IIETA International Information and Engineering Technology Association
Advancing the World of Information and Engineering

Instrumentation Mesure Métrologie
Vol. 23, No. 5, October, 2024, pp. 391-402
Journal homepage: http://iieta.org/journals/i2m

Behavioural Analysis of Hatchetman Attacker for Detection & Prevention in Low Power and Lossy IoT Network

Gaurav Soni[1], Kamlesh Chandravanshi[1], Arun Singh Kaurav[2], Aradhana Saxena[3], Durgesh Nandan[4], Anurag Mahajan[5*]

[1] School of Computing Science and Engineering (SCOPE), VIT Bhopal University, Sehore 466114, India
[2] Department of Computer Science and Engineering, Guru Nanak Institutions Technical Campus, Hyderabad 501506, India
[3] Department. of Computer Science and Engineering, Lakshmi Narain College of Technology & Science, Bhopal 462022, India
[4] School of Computer Science and Artificial Intelligence, SR University, Warangal, 506371, India
[5] Dept of E&TC, Symbiosis Institute of Technology, Pune Campus, Symbiosis International (Deemed University), Pune 412115, India

Corresponding Author Email: anurag.mahajan@sitpune.edu.in

https://doi.org/10.18280/i2m.230507

Received: 2 September 2024
Revised: 9 October 2024
Accepted: 17 October 2024
Available online: 25 October 2024

Keywords:
attacker, energy, IoT, routing, security, SHLPLN

ABSTRACT

Nodes in the IoT are movable and communicate with other nodes in the network. The nodes are heterogeneous, but they can handle the data delivery efficiently. In the IoT network, nodes send information to other devices to control the function of a particular device or to route data between sender and receiver. In this paper, proposes a security approach for the Hatchetman attacker in low power and lossy networks (SHLPLN). The Hatchetman attacker gradually enhances the flooding of unsolicited data packets in the network to consume primary source communication, i.e., the energy of nodes. The early depletion of energy in the network shows the degradation in routing performance. In the wireless network, unsolicited data flooding also affects bandwidth utilization. The SHLPLN detects nodes in the network that misbehave and intentionally attack the limited bandwidth and energy source of the network. The SHLPLN detects the attacker node's presence in the network and finally block it and, improving energy utilization in network. The previous security RPL scheme was to find the attacker's malicious behavior and figure out what was wrong with the network, but the proposed SHLPLN approach would detect unwanted flooding behavior and apply a prevention scheme to secure IoT communication. The performance of SHLPLN is measured through performance metrics, and throughput showing 20% and PDR showing 5% better performance as compared to the existing scheme in IoT network.

1. INTRODUCTION

The control of devices on a network is made possible by the Internet of Things (IoT). In the network still it's difficult to control the device's response on the basis of requirements. The IoT nodes are capable of doing work on time and efficiently controlling the functioning of other devices. The purpose of a network is to create the proper connection among a number of devices or users. Users use the internet for proper data transfer with high speed for a limited time. The users are using the internet for properly transferring of data with high speed and limited time. In the network still the challenge is to control the device reaction on the basis of requirement. The IoT nodes are capable to do work on time and efficiently control the functioning of other devices. IoT is becoming increasingly important in today's high-tech society, which is characterised by the increasing connectivity of all intelligent devices to the internet. IoT is becoming increasingly appealing because of the growing number of nodes or devices that are connected to the internet [1]. The routing protocol plays an important role in transmitting information between IoT devices. The attacker's presence only degrades the actual routing procedure. IoT nodes are used with any network like Mobile Ad-hoc network (MANET), Flying hoc Network (FANET), Vehicular Ad-hoc Network (VANET) and Wireless Sensor Network (WSN) [2]. The open network is insecure and vulnerable to attacks such as flooding attacks and Denial-of-Service (DoS) attacks, which waste energy and channel capacity [3, 4]. The Internet of Things (IoT) integrates nearly all aspects of everyday life, including things like smart homes and healthcare systems. Several utilities can talk to each other and work together to provide a wide range of services. The nodes in the IoT are considered mobile because controlling stationary nodes is easy as compared to dynamic networks. Therefore, efficient utilization of node energy cannot use properly for communication of devices. Many of these connected devices will be very small and cheap, so they can be placed wherever they can be useful. This intelligent nature of things leads to an inclusive range of applications, including home automation, smart agriculture, healthcare, military

surveillance smart cities, building management, healthcare, energy and transportation [1, 5]. The example of IoT is mentioned in Figure 1. Here the heterogeneous IoT devices or nodes are communicate with individually other with the help of internet signals.

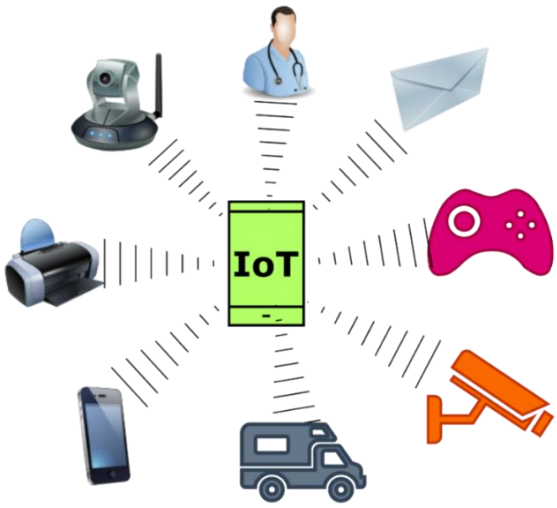

Figure 1. Example of IoT

The utilisation of IPv6 made the Internet of Things more appreciable and practicable, in addition to making its acceptance simpler [6]. Therefore, because IPv6 has a wider address space, it makes it possible for more computers to connect to the internet. As a result, they are able to communicate with each and every node in network. Additionally, machines have restricted amounts of energy, processing power, and computational capacity. In order to keep a close eye on and handle any situation, the resource-constrained sensing devices have been linked to the internet over IPv6 networks. So, for the future of Internet of Things applications, these devices need to be able to talk to each other in a safe way. The network attacker repeatedly injects incorrect information or sends out undesired packets in addition to impairing routing performance [4, 6]. Due to the widespread interest in this paradigm, low-power and lossy networks (LLN), including wireless sensor networks, have been widely deployed. A high loss rate and poor throughput are characteristics of networks with substantial resource constraints, such as energy, memory, computation, and their communication links. This is due to data being dropped or retransmitted. The efficient usage of requirements cannot be handled by the routing methods in use [5]. As a result, a full stack of standard protocols has been created, including the 6LowPAN protocol and the IEEE 802.15.4 standard protocol for the communication layers in WPANs (wireless personal area networks). The protocol is based on IPv6 and is known as RPL (Routing Protocol for Low Power and Lossy Networks) [6]. Examples of things that are connected to the IoT include a person who has an implanted heart monitor, farm animals that have biochip transponders, and automobiles that have built-in sensors to inform the driver when the tyre pressure is too low. Any other natural or man-made object that is capable of being furnished with an IP address and the capability to transmission data over a network is referred to as a network node. The increase in the number of smart nodes will result in an increase in the amount of upstream data generated by the nodes, which will give rise to new concerns around data privacy, data sovereignty, and security. The malevolent node that are capable to manipulates the source route header of the received packets is called a Hatchetman Attacker [7]. The Hatchetman attacker sends a large number of invalid packets with errors to genuine nodes. The genuine nodes are aware from the attacker presence in network. The invalid packets are dropped by genuine nodes by reply with an excessive number of error messages back to the DODAG root [6]. The congestion in network is responsible for energy consumption and poor channel capacity utilization [8].

2. ROUTING PROTOCOLS IN IOT

Routing is the process of determining the quickest path for a message to take from sender to receiver. The routing protocol is critical to communication in IoT [9, 10]. Because the nodes in the Internet of Things move at different speeds, it is impossible to establish a stationary link. The IoT routing protocol is specifically designed for use in dynamic scenarios. Figure 2 shows the classification of routing protocols.

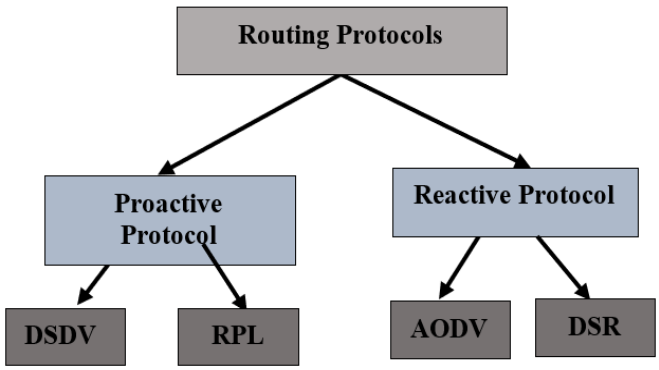

Figure 2. Routing protocols of IoT

The network nodes perform routing actions in accordance with the routing protocol chosen. Only by establishing a strong link between the sender and the receiver can a strong link be established in that network. As a result, the number of packets that a network receives decreases. The flooding of routing packets is also increasing network latency.

2.1 Proactive routing

Proactive routing protocols, also known as reactive routing protocols, establish connections in a table-like fashion, meaning that request packets or connection establishment packets are forwarded to all nearby nodes, and a record of nodes that are part of the final link established with the destination is kept. In a dynamic network, the nodes keep a record of the routing information as well as a record of nodes that have previously sent data to the destination. The proactive routing protocol has the advantage of instantly establishing a connection between sender and receiver, and it is also more reliable for link nodes that are stationary or do not change. The main disadvantage of this type of protocol is that if node movement is fast or nodes in the network are constantly moving, the sender and other nodes must keep track of all routes. It necessitates a substantial amount of memory. DSDV and RPL are the example of proactive o routing protocols. For data transfer, the RPL route employs Destination Oriented DAG (DODAG) [6, 9].

2.2 Reactive routing

Reactive routing protocols establish connections on-demand, which means that no request packets or connection establishment packets are forwarded to all nearby nodes, and no record of nodes that are part of the final link established with the destination is kept. It is also called as, on-demand routing protocols. In a dynamic network, nodes do not keep track of routing information or nodes that have previously sent data to the destination using this routing approach. Instantly establishes a connection between sender and receiver is the advantage of reactive routing protocol and it is also more reliable in rapidly changing topology environments. The main disadvantage of this type of protocol is that if node movement is slow or nodes in the network are stationary, they must repeatedly establish connections in order to send data across the network. Ad Hoc On Demand Distance Vector Routing (AODV) and Dynamic Source Routing (DSR) are the examples of reactive routing protocols.

3. TYPES OF ATTACK IN IOT

Attackers or malicious nodes in IoT are engaging in a variety of malicious activities, which have resulted in damage to fundamental facets of security such as integrity, confidentiality, and privacy [10]. The attackers are also classified into a variety of categories, and the types of attackers that are represented by these categories are mentioned in the network [11, 12]. IoT nodes' inherent characteristics in network applications imply that any resource loss or compromise, regardless of the cause, is a malicious attack initiated by the adversary class and will have a critical negative impact on the entire network. Intelligent opponents who want to sabotage, harm, or steal network messages may be active around nodes placed across a very vast region. The network will suffer more losses because of the node compromise. IoT sensor nodes set themselves apart from other networks due to their resource-constrained nature. The only goals of the attacker are to cause packet loss, use up network bandwidth or connection capacity between mobile sensor nodes, and use a fake identity to talk on the network.

3.1 Active attack

It monitors and listens on an unauthorised communication channel while simultaneously modifying the data stream that is transmitted over that communication channel. These malicious actors are actively engaging in behaviour that is harmful to the network. The active attacks that are displayed here come in a variety of flavours [13, 14].

3.1.1 Blackhole attack

A packet consumption attack is what is known as the blackhole attack in network. The attacker identify the sender which participates in routing and send data to the receiver and reply fake route information to the sender by attacker. Then, if that happens, the attacker will lose all of their data, and the performance of the network will suffer.

3.1.2 Sybil attack

The network nodes perform routing actions in accordance with the routing protocol chosen. Only by establishing a strong link between the sender and the receiver can a strong link be established in that network. As a result, the number of packets that a network receives decreases. The flooding of routing packets is also increasing network latency.

An attacker node can replicate itself, and its presence can be felt in multiple locations. It seeks to address problems associated with fault tolerance by focusing on multiple identities for other nodes, distributed storage, multipath routing and topology in the networks. These malicious actors conceal their true identities and take over the identities of nearby nodes in order to carry out their attacks.

3.1.3 Flooding attack

In the network, a malevolent node that possesses a large radio transmission range and a significant amount of power sends "HELLO" packets to a number of mobile nodes that are not in range of another. During the time that data is being transmitted to the receiver or base station, the wounded nodes are attempting to communicate with the flooding attacker, which leads to increased spoofing [14].

3.1.4 DoS attack

This may have an impact at various layers, including the physical layer, and the DoS attack is the jamming and tampering, when unintentional node failure or malicious node attacks cause any event that reduces the network's capacity. Malicious nodes target any occurrence that breaks down the network. Even though collision, unfairness, and exhaustion are going to take place in the link layer, a DoS attack is going to be guaranteed [15].

3.1.5 Hatchetman attack

An attack of this kind might also rely on the utilisation of laptop-class adversaries; that is, adversaries with a couple of orders of magnitude higher machine power than traditional IoT nodes, and with the confirmed identities of legitimate sensing element nodes that are operating within the network [7]. In addition, distributed denial of service attacks in an extremely sensing element network may lead to the exhaustion of the target node's limited energy resources as a result of the massive flow of requests that are directed towards it. This can happen if the network is extremely sensitive. In an extremely sensor network, a distributed denial of service attack is also referred to as a distributed energy-exhaustion attack. As a result of this, we have a tendency to call this type of attack by a different name. The solution against Hatchetman attacker is provided by the SHLPLN scheme.

3.1.6 Wormhole attack

This type of attack is the most severe type of attack that can be carried out on a IoT network. In this type of attack, two attackers who are working together to carry out the attack can use private high-speed networking to transfer packet at one location and replay it at the other location. This type of attacker not follows the safe path but choose path where attacker exist in network. As a result, this can be utilised against any and all communications in order to guarantee authenticity and confidentiality.

3.2 Passive attack

Passive attackers are not particularly harmful at first, but once they steal all genuine node information, they become more dangerous. However, it is possible for an unauthorised person to monitor and listen to communication channels,

which does not affect the functioning of any communication systems. Because of their stoic demeanour, it is extremely difficult to locate these kinds of attacks. Because it is difficult for them to reorganise themselves, the passive attackers do not continuously shows activeness in network or perform malicious actions into the network [16].

3.2.1 Attack on privacy

In this attacker malicious node can easily collect information from a sensor network because there is a large amount of information that is available by remote access, and the information can be accessed remotely. In this section, various intrusions into privacy are well-defined.

3.2.2 Eavesdropping and monitoring

A common type of attack is for a data adversary to be able to quickly find communication control information for sensor network design that both affects privacy protection and has information. This type of attack is known as a communication control information disclosure.

3.2.3 Traffic analysis

In this attack the messages are encrypted before being sent, there is still a high probability that communication patterns will occur due to the activities of the nodes. This could result in information being altered, which would be detrimental to the IoT network.

4. ISSUES IN IOT SECURITY

A IoT could be a unique network with unique constraints when compared to a traditional computer network. To begin, in order to make sensing element networks economically viable, nodes energy computation, and channel capacity are limited. Second, unlike ancient networks, nodes are typically positioned in easily accessible areas, posing a higher chance of physical attack. Third, nodes interact with their physical environments as well as individuals, posing new security challenges [17, 18]. Because of these constraints, it is difficult to apply current security approaches directly to the realm of IoT networks. As a result, to build reliable security mechanisms while using ideas from these security techniques, it is necessary to first perceive and comprehend these constraints [17, 18]. Figure 3 shows the issues in IoT. Limited resources and unreliable communication are the main issue and these issues are further classified. The security is the issue that resolved by proposed security scheme.

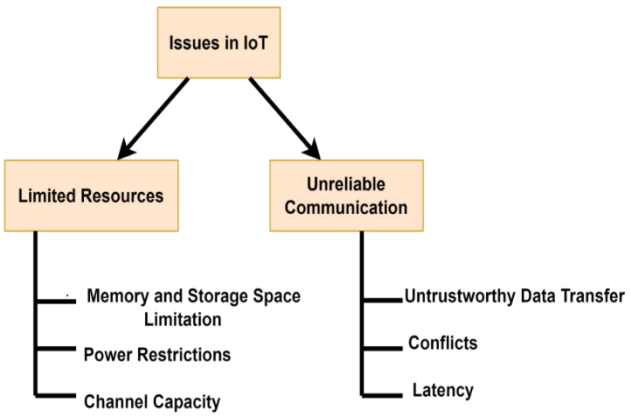

Figure 3. Issues in IoT

4.1 Limited resources

All security methods necessitate a certain number of resources for implementation, such as code space, memory, and energy to power the sensor. However, these resources are currently severely limited in an extremely small communication device. The primary parameters are as follows [19]:

4.1.1 Memory and storage space limitation

A node could be a device with very little memory and code storage space or having large memory space. To create a good security mechanism, the protection rule's code size must be limited.

4.1.2 Power restrictions

The most significant limitation of wireless sensing element capabilities is energy. Once nodes are deployed in a large network, they cannot be simply replaced (high operational cost) or recharged (high cost of IoT devices). As a result, the battery charge in the nodes should be maintained in order for the individual sensor nodes and the entire network of sensing elements to last longer.

4.1.3 Channel capacity

The IoT nodes operate in a wireless environment, and bandwidth in a wireless environment is limited. Channel capacity utilisation can improve network throughput and reduce network latency.

4.2 Unreliable communication

In actuality, a further danger to the security of sensing elements is unreliable communication. A detailed protocol, which is dependent on communication in turn, is crucial to the network's security. The following are the main factors [20]:

4.2.1 Unreliable data transfer

Packet-based routing in the WSN is connectionless and hence intrinsically unstable. Packets may be lost due to channel issues or be created at nodes that are incredibly congested. As a result, data packets on the network are lost or missing. Furthermore, broken packets are a result of erratic wireless connectivity.

4.2.2 Conflicts

Communication should remain unstable, even if the channel is. This frequently results from the open nature of the IoT. When packets collide during a transfer, conflicts might happen, and the transfer may be unsuccessful. This might be a serious drawback in a network that is very dense.

4.2.3 Latency

Due to increased network delay caused by multi-hop routing, network congestion, and node processes, synchronisation between nodes will be difficult. Whereas the protection method relies on important event reports and scientific key distribution, synchronisation problems are typically crucial to node security.

4.3 Prerequisites for security

Security is the primary issue after successful data receiving in Internet of Things (IoT). Some Internet security parameters,

such as availability, confidentiality and integrity have also become important parameters in the IoT. Some attacks, like data exploitation, are easy to do with nodes or other devices that are easy to hack. The possibility of an attack can be reduced by implementing privacy enhancements such as using a pseudonym instead of a plain ID for IoT objects. Access and communication are restricted to the trust object only. IoT networks must meet certain requirements in order to provide secure communication. These requirements provide defense against attacks on data transmitted over the network [21, 22].

4.3.1 Data confidentiality

When data flows from multiple intermediate nodes, the likelihood of data leakage increases. To ensure data confidentiality, an encrypted dataset is used, with only the recipient being able to decrypt the data to its original form. Data confidentiality is essential for protecting data from prying eyes.

4.3.2 Data integrity

The term "data integrity" refers to the fact that data received by the receiver should not be altered or modified in any way. The original data is altered by an intruder or a harsh environment. The intruder may modify the data to meet its needs and send it to the receiver. The goal of data integrity is to make sure that all of the data in a network is correct and hasn't been changed in any way.

4.3.3 Data authentication

This is the process of determining whether or not the communication between nodes is what it claims to be. It is critical for the receiver node to verify that the data has been received from an authenticated node. This indicates that you are receiving data from the correct node or receiver. The cryptographic technique confirms a network node's reliability in receiving data.

4.3.4 Data availability

Data Availability means that the services are always available, even in the event of certain attacks such as blackhole attacks, wormhole attacks, and others. The availability of resources also ensures the reliability of communication in a dynamic network. Because of its extremely limited resources, maintaining high availability has become a major task in the design and deployment of IoT. (i.e. limited energy, memory, computing, and bandwidth) [23].

4.3.5 Identification of the source

Some applications use the sink node's location information for data transmission. It is critical to grant security access to location information. Malicious nodes can control unencrypted data by sending false signal strengths or replaying signals.

4.3.6 Self-organization

There is no fixed infrastructure in a dynamic IoT network with an open connection. As a result, each node is autonomous, has adaptability to various situations, and maintains self-organizing and self-healing properties. This is a significant challenge for IoT security.

4.3.7 Data accuracy

Data freshness refers to the fact that each message sent over the channel is new and fresh. It ensures that no node can replay previously sent messages. This can be solved by including a time-related counter to check the data's freshness [24].

5. LITERATURE SURVEY

The previous work that has already been done in the field of secure IoT communication is mentioned in this section. The security from attacks is provided by each author, and each one was contributed to resolve attacker problem:

Pu et al. [7] describe a "Hatchetman attack" on RPL-based LLNs. Hatchetman attacker node tampers with a received packet's source route header to send erroneous, incorrectly-routed packets to trustworthy nodes. Because it is unable to relay incorrect packets using the error route, the legitimate node drops them. The identified research gap by the authors does not concentrate on enhancing routing performance while there are attackers present in the network. The research lacks the identity of the Hatchetman attacker [7].

Sharma et al. [25] proposed an investigation of Hatchetman's performance on RPL-6LoWPAN networks was suggested by When an unauthorised node alters the header of a packet it receives and subsequently sends faulty packets to authorised nodes with the incorrect route information, it is committing a Hatchetman attack. Unavoidably, authorised nodes will drop packets and reply to DODAG's root with several error signals. This leads unauthorised nodes to lose a lot of packets, and the excessive amount of error messages wears down the node's energy and communication bandwidth. The gap in the research is they only focuses on detection rather than how networks behave after deployed security measures. The effects of a Hatchetman assault on RPL-based IoT networks are demonstrated by simulation results, not by the effectiveness of security measures in RPL-based Internet of Things networks.

Arshad et al. [26] proposed a lightweight protocol that is effective at both detecting malicious Sybil nodes and conserving energy. It guards against fake and stolen identities for both mobile and stationary or non-stationary IoT networks. Computes are offloaded to resourceful nodes to extend network lifetime. This study focuses on increasing node energy efficiency and preventing nodes from running out of power. By removing trust-related operations from the root node, it also hopes to lower compute and data storage costs. Third, find and isolate the Sybil attack node that is based on IoT. The research gap is dropping information of packets missing in the research. In the case of a drop, the energy information is less than that of a flood of packets in a network

Soni and Sudhakar [27] proposed a L-IDS technique for WSN-assisted IoT black hole attack was proposed by Sensor nodes connected by wireless links exchange packets and data routing. RPL is the routing protocol for IPv6. The suggested IDS verified the existence of the blackhole attacker and put a halt to his nefarious activities. The research on packet dropping attacks and attacker infection has not been evaluated. The research gap is that attacker energy use is not assessed. The research is solely concerned with packet dropping rather than flooding.

Thulasiraman and Wang [28] proposed a trust-based security architecture for RPL was created by and can identify external assaults in mobile IoT. The architecture was based on widely used security mitigation strategies including nonce identity, timestamping, and network whitelisting, but this research is the first to combine these factors for RPL. Among

the paths already established in the IoT dynamic network, RPL can select the best one. The choice based on the receiving node will notify the DODAG root of the source route header issue. The research gap is the presence of attackers only, which is only decided by the trust calculation, with no other criteria decided for cross-checking the trust value count. The normal routing performance was not evaluated.

Khan and Herrmann [29] proposed an Intrusion detection system (IDS) to identify network attacks on distributed systems, such as DoS attacks. Performance of standard routing is not assessed. An IDS uses signatures to scan network traffic for signs of attacks. An anomaly-based IDS searches for behavioural anomalies that could be signs of assaults. Unlike signature-based IDS, they can discover novel attacks. They frequently report phoney attacks. How much each node can be relied upon, as well as how powerful its average received signal is. Priorities are the foundation of the trust value notion, although it is unclear how they affect performance. Unwanted packet injection by a DoS attacker was not assessed.

A straightforward approach for encrypting data with a private key was proposed by Chaudhry [30]. Modify the bundle architecture. Any routing protocol can be used with this process by altering the client information. These keys are kept in each base node together with the bit's individual ID. Using an arbitrary key from the vast encryption key, messages are jumbled.

Alsadi and Mohan [31] developed a plan in which a wireless transceiver with multi-directional antennae was attached to it. The data is safely transmitted from the reception node to the fusion centre. To prevent eavesdropping, this study proposes to develop an intelligent Internet of Things node that can identify the safest channel and deliver data over it. The suggested node's internal transceiver allows for direct communication with other network nodes. Any information the fusion centre has after sending its CW signal is sent as a backscattered signal through its semi-passive tag.

Conti et al. [32] proposed a SPLIT secure and extensible routing protocol built on RPL. The suggested method sends and receives attestation data using RPL's route discovery and periodic topology maintenance messages. While reducing overhead and device attestation time, SPLIT scales attestation. SPLIT makes advantage of the RPL protocol to aggregate attestation reports from devices in large-scale IoT networks efficiently (in terms of time, energy, and network overhead). For linking devices over RPL, the SPLIT IoT routing protocol is a reliable and scalable choice. The main gap is not only to measures the flooding malicious behaviour of attacker and effect of attacker infection on resources of communication. The few researchers highlight the classification or learning based security schemes [33-36].

6. PROBLEM IDENTIFICATION

The primary issue the IoT faces is unauthorized access to send and receive information. The basic idea behind a Hatchetman attack is to change the source information of a received packet in order to make invalid packets with an error route. These invalid packets are then sent to the legitimate nodes that were chosen as targets. The nodes can contain any sort of information and can be easily modified or read by the reader. Acquisition of data is also possible other than transmission. Next, flooding creates a problem in the IoT. It clarifies when traffic volume is high and unnecessary exhaustion of node/s buffer space takes place. Once we connect the IoT device to an Android, it becomes an open network and can be easily discovered by other devices for communication.

1) Once we connect an IoT device to an open network that other devices can easily find and use to talk for communication.
2) IoT nodes do not keep their software and devices up-to-date. Once the attacker finds the devices, they can easily access them.
3) When a malicious user with unauthorized access can change or delete the data, this is called data loss. Once the attacker gets hold of an account, it can upload certain software that will give him control of any device that comes into contact.
4) The assaulter can also work as a third body (because it is not a sender or receiver and normal forwarder) and can directly flood information from a next node, and the node drops it because it doesn't know about that.
5) Flooding from excessive traffic is also a problem. Data drop, overhead, and routing performance, as usual, are improved.
6) Because attackers are stealthier, their malicious actions are more difficult to detect. This is due to the attacker node's deceptive behaviour, which includes discarding received packets and sending several error messages in response, as well as the unlawful packets it delivers to legitimate nodes to cause them to attack the network.

7. SECURITY FORM HATCHETMAN ATTACKER IN LOW POWER AND LOSSY NETWORK(SHLPLN)

The Hatchetman's attack is highly furtive and grimmer to detect. This is due to the attacker node's deceptive behaviour, which includes discarding received packets and sending several error messages in response, as well as the unlawful packets it delivers to legitimate nodes to cause them to attack the network. Since every action a node takes requires coordination with other nodes, which is impossible without communication, the proposed SHLPLN identifies Hatchetman attacks on the basis of significant packet flooding, which uses up unnecessary resources like bandwidth and energy from other normal nodes. The research is divided into three modules:

1) Hatchetman attack Module
2) Previous RPL scheme Module
3) Security from Hatchetman Attacker in Low Power and Lossy Network (SHLPLN) module

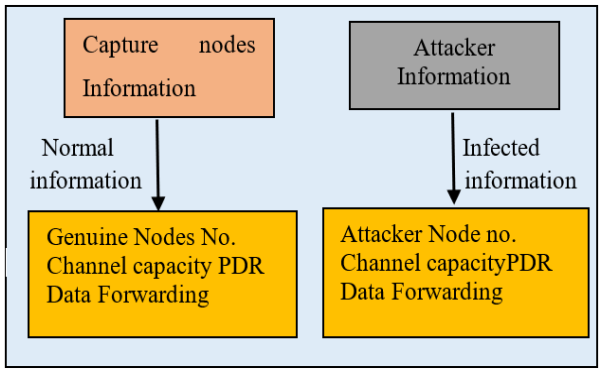

Figure 4. Simple model of SHPLN

The normal profile includes normal transmission (TCP with FTP transmission and UDP with CBR transmission). It also contains the network's packet flow path. This information is obtained prior to the attacker node entering the network. The malicious node then enters the network in place of a Hatchetman attack.

It captures information from the normal profile and infects the susceptible node in the network via detention flooding information of node/s in networks, after which the malicious node configures the flooding rate, malicious node port number and percentage of vulnerability to measure attacker infection. If the detailed network's and abstract network's probing ports are the same, the attacker node sends infected packets to all neighbour nodes and infect the whole network. A security scheme matches some information about suspicious nodes, shown below in Figure 4.

The Intrusion Information gathers information from both the normal profile and the attacker node and compares it to detect an intrusion. It looks for information such as the attacker's node number, port number, attacker symptoms, and time of intrusion.

7.1 SHLPLN attacker detection and prevention

The proposed algorithm finds Hatchetman attacks based on high packet flooding, which uses up bandwidth and energy from other normal nodes that aren't needed. This is because coordination between nodes is needed for every operation a node can do, and coordination is impossible without communication**.** Every aspect of the Internet of Things' future must be created, examined, and given the go-ahead before being extensively used. The Internet of Things as a whole will be impacted by high dimensionality, which will result in issues and difficulties in both space and time.

1) Hatchetman assault Node misbehavior can result in service disruption or even network failure. In the proposed work, we proposed a new protection scheme against node misbehavior during Hatchetman attacks. Security from Hatchetman attacker in Low Power and Lossy Networks (SHLPLN) system identifies the attacker by maintaining the profile of each node that participates in communication. The attacker's profile does not match that of normal nodes, and only infection is discovered in the case of an attacker. In this plan, the routing behavior of nodes is first looked at, and then the right, well-thought-out security plan is used to stop all of the malicious behavior of Hatchetman attacker nodes and make the network more stable. Find malicious node that causes Hatchetman attack and take away the Hatchetman attacker from the network. The clear flow mentioned in Figure 5.

2) Higher standards for safety, dependability, security, energy efficiency, performance, robustness, cost effectiveness, etc. will be imposed as the IoT develops in large-scale and pervasive directions. This implies that every aspect of the Internet of Things' future must be created, examined, and given the go-ahead before being extensively used IoT develops in large-scale and pervasive directions.

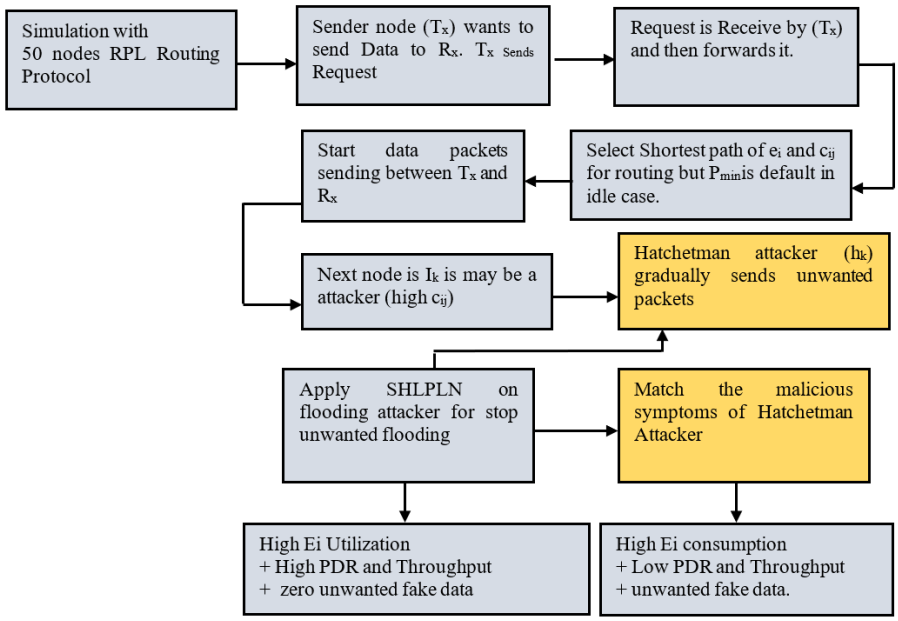

Figure 5. SHLPLN for Hatchetman Attacker Identification

The performance of previous and proposed scheme measured by different performance metrics. The performance metrics are showing better results in SHLPLN. In IoT devices having limited processing capability and memory but few devices having sufficient amount of memory for processing and forwarding information to other nodes. Nodes in network can't move but forwarding the all information to sink node for control the other devices and proper functioning.

The Hatchetman attacker is flooding the packets with unnecessary information, and because of that, the limited bandwidth and energy of nodes are wasted trying to handle the unwanted packets in the network. The IoT network is secure from attackers by applying the proposed SHLPLN scheme that not only detects but also prevents the network from attackers.

1) First of all, the sender broadcasts the request to establish a connection between the sender to receiver through RREQ (Route Request), and the intermediate nodes that receive RREQ also generate RREP (Route Reply) packets.
2) If the link in the network is not available, then the RERR

(Route Error) message is generated.

3) If the attacker is a Hatchetman, flooding is high and continuously increases in network and energy depletion is high. nodes are
4) The main focus on the energy of nodes e_i or channel capacity c_{ij} between the nodes. The c_{ij} is on priority. Only *normal* and *high* parameter consider for measure cannel capacity.
5) The high parameter measurement is depended on the heavy flooding or flooding is more than expected.
6) The target of attacker are resources like bandwidth and limited energy source.
7) In the presence of an attacker, the energy consumption of nodes is increasing but the number of data packets received is very small.
8) The flooding of unwanted data is enhancing the energy consumption to find an attacker.
9) The attacker does not receive any packets in the network, but only sends them.
10) The attacker's packet flooding is enhanced according to time constraint and watched by W_k node.
11) After attacker confirmation P_t Broadcast h_t malicious activity to all alive nodes or remaining nodes in network.
12) If the flooding is normal then no need to identified attacker, communicate with other nodes normally and sends data to destination.
13) Finally measure the effect of attacker and security scheme by metrics.
14) All metrices showing improvement in performance in presence of Hatchman attacker in network.

7.2 SHLPLN algorithm

Behavioral Analysis of Node for Hatchetman attack prevention in Low Power dynamic network. First of all, mention the inputs and use symbolic representation.

Inputs:

P_t: IoT Device or Node
T_x: Transmitter Node
I_k: intermediate node
R_x: Receiver node
h_t: Hatchetman attacker node
A_{nn}: training the network
W_k: behaviour analyser node
th_l: response threshold 70% of PDR
P_{min}: Shortest Path
e_i: energy of node or power
bh_i: I_k node behaviour(abnormal, normal,)
ch_{ij}: capacity ofchannel between I_k node
Ψ: radio range 550m^2
r_p: RPL routing protocol

Output: throughput, PDR, routing overhead, latency, energy consumption

Procedure:

P_t node in network deployed
T_x call route module
generate (T_x, R_x, r_p)
if I_k in Ψ &I_k!= R **then**
generate table t_k
Intermediate node/s (I_k)forward packet (t_k, id_k, r_p)
else if I_k in range(Ψ)&I_k== R_x& path > 1 **then**
compare (max (e_m, e_i), max (ch_{im}, ch_{ij})) by R_x
select i_j path // *normal*
send acknowledgement to T_x
send (T_x, R_x, data)
else
R_x not in range or Select P_{min}
end if
/ First Attack Identification then Prevention */*
W_k observe behaviour of neighbours/ I_x
if I_k is h_k under the current path **then**
junk messages generating by (h_k)//*high* c_{ij}
junk messages reach to P_t
if Junk message receives by P_t **then**
Unwanted flooding effect on resource utilization.
Intentionally consume network resource
junk messages forward to next hop.
Packet forwarding and receiving is affecting.
Consumes almost complete bandwidth.
end if
W_k depict the activity of k node // The c_{ij} high value based on the heavy flooding.
W_k captures profile of I_t // Attacker is an intermediate node
if message! = network profile & I_k behaviour == abnormal & $PDR_i < th_l$ **then**
I_t as h_k (confirm intermediate node is attacker node (Hatchman Attacker)
block h_t node by W_k
All P_t node broadcast blocking message to
if T_x receives blocking message, **then**
request to call R_p for generate route message
find route from T_x to R_x without participation h_k
end if
end if

The attacker information is important for detection of abnormal behaviour during the routing in network.

Table 1. Genuine nodes and attacker nodes analysis by W_k

Transmitted (T_x)	Next Hop (I_x)	Packets Forwarding	Channel Capacity (c_{ij})	Received (R_x)	PDR
T_1	True	True	Normal	R_1	>70
T_2	True	True	Normal	R_2	>70
T_3	True	True	Normal	R_3	>70
T_4	***False***	***True***	***High***	-	***<70***
T_5	True	True	Normal	R_5	>70

The all possibilities of channel capacity consumption with receiving are mentioned in Table1. The 70% PDR is the target and next hop information is false but channel capacity is high, means attacker/s are flooding in network.

Although SHLPLN security using RPL is feasible, a Hatchetman attack mechanism is presented to identify malevolent nodes. Therefore, creating a system to secure the RPL is a crucial component and an unsolved task in the Internet of Things space. To ensure that the state changes of the network components and the devices responsible for

network connectivity are managed in accordance with the security requirements, routing security must be ensured. The creation of threat models and the execution of a thorough threat analysis serve as important pre-requisites to the establishment of the security mechanism. Hatchetman attack detection is a useful technique for simulating security flaws and all potential attack starting points. All nodes participate significantly in node-to-node communication because they are either dependent base routes or collaborative forms. This gives one indicator of the issue: security. So, in this section, we create an algorithm for monitoring and defending against denial-of-service assaults. We initialize all variables first, then examine how denial-of-service assaults behave.

A Hatchetman attack is occurring if any node delivers undefined type packets at an abnormally high rate. However, the severity of that kind of attack is determined by reviewing historical data using a method that identifies the attacking node. After that, we apply a security scheme to remove malicious actions. The communication network is strengthened by the historical analysis base detection and upcoming real-time protection due to security concerns.

8. SIMULATION PARAMETERS

The simulation parameters shown in Table 2 for all proposed SHLPLN network. The same parameters are also taking for RPL and Hatchmean attacker. The evaluation uses the simulation model, which is based on network simulator-2 (ver-2.31) [37]. The network's topological structure or total grid layout, the nodes' mobility, the configuration of the service provider and receiver, protocol information of application layer and other layers and rest of all using the ns-2 simulator for simulation.

Table 2. Simulation parameters using for simulation

Parameters	Measures
Simulator	NS-2.31
Grid layout	1000m*1000m
Number of nodes	50 (mobile)
Traffic type over TCP	FTP
Traffic type over UDP	CBR
Time in seconds	5000, 500
Size of packets	1024 bytes and 512 bytes
Number of traffic connections	10
Nodes maximum Speed	Random and maximum (30 m/s)
Transmission range(meters)	500
Ideal Energy	0.0001 joules
Sense Power	0.0175 joules
Transmission Energy	0.2 joules
Receiving Energy	0.1 joules

9. RESULT ANALYSIS

The performance comparison of protocols is mentioned in this section and the performance of proposed SHLPLN protocol is better. Here, only security scheme applied on 10% and 20% flooding of data because maximum up to 20% infection of data SHLPLN identified in the presence of attacker in network. The attacker infection is very high in normal routing but SHLPLN or proposed scheme are able to handle it properly. The all performance metrices are showing better performance of proposed scheme in low power and lossy network.

9.1 PDR analysis

The successful packets receiving determine the real performance of any security solution. In this PDR analysis simulation shown in Figure 6, a scenario with 50 mobile nodes is built, and the packet delivery ratio represents the proportion of current packets transmitted by the sender and received by the authentic receiver. A greater packet delivery ratio indicates that we will do better than the competition. According to our findings, if a misbehaving node enters the network at that time and the packet delivery ratio is low because of a severe flooding infection, the node will be unable to transfer data packets to their destination. The Detection and Prevention in Low Power and Lossy Network (SHLPLN) approach prevents attackers from acting maliciously. The suggested course of action is to fully eradicate the attacker's infection.

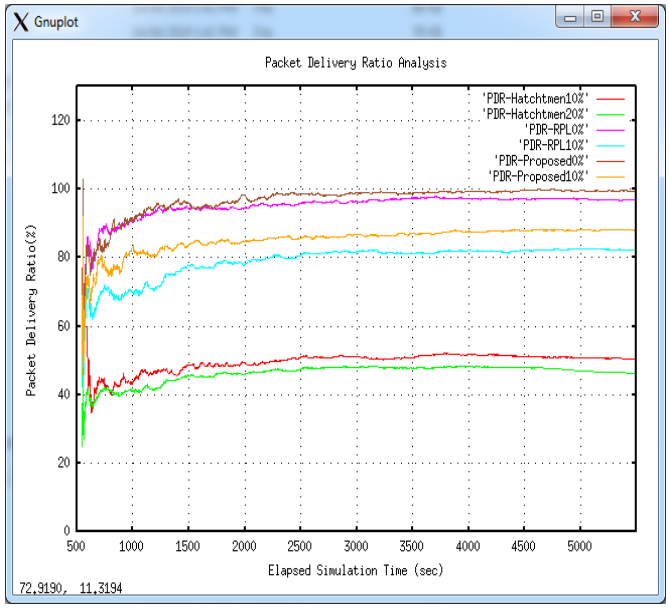

Figure 6. PDR analysis

9.2 Energy consumption analysis

The number of nodes in a network determines the availability of a scarce communication resource, i.e., energy or battery power. The energy usage of both methods is shown in Figure 7. Here, the proposed Detection and Prevention in Low Power and Lossy Network (SHLPLN) protocol is measured along with the energy usage in the case of the attacker protocol. The X-axis in this graph shows simulation time, and the Y-axis shows the total energy used by the network's 50 nodes. This graph shows the energy usage for a potential attacker, the old security method, and the suggested security method. The proposed protocol has a significantly lower energy consumption because it only uses energy for communication. The proposed protocol is performing significantly better now in terms of energy consumption. Better energy efficiency is also a factor.

9.3 Throughput analysis

The rate at which messages are successfully sent over a communication channel is known as "throughput," sometimes known as "network throughput. It is measured in terms of time

units, or per second. This information may be transmitted over a logical or physical link or via a specific mobile ad-hoc network node. The throughput is often expressed in bits per second (bit/s or bps), although it can also be expressed as data packets per second or time slots. In comparison to earlier RPL, the Hatchetman attack, and detection and prevention in low-power and lossy networks (SHLPLN) systems, the suggested security scheme performs noticeably better. An attacker's throughput performance is shown in Figure 8 (measured in bytes/seconds) is insufficient to use the entire capacity of the funnel. Due to significant network flooding caused by the attacker infestation, packet loss is increasing. The planned security plan is performing better than expected.

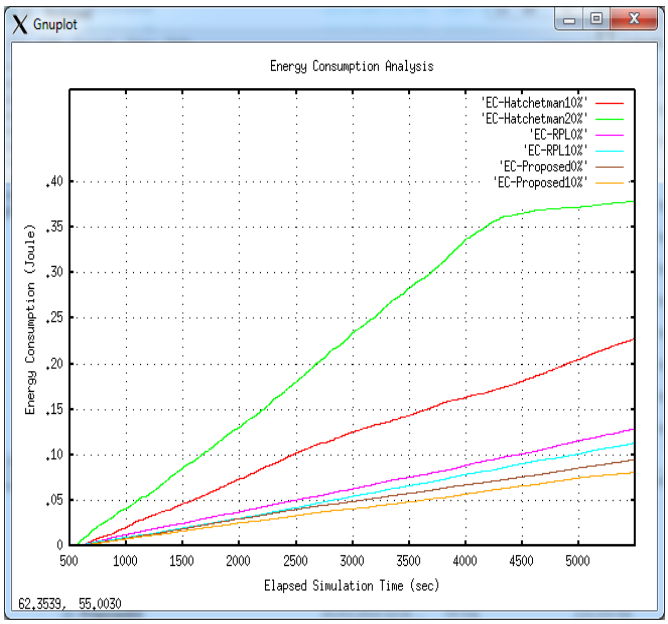

Figure 7. Energy consumption analysis

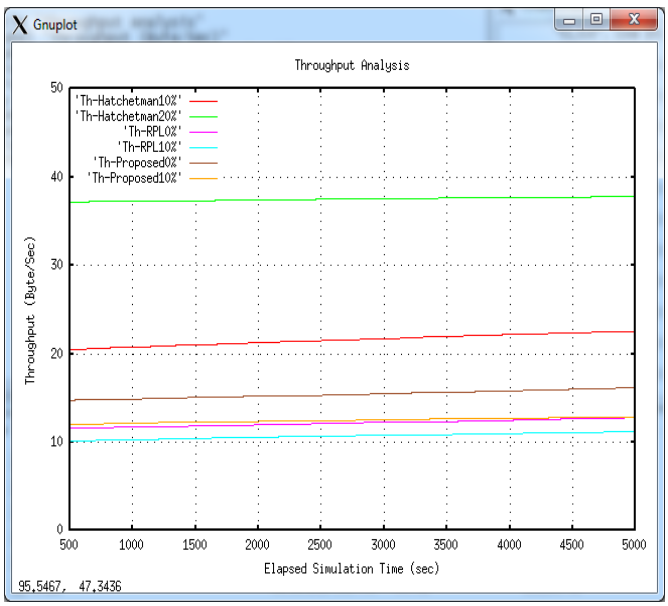

Figure 8. Throughput analysis

9.4 Attacker packets flooding analysis

Hello packets or routing packets means the total number of routing packets sent on the network for connection establishment and starts data receiving from sender. The routing overhead is the ration of data received and total routing packets. If the overhead value is lower than 1, it means overhead for data transmission is less and more amount of data packets we can send in network.

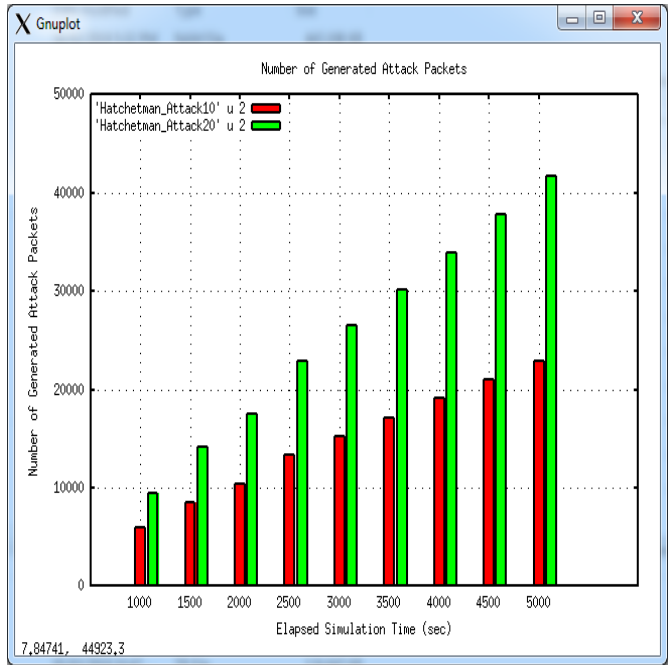

Figure 9. Attacker flooding analysis

The aim research fulfil by maximum network utilisation through actual data transmission rather than through routing packets. In simulation case mentioned in Figure 9, we analyse all three cases of network routing packet analysis, and we get if a misbehaving node enters the network, the network routing overhead suddenly increases. That means the sender must establish a new route from source to destination but can't find it, so recursively searching for the destination increases the unwanted load on the network. This graph only depicts the attacker flooding in the network over time.

10. CONCLUSION AND FUTURE WORK

Attacks on networks are popping their heads as one of the most major problems in developed as well as developing countries, and hence, IoT device simulation should be able to generate the same scenario in a research lab. The routing among the IoT devices is the major problem because of the presence of malicious nodes in the network. The attacker's behaviour is to directly attack on primary resources like bandwidth and battery capacity of nodes. There is a novel attack known as the "Hatchetman attack" that drains the energy of every device within the network and consumes the bandwidth. Ice simulation should be able to generate the same scenario as that present in a research lab. The routing among the IoT devices is the major problem due to the presence of malicious nodes in the network. The proposed Prevention in Low Power and Lossy Networks (SHLPLN) prevents attacker flooding and improves network bandwidth utilization. The proposed scheme reduces overhead, and the attacker in the network completely blocks the inflow of unwanted packets and improves channel utilization. SHLPLN for Hatchetman attack improves packet receiving. By distinguishing and removing suspicious nodes from the network, appropriate

methodology is used for implementation and increases network security and performance. The recently developed techniques or previous schemes are not an effective security technique. That means routing is performed smoothly and also the previous scheme enhances the overhead, but this overhead is controlled by SHLPLN. The only routing protocol is not able to recognize fake and malicious information in a network. SHLPLN is able to establish a secure route and send data among the nodes. The previous scheme is showing an improvement in performance but is not able to improve performance. The preventer watches the malicious nodes and also applies strict action on them. The SHLPLN shows a 10% improvement in PDR and gives 15Bytes/second more throughput (Th-proposed0%). The proposed 10% attacker infection rate gains 5 bytes per second. The performance of the proposed protocol saves up to 0.26 joules of energy compared to the attacker and 0.05 joules compared to the normal RPL. The ns-2 simulator is used for measure the performance of network. The proposed scheme not only keeps attackers from getting into the network, but it also makes RPL routing work better.

In the future, propose the Global Positioning System (GPS) to confirm the locations of nodes. This novel approach will store the locations of all nodes and let us compare the performance of the SHLPLN to the future location-based scheme in IoT.

REFERENCES

[1] Atzori, L., Iera, A., Morabito, G. (2010). The internet of things: A survey. Computer Networks, 54(15): 2787-2805. https://doi.org/10.1016/j.comnet.2010.05.010

[2] Solanki, A., Singh, A.K., Tanwar, S. (2023). Blockchain Technology for IoE: Security and Privacy Perspectives. CRC Press, pp. 22-40.

[3] Nair, R., Sharma, P., Singh, D.K. (2020). Security attacks in internet of things. In Fog, Edge, and Pervasive Computing in Intelligent IoT Driven Applications. John Wiley & Sons, pp. 237-261. https://doi.org/10.1002/9781119670087.ch14

[4] Soni, G., Chandravanshi, K. (2021). Security scheme to identify malicious maneuver of flooding attack for WSN in 6G. In 2021 8th International Conference on Signal Processing and Integrated Networks (SPIN), Noida, India, pp. 124-129. https://doi.org/10.1109/SPIN52536.2021.9566066

[5] Goyal, P., Sahoo, A.K., Sharma, T.K., Singh, P.K. (2021). Internet of Things: Applications, security and privacy: A survey. Materials Today: Proceedings, 34: 752-759. https://doi.org/10.1016/j.matpr.2020.04.737

[6] Winter, T., Thubert, P., Brandt, P., Hui, J., Kelsey, R., Levis, P., Pister, K., Struik R., Vasseur, J., Alexander, R. (2012). RPL: IPv6 routing protocol for low- power and lossy networks. RFC 6550, IETF.

[7] Pu, C., Song, T. (2018). Hatchetman attack: A denial of service attack against routing in low power and lossy networks. In 2018 5th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud)/2018 4th IEEE International Conference on Edge Computing and Scalable Cloud, Shanghai, China, pp. 12-17. https://doi.org/10.1109/CSCloud/EdgeCom.2018.00012

[8] Soni, G., Sudhakar, R., Pathak, K. (2018). Cluster based techniques for eradicating congestion in WSN aided IoT: A survey. International Journal of Emerging Technology and Advanced Engineering, 8(12): 166-172.

[9] Dawson-Haggerty, S., Tavakoli, A. (2009). Overview of Existing Routing Protocols for Low Power and Lossy Networks. Internet Engineering Task Force (IETF) Internet Draft: draft-ietf-roll protocols survey- 07.

[10] Suchitra, C., Vandana, C.P. (2016). Internet of Things and security issues. International Journal of Computer Science and Mobile Computing, 5(1): 133-139.

[11] Daud, S., Gilani, S.M.M., Riaz, M.S., Kabir, A. (2019). DSDV and AODV protocols performance in Internet of Things environment. In 2019 IEEE 11th International Conference on Communication Software and Networks (ICCSN), Chongqing, China, pp. 466-470. https://doi.org/10.1109/ICCSN.2019.8905256

[12] Al-Karaki, J.N., Kamal, A.E. (2004). Routing techniques in wireless sensor networks: A survey. IEEE Wireless Communications, 11(6): 6- 28. https://doi.org/10.1109/MWC.2004.1368893

[13] Al-Qudsy, Z.N., Fadhil, Z.M., Jaleel, R.A., Zahra, M.M.A. (2023). Blockchain and 1D-CNN based IoTs for securing and classifying of PCG sound signal data. Fusion: Practice and Applications, 12(2): 28-41. https://doi.org/10.54216/FPA.120203

[14] Ab Kadir, M.Z.A., Algrnaodi, M., Al-Masri, A.N.A. (2021). Optimal algorithm for shared network communication bandwidth in IoT applications. International journal of wireless and ad hoc communication, 2(1): 33-48. https://doi.org/10.5281/zenodo.5215451

[15] Elhoseny, M., Yuan, X., Abdel-basset, M. (2021). Energy aware enhanced krill herd algorithm enabled clustering for unmanned aerial vehicles. International Journal of Wireless and Ad Hoc Communication, 3(1): 17-25. https://doi.org/10.54216/IJWAC.030102

[16] Rayen, S.J. (2021). Survey on smart cane for visually impaired using IoT. Journal of Cognitive Human-Computer Interaction, 1(2): 81-85. https://doi.org/10.54216/JCHCI.010205

[17] Sadique, K.M., Rahmani, R., Johannesson, P. (2018). Towards security on Internet of Things: Applications and challenges in technology. Procedia Computer Science, 141: 199-206. https://doi.org/10.1016/j.procs.2018.10.168

[18] Alsaadi, E., Tubaishat, A. (2015). Internet of Things: Features, challenges, and vulnerabilities. International Journal of Advanced Computer Science and Information Technology, 4(1): 1-13.

[19] Sharma, A., Tayal, S., Bansal, R., Verma, S. (2020). Energy efficiency techniques in heterogeneous networks. Journal of Cybersecurity and Information Management, 2(1): 13-19. https://doi.org/10.54216/JCIM.020102

[20] Embarak, O.H., Zitar, R.A. (2023). Securing wireless sensor networks against DoS attacks in Industrial 4.0. Journal of Intelligent Systems & Internet of Things, 8(1): 66-74. https://doi.org/10.54216/JISIoT.080106

[21] Sicari, S., Rizzardi, A., Grieco, L.A., Coen-Porisini, A. (2015). Security, privacy and trust in Internet of Things: The road ahead. Computer networks, 76: 146-164. https://doi.org/10.1016/j.comnet.2014.11.008

[22] Dragomir, D., Gheorghe, L., Costea, S., Radovici, A. (2016). A survey on secure communication protocols for IoT systems. In 2016 International Workshop on Secure Internet of Things (SIoT), Heraklion, Greece, pp. 47-62.

https://doi.org/10.1109/SIoT.2016.012
[23] Abdelmonem, A., Mohamed, S.S. (2022). Deep learning defenders: Harnessing convolutional networks for malware detection. International Journal of Advances in Applied Computational Intelligence, 1(2): 46-55. https://doi.org/10.54216/IJAACI.010203
[24] Myvizhi, M. (2023). Neutrosophic MCDM model for evaluation and selection best 5G network architecture. International Journal of Advances in Applied Computational Intelligence, 4(1): 8-18. https://doi.org/10.54216/IJAACI.040101
[25] Sharma, G., Grover, J., Verma, A., Kumar, R., Lahre, R. (2022). Analysis of hatchetman attack in RPL based IoT networks. In International Conference on Emerging Technologies in Computer Engineering (ICETCE 2022), Jaipur, India, pp. 666-678. https://doi.org/10.1007/978-3-031-07012-9_55
[26] Arshad, D., Asim, M., Tariq, N., Baker, T., Tawfik, H., Al-Jumeily OBE, D. (2022). THC-RPL: A lightweight Trust-enabled routing in RPL-based IoT networks against Sybil attack. PLoS One, 17(7): e0271277. https://doi.org/10.1371/journal.pone.0271277
[27] Soni, G., Sudhakar, R. (2020). A L-IDS against dropping attack to secure and improve RPL performance in WSN aided IoT. In 2020 7th International Conference on Signal Processing and Integrated Networks (SPIN), Noida, India, pp. 377-383. https://doi.org/10.1109/SPIN48934.2020.9071118
[28] Thulasiraman, P., Wang, Y. (2019). A lightweight trust-based security architecture for RPL in mobile IoT networks. In 2019 16th IEEE Annual Consumer Communications & Networking Conference (CCNC), Las Vegas, NV, USA, pp. 1-6. https://doi.org/10.1109/CCNC.2019.8651846
[29] Khan, Z.A., Herrmann, P. (2017). A trust based distributed intrusion detection mechanism for internet of things. In 2017 IEEE 31st international conference on advanced information networking and applications (AINA), Taipei, Taiwan, pp. 1169-1176. https://doi.org/10.1109/AINA.2017.161
[30] Chaudhry, S. (2018). An encryption-based secure framework for data transmission in IoT. In 2018 7th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO), Noida, India, pp. 743-747. https://doi.org/10.1109/ICRITO.2018.8748523
[31] Alsadi, A., Mohan, S. (2018). Improving the physical layer security of the Internet of Things (IoT). In 2018 IEEE International Smart Cities Conference (ISC2), Kansas City, MO, USA, pp. 1-8. https://doi.org/10.1109/ISC2.2018.8656930
[32] Conti, M., Kaliyar, P., Rabbani, M.M., Ranise, S. (2018). SPLIT: A secure and scalable RPL routing protocol for Internet of Things. In 2018 14th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), Limassol, Cyprus, pp. 1-8. https://doi.org/10.1109/WiMOB.2018.8589115
[33] Nandan, D., Kanungo, J., Mahajan, A. (2016). An Efficient VLSI architecture design for antilogarithmic converter by using the error correction scheme. In International Conference on Signal Processing (ICSP 2016). https://doi.org/10.1049/cp.2016.1445
[34] Suma Priya, D.S.V., Esther Rani, D., Pavan Shankar Sai, A., Konda Babu, A., Nandan, D. (2020). A review on the importance of machine learning and artificial intelligence in real life problem solving. Journal of Computational and Theoretical Nanoscience, 17(9-10): 4336-4339. https://doi.org/10.1166/jctn.2020.9072
[35] Nandan, D., Mahajan, A., Kanungo, J. (2017). An efficient antilogarithmic converter by using 11-regions error correction scheme. In 2017 4th international conference on signal processing, computing and control (ISPCC), Solan, India, pp. 118-121. https://doi.org/10.1109/ISPCC.2017.8269661
[36] Singh, M.K., Kumar, S., Nandan, D. (2023). Faulty voice diagnosis of automotive gearbox based on acoustic feature extraction and classification technique. Journal of Engineering Research, 11(2): 100051. https://doi.org/10.1016/j.jer.2023.100051
[37] The CMU Monarch Project, The CMU Monarch Extensions to the NS Simulator. http://www.monarch.cs.cmu.edu/, accessed on February 20th, 2018.