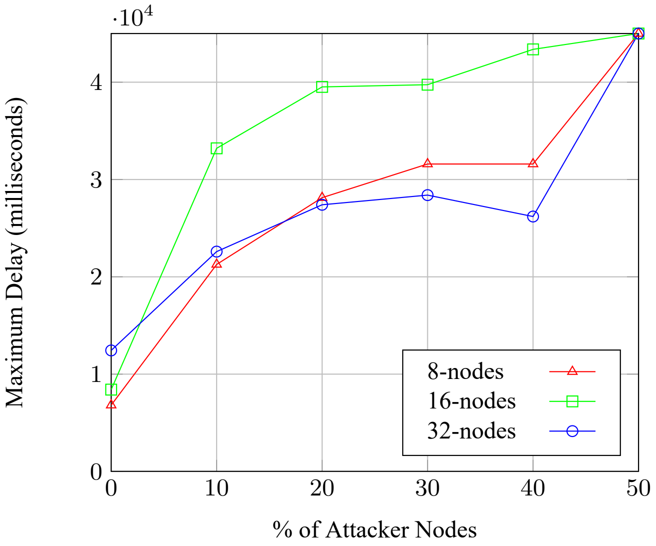


Figure 10 Maximum packet delay in broadcast scenario (see online version for colours)



In the context of the proposed approach, robustness is defined by accurate and timely delivery of CIP packets at the BR. To verify robustness, three networks with 8, 16 and 32 nodes with attackers up to 50% of the network size were simulated for each scenario 30 minutes ten times. Attacker nodes considered are not generating or broadcasting any CIP. Attackers were deployed randomly, but to simulate the worst-case scenario, they intentionally kept nearby the BR.

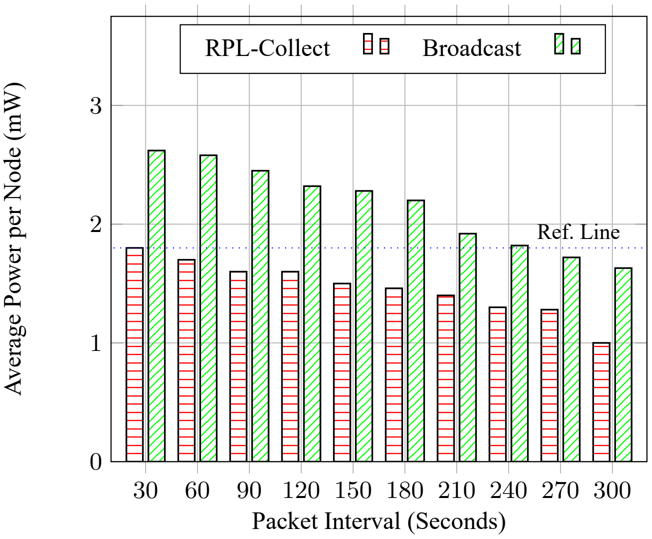
Figure 9 shows comparison between PDR values of three network setup consisting of 8, 16 and 32 nodes. Simulation analysis shows that in any network, a broadcast mechanism can achieve 100% PDR in the presence of 10% attackers, and it gradually decrease when more attackers are added. For more than 50% of attackers, a broadcast mechanism will not be able to deliver a packet or have very less PDR.

Figure 10 shows the maximum time taken by a packet from a node to reach BR in the broadcast scenario. Simulation results show that in the simulation environment, a maximum delay will gradually increase with the increase in numbers of attackers, and with 50% attacker nodes, it reaches infinity, i.e., all packets will be lost. Simulation analysis also shows that network size impacts packet delay; for a small network with 8 nodes, has more delay occurred than 16 and 32 nodes. For a small network in the worst-case scenarios, a packet has to move through multiple hops to reach BR whereas in a large dense network, a packet has multiple paths and can traverse comparatively fast.

6.4 Energy consumption analysis

Robustness of broadcast medium is already discussed in Section 6.3. Considering the fact that most of the energy in 6LoWPAN devices is consumed during a transmission operation in devices (Akyildiz et al., 2002), this section presents an energy consumption analysis by the proposed broadcast mechanism.

Figure 11 Average power consumption (see online version for colours)



The simulation environment is configured with RPL protocol to send fixed-size packets to the BR at regular intervals, and the same messages are then broadcasted at the same intervals and handled by BR. For an analysis purpose, intervals of 30, 60, 90, 120, ... up to 300 seconds are considered. Profiling tools available in Cooja gives average power consumption of individual node in the network. Network-wide energy collected using the profiling tool is then divided by the total number of nodes to calculate average power consumption per node.

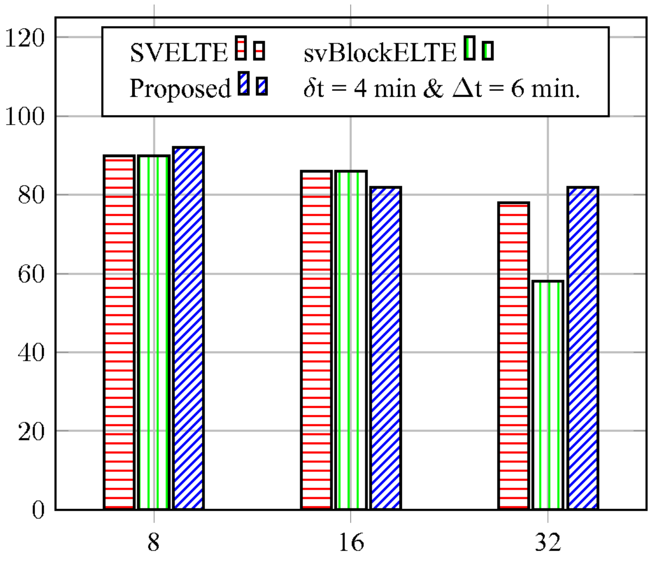
Figure 11 shows a comparison between RPL and broadcast scenarios with the same size and same numbers of packets. Time intervals 30, and 120 are used in literature to collect data at BR (Weekly and Pister, 2012; Wallgren et al., 2013; Ribera et al., 2020; Raza et al., 2013; Luangoudom et al., 2020).

Attempted simulation analysis shows that per node energy consumption for the small-time period in RPL scenario is near equals to the large-time period in a broadcast scenario. Reference line in Figure 11 emphasises the same observation in the graph. Energy consumption analysis also supports the claim laid by a proposed approach that by broadcasting a CIP at a comparatively large interval, robustness can be achieved with the same energy consumption. For further evaluation broadcast interval of 240 seconds is considered to send CIP at the BR.

6.5 Detection accuracy

This section presents the quantitatively evaluated detection rate of the proposed approach. For comparative analysis, True positive rate, i.e., the total number of successful alarms divided by the total number of alarms, is used. The proposed approach is executed over simulation environments consisting of 8, 16, and 32 nodes with less than 10% of attackers randomly positioned in the network. Every node in the network broadcasts CIP at regular interval of $\delta_t = 4$ minutes and the BR execute blackhole detection algorithm at the interval of $\Delta_t = 6$ minutes.

Figure 12 True positive rate (see online version for colours)



Blackhole detection algorithm, set to be executed initially after 4 minutes of booting, yields nothing as some CIPs are in commute or being processed. Therefore the earliest possible time for an initial call to detection algorithm is after 6 minutes of the first CIP is received. After that, it will be executed at a regular interval of 6 minutes. Experimental evaluations also show that the detection algorithm behaves accurately in a lossless environment. Hence, to verify its robustness in a lossy environment, we set up a simulation with 20% packet loss.
Figure 12 shows a comparison between true positive rate (TPR) values of the proposed approach, with existing approaches from the literature. TPR values of SVELTE (Raza et al., 2013) and svBLOCK (Luangoudom et al., 2020) are used to compare accuracy of the proposed approach. The proposed approach gives better accuracy in a network with 8 nodes but degrades slightly but remains somewhat stable with 16 and 32 nodes. A small degrade in the accuracy is due to a lossy environment as some data and CIP packets are lost in transit and decrease their corresponding node's trust values at BR.

7 Conclusions

This paper proposes a novel robust lightweight specification-based approach to detect and isolate blackhole attackers in 6LoWPAN. Resource constraint nodes maintain a lightweight data structure called a CIT with little memory and negligible computation overhead. To make the detection system robust in the presence of attacker nodes periodically broadcasts the information from CIT towards the BR. Our analysis shows that broadcasting over a large time interval does not impose any extra overhead over a device. All energy sensitive tasks are carried out by the BR after collecting broadcast packets from the nodes. Our experiments show that the proposed approach gives more than 80% of the true positive rate even in the presence of 10% attacker nodes. Compared to the state-of-the-art approaches, the true positive rate for blackhole node detection remains stable when the network size increases. To maintain the trade-off between accuracy and energy, detection decision here is delayed as broadcasting a packet at a small interval consumes more energy.

References

Akyildiz, I., Weilian, S., Sankarasubramaniam, Y. and Cayirci, E. (2002) 'A survey on sensor networks', *IEEE Communications Magazine*, Vol. 40, No. 8, pp.102–114.

Atzori, L., Iera, A. and Morabito, G. (2010) 'The internet of things: a survey', *Computer Networks*, Vol. 54, No. 15, pp.2787–2805.

Bhalaji, N., Hariharasudan, K. and Aashika, K. (2020) 'A trust based mechanism to combat blackhole attack in RPL protocol', *International Conference on Intelligent Computing and Communication Technologies*, pp.457–464.

Chowdhury, M. (2022) 'An energy harvesting, blockchain, and qos-aware intelligent healthcare task coordination policy for IoT-assisted networks', *International Journal of Embedded Systems*, Vol. 15, No. 4, pp.313–325.

da Silva, T.B., Chaib, R.S., Cerqueira, S.A., Righi, R.d.R. and Alberti, A.M. (2021) 'Towards future internet of things experimentation and evaluation', *IEEE Internet of Things Journal*, Vol. 9, No. 11, p.1.

Djedjig, N., Tandjaoui, D. and Medjek, F. (2015) 'Trust-based RPL for the internet of things', *2015 IEEE Symposium on Computers and Communication (ISCC)*, IEEE, pp.962–967.

Djedjig, N., Tandjaoui, D., Medjek, F. and Romdhani, I. (2017) 'New trust metric for the RPL routing protocol', *8th International Conference on Information and Communication Systems (ICICS)*, IEEE, pp.328–335.

Dunkels, A., Gronvall, B. and Voigt, T. (2004) 'Contiki – a lightweight and flexible operating system for tiny networked sensors', *29th Annual IEEE International Conference on Local Computer Networks*, pp.455–462.

Gebremariam, G.G., Panda, J. and Indu, S. (2023) 'Design of advanced intrusion detection systems based on hybrid machine learning techniques in hierarchically wireless sensor networks', *Connection Science*, Vol. 35, No. 1, p.2246703.

Glissa, G., Rachedi, A. and Meddeb, A. (2016) 'A secure routing protocol based on RPL for internet of things', *IEEE Global Communications Conference (GLOBECOM)*, IEEE, Washington, DC, USA, pp.1–7.

Hui, J., Thubert, P. et al. (2011) *Compression Format For IPv6 Datagrams Over IEEE 802.15.4-Based Networks*, Tech. Rep., RFC6282, IETF 6LoWPAN WG.

Janani, K. and Ramamoorthy, S. (2022) 'Threat analysis model to control iot network routing attacks through deep learning approach', *Connection Science*, Vol. 34, No. 1, pp.2714–2754.

Khan, Z.A. and Herrmann, P. (2017) 'A trust based distributed intrusion detection mechanism for internet of things', *IEEE 31st International Conference on Advanced Information Networking and Applications (AINA)*, pp.1169–1176.

Lamaazi, H., Benamar, N. and Jara, A.J. (2018) 'RPL-based networks in static and mobile environment: a performance assessment analysis', *Journal of King Saud University – Computer and Information Sciences*, Vol. 30, No. 3, pp.320–333.

Lokhande, M.P. and Patil, D.D. (2022) 'Enhancing the energy efficiency by leach protocol in the internet of things', *International Journal of Computational Science and Engineering*, Vol. 25, No. 1, pp.1–10.

Lu, Q., Li, H., Zheng, J., Qin, J., Yang, Y., Li, L. and Jiang, K. (2023) 'A new reinforcement learning approach for improving energy trading management for smart microgrids in the internet of things', *International Journal of Embedded Systems*, Vol. 16, No. 1, pp.47–56.

Luangoudom, S., Tran, D., Nguyen, T., Tran, H.A., Nguyen, G. and Ha, Q.T. (2020) 'svBLOCK: mitigating black hole attack in low-power and lossy networks', *International Journal of Sensor Networks*, Vol. 32, No. 2, pp.77–86.

Nikam, A. and Ambawade, D. (2018) 'Opinion metric based intrusion detection mechanism for RPL protocol in IoT', *3rd International Conference for Convergence in Technology (I2CT)*, pp.1–6.

Niranjan, L., Venkatesan, C., Suhas, A., Satheeskumaran, S. and Nawaz, S.A. (2021) 'Design and implementation of chicken egg incubator for hatching using IoT', *International Journal of Computational Science and Engineering*, Vol. 24, No. 4, pp.363–372.

Österlind, F., Dunkels, A., Eriksson, J., Finne, N. and Voigt, T. (2006) 'Cross-level sensor network simulation with Cooja', *First IEEE International Workshop on Practical Issues in Building Sensor Network Applications (SenseApp 2006)*, pp.641–648.

Patel, H.B. and Jinwala, D.C. (2019) 'Blackhole detection in 6LoWPAN based internet of things: an anomaly based approach', *TENCON 2019 – IEEE Region 10 Conference (TENCON)*, Kochi, Kerala, India, pp.947–954.

Patel, H.B., Jinwala, D.C. and Patel, D.R. (2016) 'Baseline intrusion detection framework for 6LoWPAN devices', *Adjunct Proceedings of the 13th International Conference on Mobile and Ubiquitous Systems: Computing Networking and Services, MOBIQUITOUS 2016*, Association for Computing Machinery, pp.72–76.

Pishdar, M., Seifi, Y., Nasiri, M. and Bag-Mohammadi, M. (2021) 'PCC-RPL: an efficient trust-based security extension for RPL', *Information Security Journal: A Global Perspective*, pp.1–11.

Raza, S., Wallgren, L. and Voigt, T. (2013) 'SVELTE: real-time intrusion detection in the internet of things', *Ad Hoc Networks*, Vol. 11, No. 8, pp.2661–2674.

Ribera, E.G., Martinez Alvarez, B., Samuel, C., Ioulianou, P.P. and Vassilakis, V.G. (2020) 'Heartbeat-based detection of blackhole and greyhole attacks in RPL networks', *12th International Symposium on Communication Systems, Networks and Digital Signal Processing (CSNDSP)*, pp.1–6.

Shi, S., Han, D. and Cui, M. (2023) 'A multimodal hybrid parallel network intrusion detection model', *Connection Science*, Vol. 35, No. 1, p.2227780.

Silva, M.V., Mosca, E.E. and Gomes, R.L. (2022) 'Green industrial internet of things through data compression', *International Journal of Embedded Systems*, Vol. 15, No. 6, pp.457–466.

ul Hassan, T., Asim, M., Baker, T., Hassan, J. and Tariq, N. (2021) 'CTrust-RPL: a control layer-based trust mechanism for supporting secure routing in routing protocol for low power and lossy networks-based internet of things applications', *Transactions on Emerging Telecommunications Technologies*, Vol. 32, No. 3, pp.1–20.

Vasseur, J., Kim, M., Pister, K., Dejean, N. and Barthel, D. (2012) *Routing Metrics Used for Path Calculation in Low-Power and Lossy Networks*, Tech. Rep., RFC-6551, IETF ROLL WG.

Verma, U. and Bhardwaj, D. (2021) 'ECC-based lightweight mutual authentication protocol for fog enabled IoT system using three-way authentication procedure', *International Journal of Computational Science and Engineering*, Vol. 24, No. 5, pp.505–516.

Wallgren, L., Raza, S. and Voigt, T. (2013) 'Routing attacks and countermeasures in the RPL-based internet of things', *International Journal of Distributed Sensor Networks*, Vol. 9, No. 8, pp.1–11.

Weekly, K. and Pister, K. (2012) 'Evaluating sinkhole defense techniques in RPL networks', *20th IEEE International Conference on Network Protocols (ICNP)*, IEEE, Austin, TX, USA, pp.1–6.

Winter, T., Thubert, P., Clausen, T., Hui, J., Kelsey, R., Levis, P., Pister, K., Struik, R., Vasseur, J. and Alexander, R. (2012) *RPL: IPv6 Routing Protocol for Low Power and Lossy Networks*, Tech. Rep., RFC-6550, *IETF ROLL WG*.

Yasser, M., Mohammed, L., Yasser, E., Abderrahim, T., Abdellah, T. and An, B. (2020) 'A middleware based on service oriented architecture for heterogeneity issues within the internet of things (MSOAH-IoT)', *Journal of King Saud University – Computer and Information Sciences*, Vol. 32, No. 10, pp.1108–1116.