


RESEARCH

Open Access



Secure and efficient transmission of data based on Caesar Cipher Algorithm for Sybil attack in IoT

Aditya Sai Srinivas Thuluva¹, Manivannan Sorakaya Somanathan², Ramasubbareddy Somula³, Sankar Sennan⁴ and Daniel Burgos^{5*} 

* Correspondence: daniel.burgos@unir.net

⁵Research Institute for Innovation & Technology in Education (UNIR iTED), Universidad Internacional de La Rioja (UNIR), 26006 Logroño, La Rioja, Spain

Full list of author information is available at the end of the article

Abstract

The Internet of Things (IoT) is an emerging concept in the field of information technology. IoT can integrate any real-time entity with another, using sensing, computing and communication capabilities to offer enhanced services in everyday life. In this article, IoT-based patient health monitoring is considered for use in IoT sensors deployed in devices. These devices are attached to the body of the patient for timely tracking of his or her health condition. During data transfers from devices connected to the patient's body to the doctor, the data may be susceptible to security threats. IoT devices are subjected to many routing attacks, like blackhole, greyhole, Sybil, sinkhole and wormhole attacks. Sybil attacks are the most dangerous routing attacks. This type of attack involves stealing the identities of legitimate nodes; this, in turn, leads to information loss, misinterpretation in the network and an increase in routing disturbances. Hence, in this paper, we propose the use of the traditional Caesar Cipher Algorithm (CCA) along with the lightweight encryption algorithm (LEA) and the Received Signal Strength Indicator (RSSI) to detect and prevent Sybil attacks in an IoT environment. The proposed algorithm detects the false node in a particular path by announcing the attack to another node. It also prevents the attack by choosing an alternative path by which to forward data packets to the desired users. To ensure authentication, privacy and data integrity, the lightweight encryption algorithm with a 64-bit key is used with AODV as the routing protocol.

0.0.0.1 Index terms Internet of Things (IoT) Sybil attack Received Signal Strength Indicator (RSSI) Lightweight encryption algorithm (LEA) Caesar Cipher Algorithm (CCA)

1 Introduction

The Internet of Things (IoT) [1–3] is a new concept that describes how real-time entities are integrated within a network. Real-time entities can be sensors, actuators, Radio Frequency Identification (RFID) tags [4], mobile phones, wearable devices and so on. In this paper, we consider an IoT-based patient health monitoring system. Many people are dying from chronic illness [5] due to air and water pollution, unhealthy diet

habits or lack of physical exercise. Based on a 2016 World Health Organization survey, nearly 2.6 million people are suffering from being overweight, 4.9 million from lung cancer, 4.4 million people from cholesterol problems and so on. By 2026, these diseases could affect 64 million people [6].

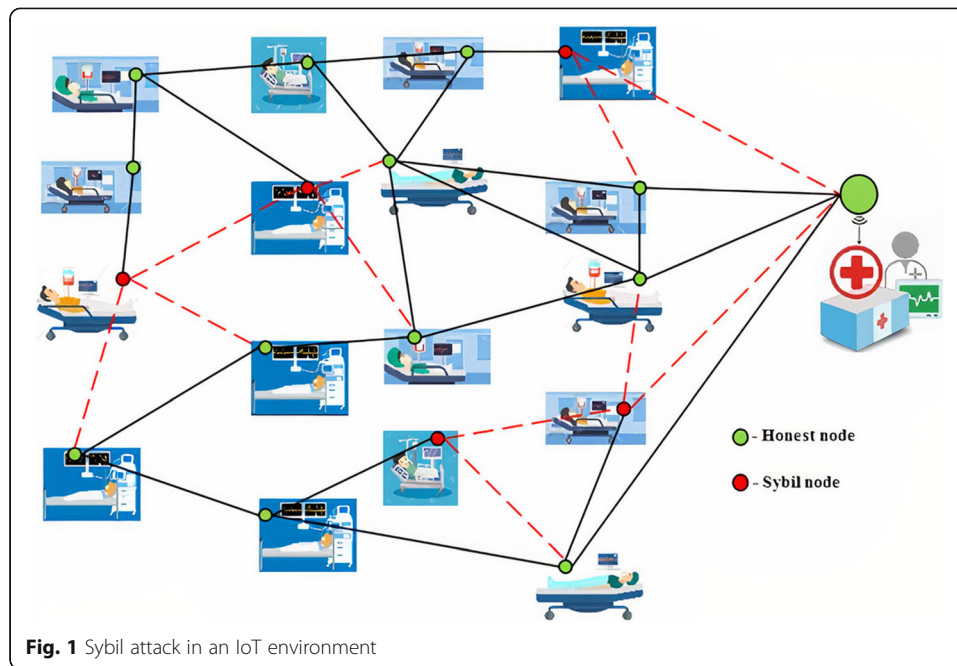
Sensors can monitor vital signs, such as heart rate, sugar levels and body temperature. These sensors are directly attached to the body of the patient or embedded in a device. A patient's family members are often very concerned about the health condition of the patient, and there should always be one person present to look after him or her. But with the help of an IoT-based patient health monitoring system, the patient's health condition can be directly monitored by a doctor through an Internet connection. Devices that are connected to the body of the patient will have sensors that will continuously sense the patient's health condition. RFID tags can be implanted under the patient's skin to read their condition [7].

In the past, in order for the patient's sugar levels, blood pressure and glucose levels to be measured, the patient would need to be taken to a hospital or healthcare centre. But today, for example, if there is any sudden increase or decrease in a patient's heart rate, sugar levels, body temperature or blood pressure, then sensors will notify the doctor about the change. This data can be transmitted through the Internet from the patient to the doctor and vice versa. End users can access the information through Web or mobile devices from anywhere in the world through the Internet. When data is being transmitted in a wireless medium, there is a chance that routing attacks [8], such as blackhole attacks, greyhole attacks and Sybil attacks, will take place. In a blackhole attack [9, 10], the attacker node publicises as if the destination node has the shortest route and then collects the packets without redirecting them to the target node. A greyhole attack [11] is a variation of a blackhole attack in which selected packets are forwarded to the destination and remaining packets are dropped without being sent to the destination. A Sybil attack [12] is one of the most dangerous types of routing attacks. In a Sybil attack, a malicious or attacker node will create many fake identities to affect the overall network performance. Sybil nodes are capable of generating false reports, spamming users with messages and causing breaches in privacy.

This paper discusses Sybil attacks in an IoT-based patient monitoring system. Figure 1 shows the presence of a Sybil attack in an IoT environment. The small red nodes represent Sybil nodes or malicious nodes, and the green nodes are normal nodes. All the nodes are interconnected with one another. During data transmission from one normal node to another, i.e. from patient to doctor or vice versa via a normal node, data reaches its destination without any loss of integrity. However, if the data is transmitted via a Sybil node [13–15], then the data is subjected to incorrect report generation, loss or spam, or it can be misinterpreted.

The paper's key findings are stated as follows:

1. The effective detection of the Sybil nodes that are in the network is made by the received signal strength.
2. The AODV routing protocol is used for electing the optimal route, and this route is optimised by the distance from one node to another and each node's residual energy. AODV is also used for preventing the network from being harmed by the Sybil nodes by broadcasting information about the Sybil nodes to all the legitimate nodes.



3. The confidentiality of shared information is improved with the help of the CCA with the LEA.
4. Furthermore, this type of Sybil detection and secured data transmission is used in applications in the real-time world. For example, here, the network is considered a hospital environment, and each patient comprises one node for transmitting information about the patients.

1.1 Sybil attack

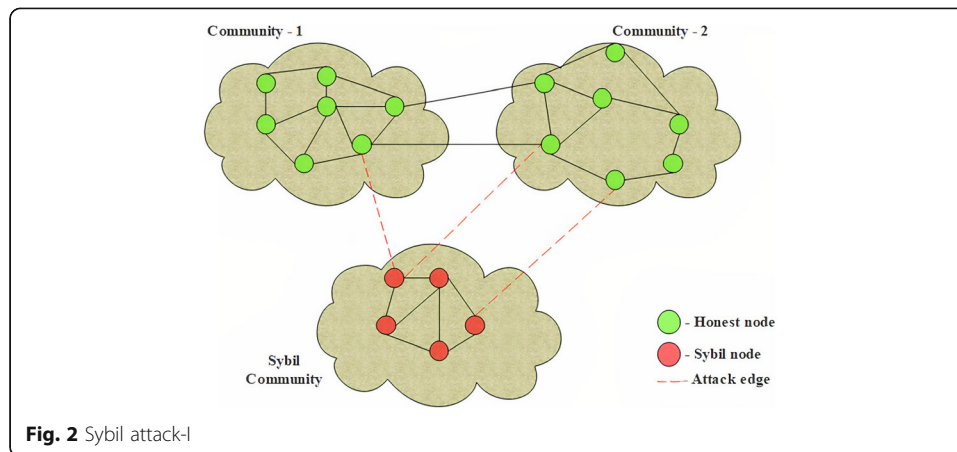
Sybil attacks [12] possess several identities and are given to the remaining nodes. But it is a node replication and is essentially a spoofing of the IDs of the nodes. Sybil attack was graded into Sybil attack-I, Sybil attack-II and Sybil attack-III.

1.1.1 Sybil attack-I (SA-I)

SA-I is viewed as creating social links, within the Sybil region. Here, Sybil nodes are connected with other Sybil nodes as shown in Fig. 2. In this attack, Sybil nodes make limited social connections to normal or honest nodes, i.e. attack edges are less. This attack mainly occurs in social and sensing domains. For example in an online voting system, attackers can have fake identities and can manipulate overall rating or votes.

1.1.2 Sybil attack-II (SA-II)

SA-II is different from SA-I. Here, social connections can be established from Sybil nodes to honest nodes or normal nodes as shown in Fig. 3. This attack mainly occurs in the social domain. More attack edges will be present in between Sybil and normal nodes. The main aim of SA-II is to distribute spam messages, malware and ads. For example in OSNs, this attack can manipulate users' reviews, i.e. attackers can change all negative reviews/comments to positive comments or vice versa.



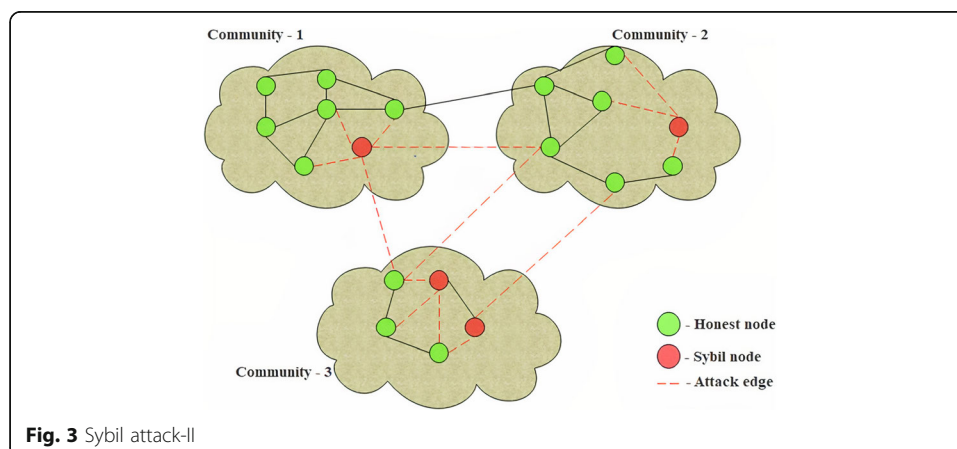
1.1.3 Sybil attack-III (SA-III)

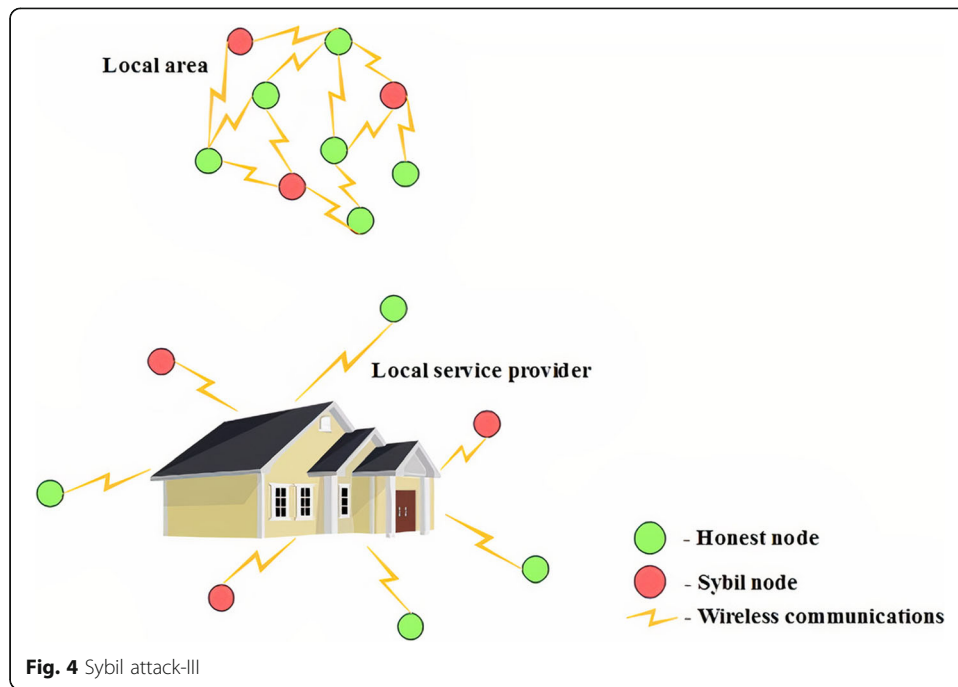
SA-III mainly focuses on the mobile domain. This attack is similar to SA-II. Users will be moving from one place to other so the topology of the network changes frequently as shown in Fig. 4. Due to this, the effect of this network lasts for a short amount of time.

The remainder of the paper is structured as follows: Detection and prevention methods for dealing with Sybil attacks are addressed in Section 2. In Section 3, the classification of Sybil attacks is outlined. In Section 4, the system architecture is discussed. Section 5 describes how the Sybil node is avoided while generating the route from the source to the destination. The results are discussed in Section 6. Lastly, the paper is summarised in Section 6.

2 Related work

Amuthavalli et al. proposed the Random Password Creation (RPC) [16] method, which uses three parameters: node id, time delay and password. Two routing tables, one RPC database and another routing table, are constructed using source and destination nodes. These two tables are compared to determine if the three parameters match. Then, the node is deemed to be a normal node if it is not a Sybil node. RPC controls the position of the node for preventing the Sybil attack. This is because these Sybil nodes are directly detected by checking the ID (identification).





Thus, the RPC method prevents the Sybil attack. However, no alternative route selection is required in case of route failure.

Bedi and Singh proposed the Bee Colony Optimization (BCO) [17] method to detect and prevent a Sybil attack that occurs over Low-Energy Adaptive Clustering Hierarchy (LEACH)-based Wireless Sensor Networks (WSNs) when this attack has resulted in some concerns while creating the route over the network. This algorithm finds the optimised route during a Sybil attack. Thus, this method detects the Sybil attack efficiently. However, it finds difficult to create a route in the network.

Xiao proposed a scheme to identify Sybil attacks in wireless networks. Channel-based authentication [18] exploits the spatial variability of a radio channel. This authentication method degrades the system's performance when it depends on the spatial information that is associated with channel path loss. Thus, this method can detect Sybil attacks efficiently. However, the system performance will be degrading.

Ng et al. [19] proposed DeeRaI with CuI as a method for detecting DoS attacks using information taken from radial basis functions. CuI was developed using the NSL KDD and UNSW NB15 datasets to aid in the optimization of DeeRaI network weight values. Thus, this method is well suitable for detecting DoS attacks. However, it does not work with Sybil attacks.

Sarigiannidis et al. presented the Rule-Based Anomaly Detection System (RADS) [20] for identifying Sybil nodes and for monitoring and detecting Sybil nodes that are present inside the network. The RADS method relies on ultra-wideband (UWB) ranging detection and does not allow any information sharing between the sensor nodes. The RADS performs distance checks, and if variations occur, it raises the alarm and blacklists the Sybil node. It provides minimum communication overhead, high detection precision and a low false security alarm rate. The minimum

communication overhead of this system is maintained by lightweight UWB ranging-based detection. The RADS requires an analysis of its energy usage. Thus, this approach can detect a Sybil attack. Hence, low false alarm rate needs analysis on energy consumption.

Singh et al. introduced Trust-Based Sybil Detection (TBSD) [21]. This TBSD scheme depends on the manipulative trust values that are sent by adjacent sensor nodes. Every node in the cluster calculates the adjacent node's trust value and sends it to the cluster head. A node is declared as a Sybil node when the node has a trust value that is less than the threshold value. The distance between the sensor nodes is not considered in this work. Thus, this approach can detect Sybil nodes. However, the distance between the sensor nodes is not considered in this work.

Alsaedi et al. presented the Energy Trust System (ETS) [22] to identify Sybil nodes in a group of nodes. The ETS employs multi-level detection, which is related to the position and identity verification. The trust algorithm is also implemented based on the energy of every node. The data aggregation mechanism and the avoidance of feedback exchange are used for improving the efficiency of the network. The ETS approach requires less energy consumption. The total packet send and throughput are not discussed in this work. Thus, this approach can identify Sybil attacks using ETS. However, some parameters like throughput are not discussed.

Vamsi et al. detected the Sybil attack using sequential analysis [23]. It takes a node-centric approach, which works through two stages: evidence collection and validation. In the first stage, the behaviour of each node is analysed by monitoring the activities of neighbouring nodes, and this evidence (i.e. behaviour) is given as the feedback to the next level. In the second stage, the collected evidence is validated by sequential analysis to detect if the neighbour node is an attacker node or not. Thus, the low processing and communication overhead are the main benefits of this system.

Palak presented the fuzzy membership function [24] (i.e. trapezoidal membership function) for preventing Sybil attacks. In this function, fuzzy membership function values are used for updating the detection and F-MEM values in every iteration. The node is determined to be either a Sybil node or a legitimate node based on the trust factor of the fuzzy system. The backup routing paths are not considered in this work. If it is not considered, the packet loss occurs in the presence of route failure. Thus, the membership function is used to detect Sybil attacks. Hence, no backup routing path is not considered.

Dhamodharan et al. presented a combination of CAM-PVM and MAP [25] to detect and eliminate the attacker node from the network. The CAM-PVM algorithm is used for detecting Sybil activity that is present in the network. The MAP is then used for avoiding the Sybil node. Data loss is avoided by detecting the Sybil nodes. This MAP comprises unicast and multicast communication through the network. The time consumption of the MAP algorithm is high.

Singh et al. [18] detected the Sybil node by using the Trust-Based Identity Detection (TBID) [26] mechanism. Initially, the sensor nodes are divided into clusters, and the TBID assigns trust values for each node. The trust value of a node decreases when the

node changes the identification has unlike the adjacent nodes. These trust values are sent to the CH. The node is detected as an attacker node only when the trust value is less than the predefined threshold. Thus, this approach can detect the Sybil node efficiently using the TBID mechanism. However, the energy consumption of this entire system is not discussed in this work.

Jan et al. presented a lightweight detection mechanism for Sybil attack detection, which depends on the obtained signal strength of the packets [27]. This is the implementation of a centralised clustering-based hierarchical network. The sensor nodes of the network are categorised based on their own energy levels. The node with the higher energy level is then aided to detect the Sybil nodes at the base station, and it also prevents the Sybil nodes from selecting the cluster head. The normal nodes of each cluster are identified by their energy levels, geographical location and previous selection history. The optimal number of clusters in each round is identified to preserve the energy consumption and network lifetime. Thus, this method higher energy node is used to detect the attack. Hence, sometimes an unbalanced cluster is occurred inside the network, because the node in the current round may become the cluster head in the next round.

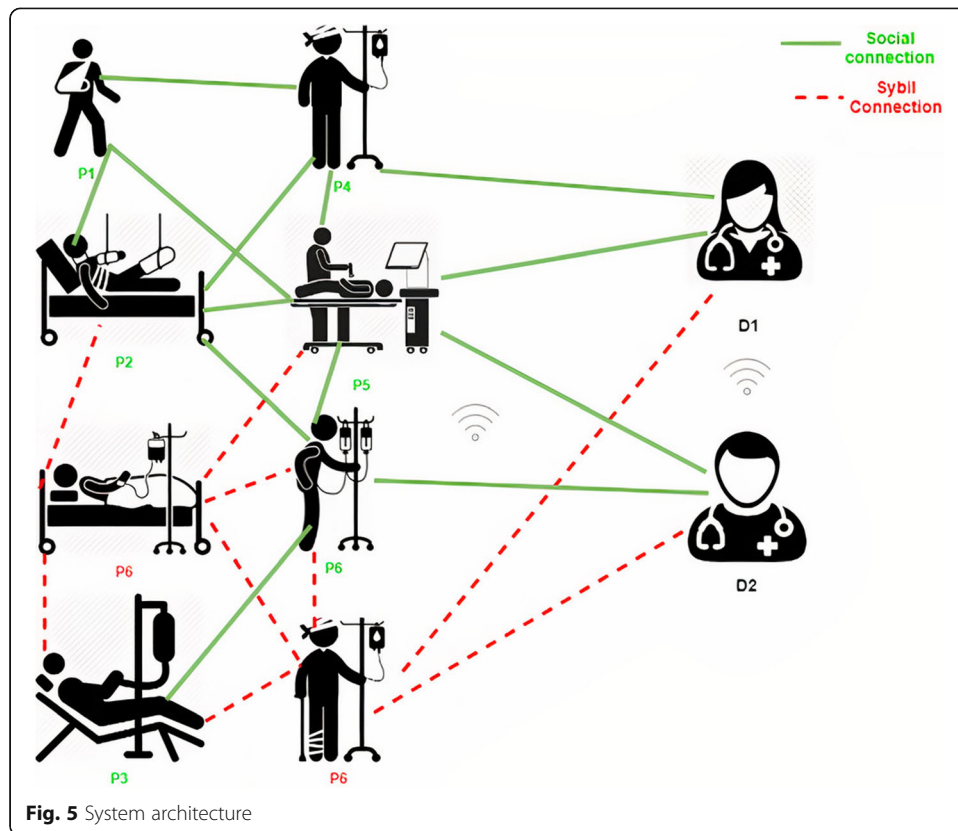
3 System architecture

In an IoT-based patient monitoring system, the patient is the important entity. Devices that contain sensors are attached to the patient's body. These sensors monitor vital signs, such as blood pressure, body temperature, heart rate and sugar levels, from the patient's body. These values are sent to the doctor via a wireless communication technology, such as Wi-Fi. During data transmission, the data can be subjected to a Sybil attack. Attackers can access the data and inject spam or alter the message, which could lead to harm to or even the death of the patient. For example, the system could be set up such that a doctor is notified when the patient's body temperature reaches 100 degrees. But if attackers drop the packets or send them to the wrong person, then the doctor will not be notified about the patient's health condition, which could lead to severe problems.

In this paper, we are considering SA-II. Figure 5 shows patients $P = \{P1, P2, P3, P4, P5 \text{ \& } P6\}$ and doctors $D = \{D1, D2\}$. Eight patients are connected with sensors, but due to a Sybil attack on the network, there are only six IDs. One patient P6 node is the original, and the other two P6 nodes are duplicates. The RSSI-LEA-AODV method is used to detect and prevent an attack.

4 Caesar Cipher Method

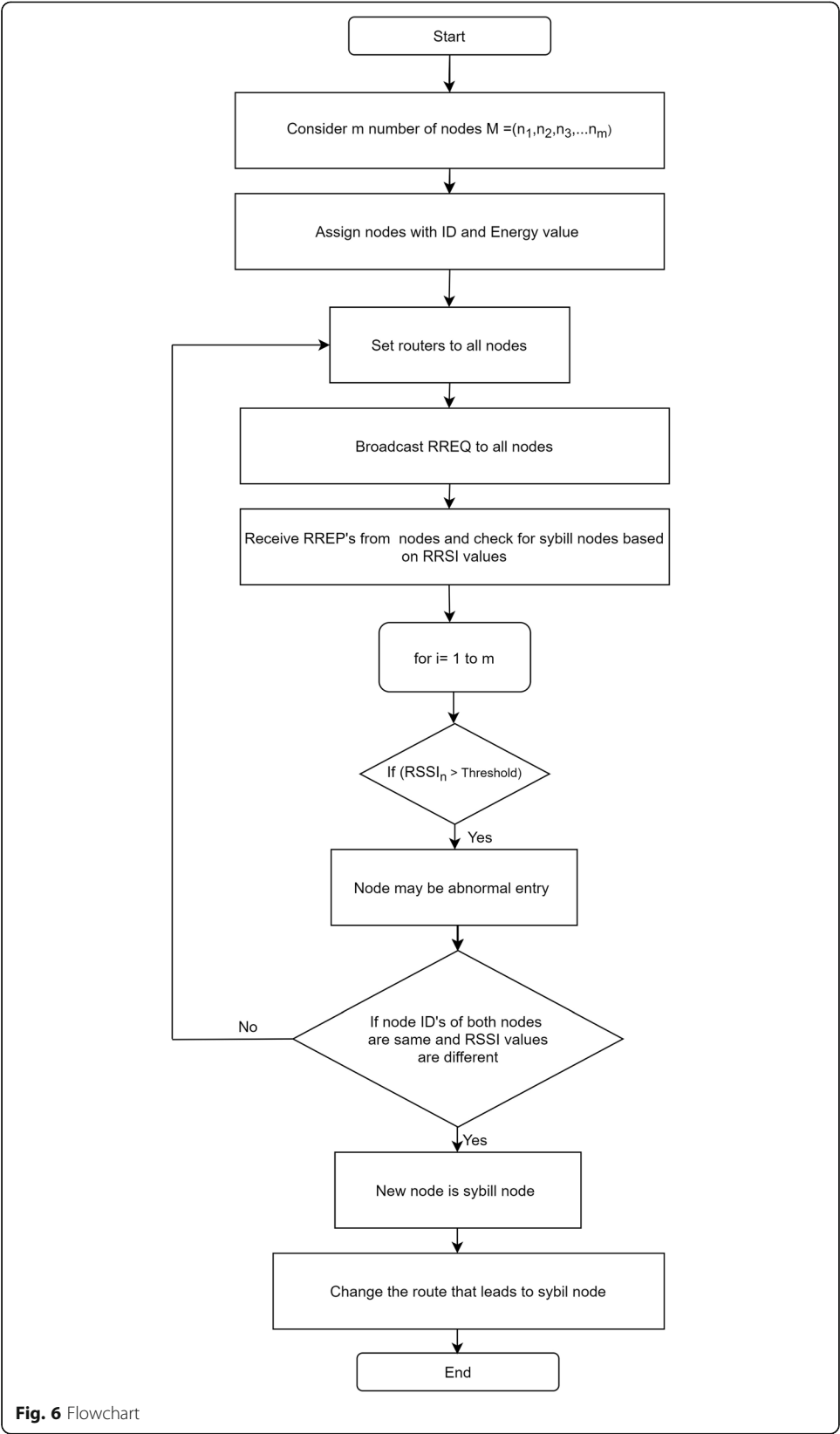
This method is a variation of the Received Signal Strength Indicator (RSSI) and the lightweight encryption algorithm (LEA) using the AODV routing protocol. By enabling the RSSI, the Sybil attack that is present in the network is detected, and then the information about the Sybil nodes is sent to the remaining nodes in the network. Based on that information, the Sybil nodes are avoided during the creation of a route from one node to another with the AODV routing protocol. AODV is a reactive routing protocol with proactive routing protocol features. It detects the optimal route by focusing on the distance between nodes and the residual energy of



each node. The overall process of RSSI-LEA-AODV is illustrated as a flowchart in Fig. 6.

The process of RSSI-LEA-AODV is given as follows:

1. A set of sensor nodes is considered and deployed randomly.
2. Initial information about the network is identified, such as the positions of the sensor nodes, the distance between the sensor nodes, the residual energy and the received signal strength of each sensor.
3. Based on the received signal strength, the Sybil nodes are detected, and these nodes are added to the Sybil nodes list. Then, this information is transferred to other legitimate nodes.
4. The confidentiality over the network is made by the Caesar Cipher Algorithm along with the lightweight encryption algorithm.
5. The encrypted data is transferred through the network by AODV routing. The AODV routing is optimised by focusing on distance and energy values.
6. The Sybil nodes are avoided in AODV routing while generating the route from one node to another.
7. The node that has less energy is not considered in the AODV route generation. If it happens, AODV once again creates the route from the source to the destination.
8. The data packets are transferred to the destination.
9. This process is continued until the full iteration count is reached.
10. Finally, the performance is analysed in terms of alive nodes, dead nodes, energy consumption, throughput and total packet send.



4.1 Received signal strength-based Sybil node detection

The differences between the normal and attacker nodes are identified by the RSSI [28, 29]. The RSS of a node is very low when the node enters into another node's radio range. Whenever an attacker creates a new Sybil node, the signal strength from other nodes will be high. The RSSI is validated by the transmitter's ID. For example, the destination ID first receives the message from the source ID, and then the destination ID receives the message from a different source ID. Based on this, the destination is identified by the data from the source ID. This RSSI is used for better defence against Sybil attacks. The formula for finding the received signal strength is given in Eq. (1).

$$R_i = RSSI(d_0) - 10n \log(d/d_0) \quad (1)$$

where R_i is the received signal strength of node i , $RSSI(d_0)$ is the received signal strength at a reference distance, n is the constant and d is the Euclidean distance.

During data transmission, every node calculates and maintains the signal strength values of the neighbour nodes. The least or smallest RSSI value is considered as the threshold. Whenever a sensor or node joins the network, its RSS value will be calculated, and if that value is more than the threshold, then it is regarded as suspicious. Then, the new and old node IDs and RSS values will be checked. If the RSS value is more than or equal to the threshold, it indicates that the newly joined node is an attacker node. The major advantage of this scheme is its high level of accuracy. The algorithm of the RSSI method is as follows:

Algorithm for RSS-based Sybil node detection

Notations	Explanations
node_id	Sensor node ID
node_list	Node type
RSS (node_id)	Received signal strength of node
RSS UB_THRESHOLD	Threshold value of RSS level

Algorithm for RSS-based Sybil node detection

1. **Input:** node_id
2. **Output:** node_list
3. Calculate RSS UB_THRESHOLD value
4. Address of the node is checked in table
5. **If** RSS (node_id) >= RSS UB_THRESHOLD
Add it into Sybil node list
6. **Else**
Add its address in table of legitimate nodes
7. **End If**

4.2 Caesar Cipher Algorithm

The Caesar cipher replaces every letter of a message with a letter that is a fixed number of positions down the alphabet. For example, Julius Caesar takes the second letter and repeatedly uses it. In this case, one function is used to replace the character, which is

called scrambling. The purpose of scrambling is to substitute a character (or byte) of data for another character (or byte) of data.

4.2.1 CCA encryption

Input: The plain text.

Output: The ciphertext, which is encrypted by CCA.

1. The following expression (2) describes the CCA encryption process.

$$P = (m + n) \bmod 26 \quad (2)$$

where c is the ciphertext, (m) is the plain text and n is the number of shifts. This ciphertext P is encrypted again using LEA.

4.3 Lightweight encryption algorithm

The data that is encrypted by CCA is transferred to lightweight encryption. The SIT [30] is a symmetric key block cipher that uses 64-bit plain-text keys. In the symmetric key algorithm, the encryption process consists of encryption rounds, with each round creating confusion and diffusion. An increase in the number of rounds provides better security, but the use of limited energy inevitably increases. LEA is a key generation process, which must also be reduced to an extent to ensure proper security in the data transmission process from source to destination. The key is the main component in the processes of encryption and decryption, which depend on the complete security of the data from the Sybil attackers. The encryption/decryption of the LEA algorithm is carried out with a 64-bit block cipher. The user's input is a 64-bit cypher key, which serves as an input to the key expansion block. The block performs a series of operations to create confusion and diffusion in the input key, and it generates five unique keys. The five keys can be used in either encryption or decryption and are powerful enough to stay indistinct during an attack. The key expansion block architecture is shown in Fig. 7.

The components of key expansion are described as follows:

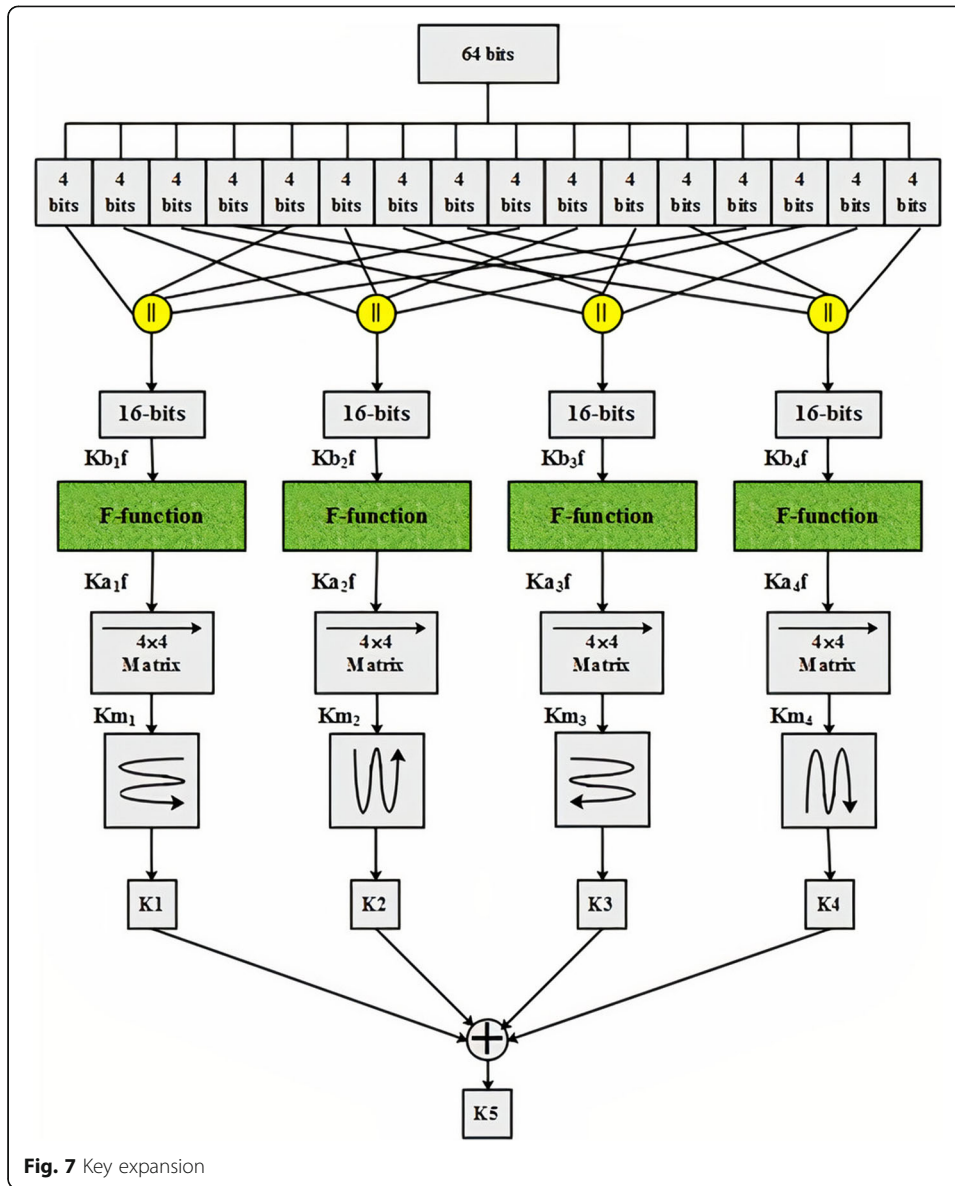
1. Initially, the 64-bit cipher key (Kc) is separated into 4-bit segments.
2. The f-function works on 16-bit data. Four f-function blocks are used in this key expansion. Equation (3) shows an initial population of cipher key segments.

$$Kb_i = \parallel_{j=1}^4 Kc_{4(j-1)+i} \quad (3)$$

where $i = 1$ to 4 for the first four round keys.

3. The 16 bits of each f-function are achieved by giving a Kb_i of 16 bits, which is given in Eq. (4).

$$Ka_i f = f(Kb_i f) \quad (4)$$



4. There are two kinds of tables available in the f-function: P and Q. These two tables are created to perform the linear and non-linear transformations.
5. The K1, K2, K3 and K4 matrices are transformed into four arrays of 16 bits for obtaining the round keys. The round key is called as round keys (K_r).

The four arrays of keys are expressed as follows:

$$K1 = a4 \parallel a3 \parallel a2 \parallel a1 \parallel a5 \parallel a6 \parallel a7 \parallel a8 \parallel a12 \parallel a11 \parallel a10 \parallel a9 \parallel a13 \parallel a14 \parallel a15 \parallel a16$$

$$K2 = b1 \parallel b5 \parallel b9 \parallel b13 \parallel b14 \parallel b10 \parallel b6 \parallel b2 \parallel b3 \parallel b7 \parallel b11 \parallel b15 \parallel b16 \parallel b12 \parallel b8 \parallel b4$$

$$K3 = c1 \parallel c2 \parallel c3 \parallel c4 \parallel c8 \parallel c7 \parallel c6 \parallel c5 \parallel c9 \parallel c10 \parallel c11 \parallel c12 \parallel c16 \parallel c15 \parallel c14 \parallel c13$$

$$K4 = d13 \parallel d9 \parallel d5 \parallel d1 \parallel d2 \parallel d6 \parallel d10 \parallel d14 \parallel d15 \parallel d11 \parallel d7 \parallel d3 \parallel d4 \parallel d8 \parallel d12 \parallel d16$$

From the above four round keys, the fifth key is found by using the XOR operation, which is shown in Eq. (5).

$$K5 = \sum_{i=0}^4 Ki \quad (5)$$

4.3.1 Encryption of LEA

The LEA encryption process starts after the key generation process is performed. The logical operations are performed in the diffusion of the text (i.e. input) to create confusion. The encryption process is shown in Fig. 8.

At first, the data from the CCA is given as input (i. e. plain text – P_t) to the LEA encryption process, and then, this plain text is divided into four segments: P_{x0-15} , P_{x16-31} , P_{x32-47} and P_{x48-63} . The original data is altered in each round by the swapping operation, which maximises the confusion of the plain text.

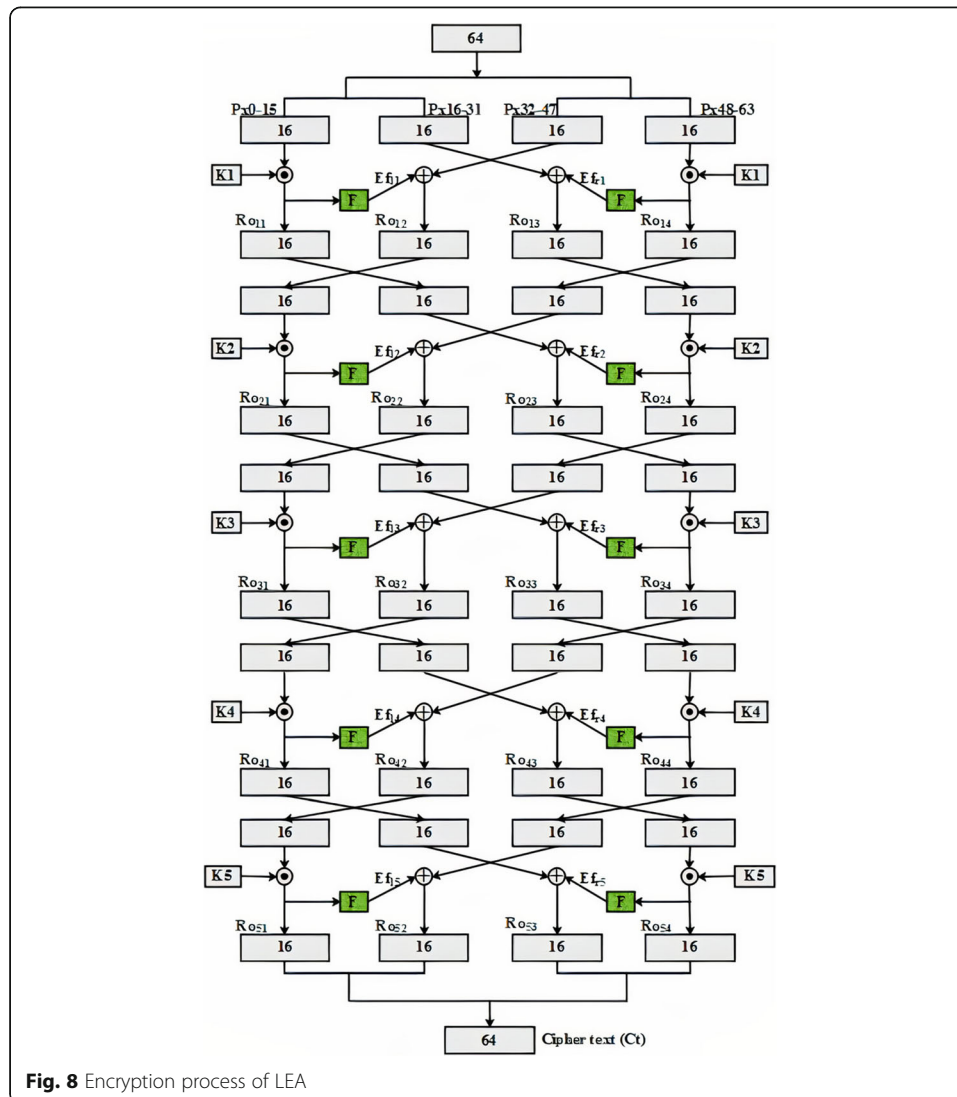


Fig. 8 Encryption process of LEA

The f -function used in this encryption is similar to the key expansion, and this encryption comprises swapping and substitution operations, as shown in Fig. 6. The bit-wise XOR function is applied among $Ef1$ & $Px32-47$ to obtain $Ro12$ and $Efr1$ & $Px16-31$ to find $Ro13$.

$$Ro_{i,j} = \begin{cases} Px_{i,j} \odot K_i; & j = 1 \& 4 \\ Px_{i,j+1} \oplus Ef_{li}; & j = 2 \\ Px_{i,j-1} \oplus Ef_{ri}; & j = 3 \end{cases} \quad (6)$$

After performing the first round, $P_{x_{16-31}}$ is in $Ro11$, $P_{x_{0-15}}$ in $Ro12$, $P_{x_{48-63}}$ in $Ro13$ and $P_{x_{32-47}}$ in $Ro14$, as shown in Fig. 6.

Equation (7) is used for the remaining rounds. At the end of all rounds, the concatenated result, which is composed of ciphertext (Ct), is obtained. This ciphertext is given as follows:

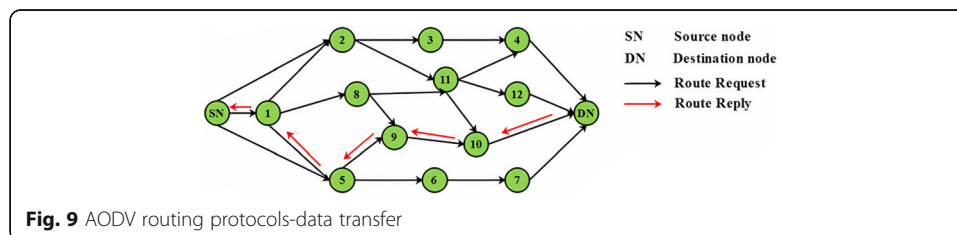
$$(Ct) = R51 \parallel R52 \parallel R53 \parallel R54 \quad (7)$$

4.4 AODV routing protocol

To transfer the encrypted message from one node to another, the AODV protocol is used in the RSSI-LEA-AODV method. The routing protocol is meant to create mobility among nodes in the network. AODV [27] is designed to reduce the energy dissemination and control overhead. AODV has two stages: (1) route discovery and (2) route maintenance. In the route discovery stage, fresh or new routes are found. In the route maintenance stage, link breaks of existing routes are found and repaired. AODV is a reactive routing protocol that creates routes on demand but does not establish a fixed route table. The method of moving data in the AODV routing protocol is shown in Fig. 9.

4.4.1 Prevention of Sybil attacks

The Sybil node blindly responds to every routing request (RREQ) with a huge sequence number and least hop count values to convince the SN that it has a new route to the DN. In the RSSI-LEA-AODV method, AODV routing is used for discovering a transmission path between the source and the destination that is free of any Sybil nodes. If any path has a Sybil node, the path has to be discarded, and the new route is to be formed based on the AODV's consideration. The Sybil attack is discovered by relying on the energy levels of every node in the network. At first, the SN delivers the request to the neighbour's node based on the threshold range that is fixed in the network. If the node has adequate energy to transmit the data, that node is used in creating the transmission path; otherwise, the



node is discarded from the transmission. By avoiding nodes with less energy, the Sybil is reduced, and the amount of information transmitted in the network is increased.

a. Algorithm for prevention of Sybil attacks in AODV routing

Notations	Explanations
des_id	Destination node ID
out_id	The node that is linked to another node
s_id	Source ID
Dist	Distance between the source node and the other nodes
thre	Threshold value for finding the nodes in the communication range
new_id	The nodes that are capable of transmitting the information to the destination
next_id	The node is connected to the source node that has higher energy and less distance

Algorithm for prevention of Sybil attacks in AODV routing

```

1. Input: des_id
2. Output: Out_id
3. While (out_id = des_id)
    s_id = rand (id); # id is the node's ID number
4. While (1)
    id = find (dist < thre);
    new_id = find (energy (id) > 0.1);
    # here, 0.1 is minimum energy level of the nodes
    next_id = mindis (new_id);
    # the node that has higher energy and less distance has an out_id
5. If (next_id = Sybil node)
    return;
    # Sybil node detection
6. Else
    out_id = next_id;
    s_id = out_id;
7. End If
8. End While
9. End While

```

4.5 LEA and CCA decryption

LEA decryption is simply the LEA encryption in reverse. The data from the LEA decryption is again decrypted using CCA decryption. The CCA is used to decrypt the message, which is given at the source side.

Input: The ciphertext that is collected from the LEA decryption.

Output: The plain text.

1. The CCA decryption is given in Eq. (8).

$$m = (c - n) \bmod 26 \quad (8)$$

5 Results and discussion

The RSSI-LEA-AODV method has been simulated by using MATLAB 2017a. In the RSSI-LEA-AODV method, RSSI-based Sybil detection is used for detecting the Sybil nodes, and the AODV routing approach is adopted to create a route between the source and the destination. Table 1 displays the simulation parameters used in the RSSI-LEA-AODV method. It is compared with the network in the presence of a Sybil attack to understand the results of the RSSI-LEA-AODV method.

Table 1 Simulation parameters

Parameter	Value
Network size	300*300 m ²
Sensors	200
Initial energy of sensor nodes	0.5 J
Number of iterations	Length (message)
Communication range of each node	50 nm
E_T	0.2 PJ/bit/m ²
E_R	0.1 PJ/bit/m ²
Packet size	4000 bits
Message size	200 bits

The performance parameters that are analysed in this system are described as follows.

5.1 Alive nodes

Nodes with sufficient energy to move the data are called alive nodes. More alive nodes are needed for sufficient data transmission.

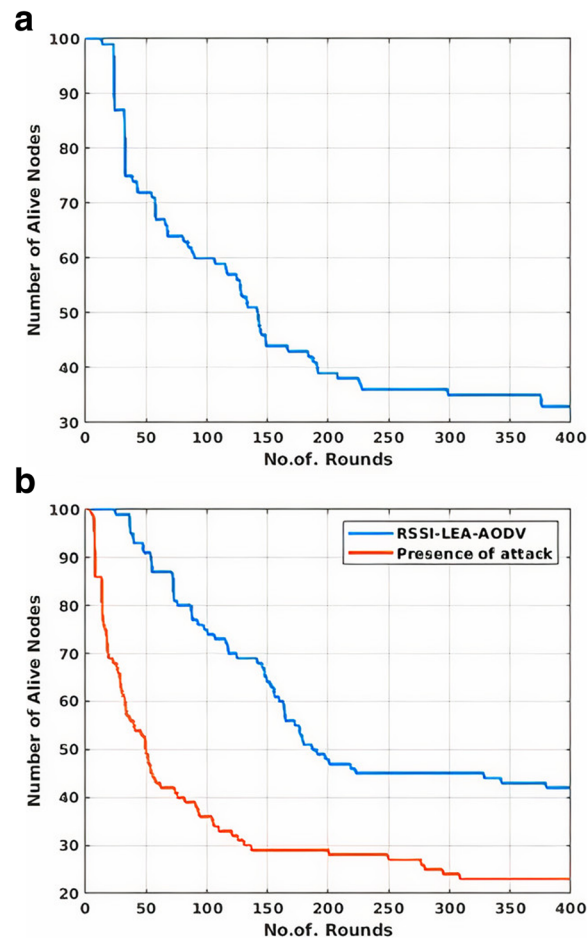


Fig. 10 **a** Alive nodes in the network without a Sybil attack. **b** Performance comparison of alive nodes

Figure 10a shows the network without a Sybil attack, and Fig. 10b shows the alive nodes of the network with an attack and the RSSI-LEA-AODV method. Based on the figure, it is inferred that the RSSI-LEA-AODV method has more alive nodes compared with the Sybil attack. More alive nodes transmit information (ciphertext) for more time. The alive nodes of the network mainly depend on the distance between the nodes. This is because if there is less distance from one node to another, there is also less utilisation of energy.

5.2 Dead nodes

Nodes with no energy to relay information are called dead nodes. Dead nodes are to be minimised in the network to prevent packet loss, and this, in turn, enhances the network performance.

$$\text{Deadnodes} = \text{Total number of nodes} - \text{number of alive nodes} \quad (7)$$

where Eq. (7) is used for determining the number of dead nodes.

Figure 11a shows the dead nodes in the network without a Sybil attack, and Fig. 11b shows the comparison of the dead nodes in the network with an attack and

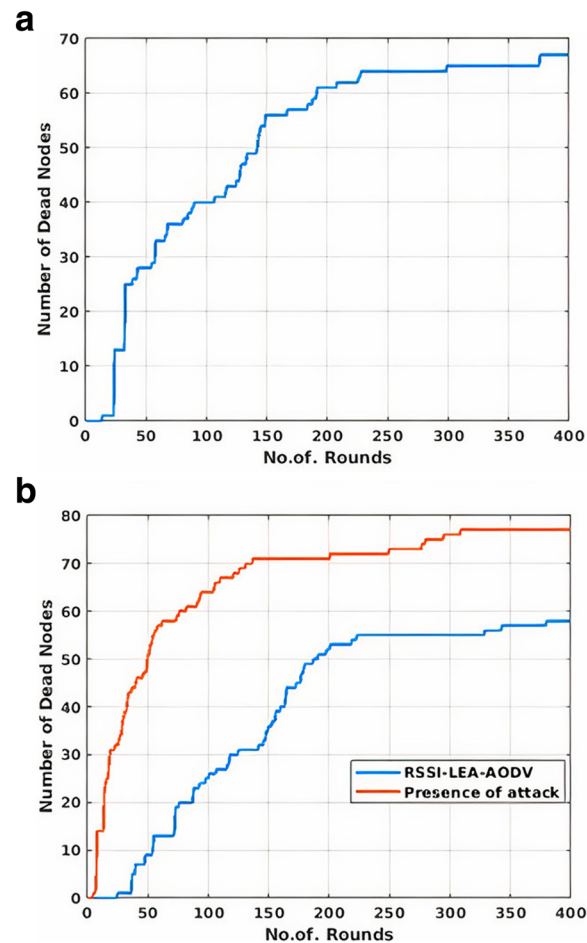


Fig. 11 a Dead nodes in the network without a Sybil attack. **b** Performance comparison of dead nodes

the RSSI-LEA-AODV method. The number of dead nodes in the RSSI-LEA-AODV method is reduced by contrasting the two methods. A smaller number of dead nodes result in lower packet loss and the minimisation of the Sybil attack. These dead nodes are avoided during the creation of the path from the source to the destination. This is because the path that contains the dead nodes creates packet loss within the network.

5.3 Energy consumption

In the AODV protocol, each node's total energy for transmitting the message across the route is extracted. The energy consumption of an entire network is given in Eq. (8).

$$E_c = E - (E_T + E_R) \quad (8)$$

E_c energy consumption, E total energy, E_T transmitting and E_R receiving energy.

Figure 12a shows the energy consumption without a Sybil attack, and Fig. 12b shows the comparison of the attack and the RSSI-LEA-AODV method. The energy consumption of the network with the Sybil attack is greater than that of the RSSI-LEA-AODV method. As the load balancing in the transmission path becomes higher, the energy

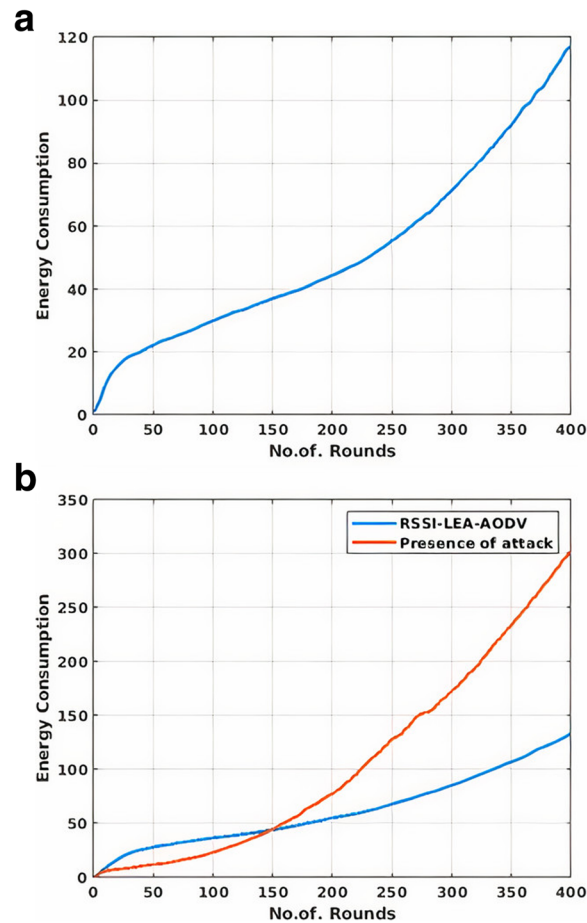


Fig. 12 a Energy consumption of the network without a Sybil attack. **b** Performance comparison of energy consumption

consumption also increases. The energy efficiency of the network also relies primarily on the distance between the nodes. Therefore, the network that is under a Sybil attack consumes more energy.

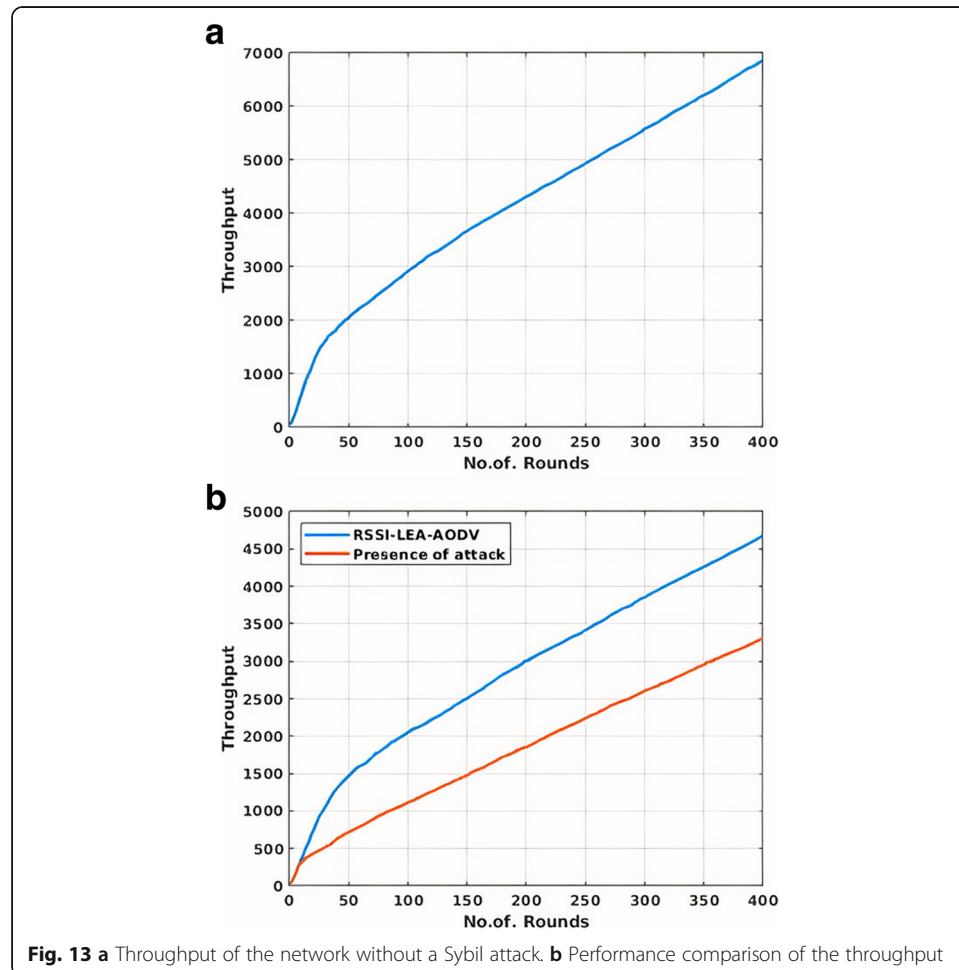
5.4 Throughput

Throughput is defined as the number of messages transmitted to the destination. This value should be high for efficient data transmission. Equation (9) gives the throughput.

$$T_H = N_T \times P_L \quad (9)$$

where T_H represents the throughput of the network, N_T represents the total number of rounds and P_L represents the length of the packet.

Figure 13a shows the throughput of the network without a Sybil attack, and Fig. 13b shows the comparison of the throughput of the network with an attack and the RSSI-LEA-AODV method. The throughput of the RSSI-LEA-AODV method is increased when compared to the network with an attack. This is because the network that has the Sybil nodes consumes more energy during the transmission between the nodes. The attack causes the link failure through the network. Due to



this link failure, packet loss occurs in the network with the presence of a Sybil attack.

5.5 Packets sent and packet loss

Figure 14a shows the packet sent of the network without a Sybil attack, and Fig. 14b shows the comparison of the packet send of the network with an attack and the RSSI-LEA-AODV method. This will be the same for both systems because the same number of packets is sent to these systems. The packet losses based on the system considerations are shown in Fig. 15.

Figure 15a shows the packet loss of the network without a Sybil attack, and Fig. 15b shows the comparison of the packet loss of the network with an attack and the RSSI-LEA-AODV method. It is inferred from the study that the performance of the RSSI-LEA-AODV method is lower. This is because the throughput is maximised without any packet loss. In this case, the packet loss of the RSSI-LEA-AODV is small, avoiding the dead nodes during the path creation from one node to another. If the path contains dead nodes (i.e. link failure), the AODV routing protocol is initiated again to transfer the data packets.

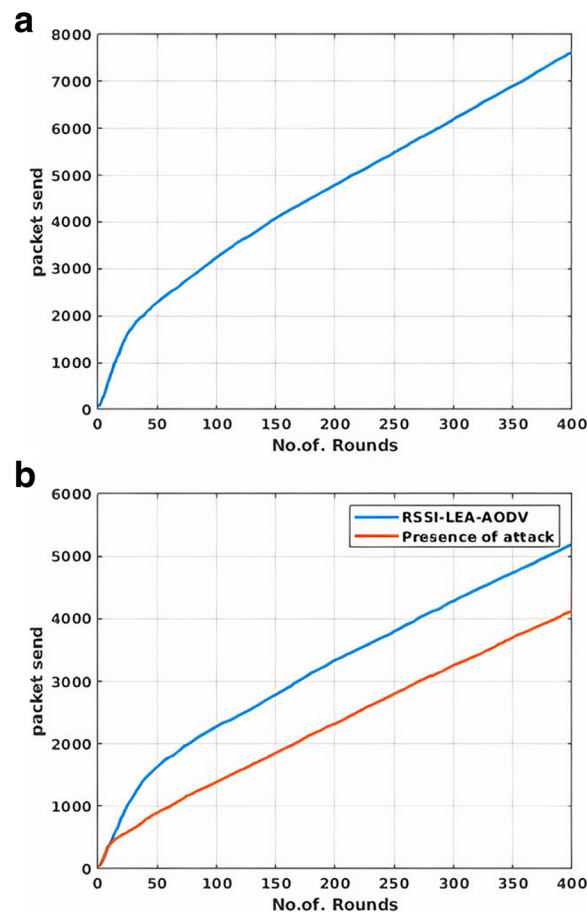
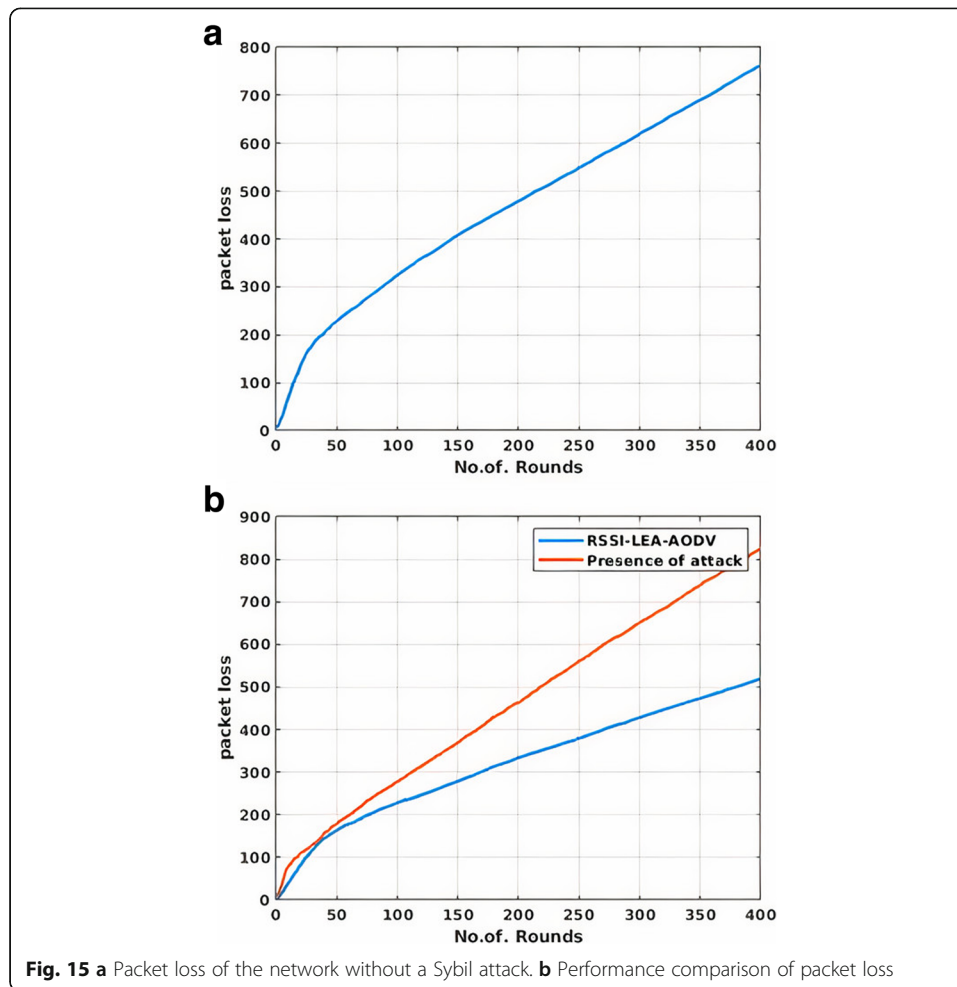


Fig. 14 a Packet send of the network without a Sybil attack. b Performance comparison of the packet sent



6 Conclusion

Because Sybil attacks in networks are severe, addressing Sybil attacks is a crucial issue for the security of networks. Sybil attacks use numerous identities or the identification of another node that exists in the network. The presence of Sybil nodes disturbs the communication between the sensor nodes and reduces the trust of the normal nodes in the network. In this paper, RSSI-based Sybil detection is used for detecting the Sybil nodes (i.e. those that create the Sybil attack). The detection of the Sybil nodes depends on the received signal strength of each node. If the RSS of a node goes beyond a certain threshold level, that node is added to the Sybil node list. The lightweight encryption method is used for sending the data from one node to another to improve confidentiality.

The AODV routing protocol is utilised for creating the optimal route from one node to another. The AODV routing protocol is optimised by two parameters: the energy of each sensor node and the distance between the sensor nodes. The data, which is encrypted by CCA with LEA, is transmitted via the route of AODV. The Sybil nodes are avoided during the establishment of a route from one node to another node. By avoiding the Sybil nodes in the network, the communication among the sensor nodes occurs properly. The performance of this system is analysed by the network with the

presence of a Sybil attack. Based on the comparison, we conclude that the RSSI-LEA-AODV method provides effective performance when the network is under a Sybil attack.

Furthermore, the performance of the Sybil attack detection can be improved by using SVM or any other optimisation methods. These Sybil nodes will be avoided while transmitting data. Indeed, this Sybil attack detection and prevention is useful in healthcare systems, like when a patient's health condition changes suddenly beyond the specified range the system will alert the doctor.

Future scope involves cost-effective and efficient Sybil attack detection. Performance can be improved by using SVM or any other optimization methods. These Sybil nodes will be prevented while transmitting data.

Acknowledgements

Not applicable

Authors' contributions

The authors have contributed equally to this paper. The authors read and approved the final manuscript.

Authors' information

T. Aditya Sai Srinivas received the master's degree in computer science and engineering, in 2012. He is currently working as an Assistant Professor in the Department of CSE, in G. Pullaiah College of Engineering and Technology, Kurnool, India. His areas of interest are the Internet of Things, network security and Big Data.

Dr. S.S. Manivannan. Associate Professor in VIT Vellore. Received the degree in computer science and engineering from VIT Vellore. Life member in CSI. Published 25+ papers and participated in 50+ conferences. Interest areas include the Internet of Things, network security and Big Data.

Mr. Somula Ramasubbareddy is pursuing his PhD in Computer Science and Engineering (CSE), from VIT University, Vellore, India. He did his M.tech from JNTUA, Anantapur, India, in 2015. His research areas are mobile cloud computing, network security, distributed computing, computer communications (networks) and IoT.

Dr. S. Sankar received M.E degree from Anna University and PhD degree from VIT University, Vellore, India, in 2019. He is currently working as an Assistant Professor in Sona College of Technology, Salem. Research interest includes the Internet of Things, wireless sensor networks and machine learning. He has published various papers in international journals and conferences.

Daniel Burgos is a Professor of Technologies for Education and Communication, Vice-rector for International Research, Director of the UNESCO Chairs in eLearning and ICDE in Open Educational Resources and Director of the Research Institute for Innovation & Technology in Education (UNIR iTED) at Universidad Internacional de La Rioja (UNIR). He is also a professor at An-Najah National University (Palestine), Universidad Nacional de Colombia and North-West University (South Africa).

Funding

There is no external funding.

Availability of data and materials

Data are available under reasonable request to the corresponding author. Some restrictions may apply to that availability.

Declarations

Ethics approval and consent to participate

Not applicable

Consent for publication

Not applicable

Competing interests

The authors declare that they have no competing interests.

Author details

¹SCOPE, Vellore Institute of Technology, Vellore, India. ²SITE, Vellore Institute of Technology, Vellore, India. ³Department of Information Technology, VNRVJIT, Hyderabad 500090, India. ⁴Department of Computer Science and Engineering, Sona College of Technology, Salem, India. ⁵Research Institute for Innovation & Technology in Education (UNIR iTED), Universidad Internacional de La Rioja (UNIR), 26006 Logroño, La Rioja, Spain.

Received: 15 February 2021 Accepted: 17 June 2021

Published online: 16 July 2021

References

1. R. Khan, S.U. Khan, R. Zaheer, S. Khan, in *Frontiers of Information Technology (FIT), 2012 10th International Conference on*. Future internet: the internet of things architecture, possible applications and key challenges (2012), pp. 257–260
2. D. Dejene, B. Tiwari, V. Tiwari, TD²SecIoT: temporal, data-driven and dynamic network layer based security architecture for industrial IoT. *Int. J. Interact. Multimed. Artif. Intell.* **6**(4) (2020)
3. C. González García, E.R. Núñez Valdéz, V. García Díaz, B.C. Pelayo García-Bustelo, J.M. Cueva Lovelle, A review of artificial intelligence in the internet of things. *Int. J. Interact. Multimed. Artif. Intell.* **5** (2019)
4. L. Tan, N. Wang, Future internet: the internet of things. *Advanced Computer Theory and Engineering (ICACTE), 2010 3rd International Conference on* **5**, V5–V376 (2010)
5. J. Gomez, B. Oviedo, E. Zhuma, Patient monitoring system based on internet of things. *Procedia Comput. Sci.* **83**, 90–97 (2016)
6. K.S. Fayaz, "Health care monitoring system in Internet of Things (IoT) by using RFID." 2017 6th International Conference on Industrial Technology and Management (ICITM). IEEE, 2017.
7. J. Viret, A. Bindel, P. Conway, L. Justham, H. Lugo, A. West, in *Microelectronics and Packaging Conference (EMPC), 2011 18th European*. Embedded RFID TAG inside PCB board to improve supply chain management (2011), pp. 1–5
8. D. Sharma, I. Mishra, S. Jain, A detailed classification of routing attacks against RPL in Internet of Things (2017)
9. D. Nitaware, A. Thakur, in *Signal Processing and Integrated Networks (SPIN), 2016 3rd International Conference on*. Black hole attack detection and prevention strategy in DYMO for MANET (2016), pp. 279–284
10. K. Chugh, L. Aboubaker, J. Loo, in *Proc. of the Sixth International Conference on Emerging Security Information, Systems and Technologies (SECURWARE), Rome, Italy (August 2012)*. Case study of a black hole attack on LoWPAN-RPL (2012), pp. 157–162
11. L. Wallgren, S. Raza, T. Voigt, Routing attacks and countermeasures in the RPL-based Internet of Things. *Int. J. Distrib. Sens. Networks* **9**(8), 794326 (2013)
12. K. Zhang, X. Liang, R. Lu, X. Shen, Sybil attacks and their defenses in the internet of things. *IEEE Internet Things J.* **1**(5), 372–383 (2014)
13. D. Airehrour, J. Gutierrez, S.K. Ray, Securing RPL routing protocol from blackhole attacks using a trust-based mechanism. *26th Int. Telecommun. Networks Appl. Conf. ITNAC* **2016**, 115–120 (2017)
14. S. Pawar, P. Vanwari, Sybil attack in internet of things. *Int. J. Eng. Innov. Technol.* (2016)
15. S. Kumar, V.K. Solanki, S.K. Choudhary, A. Selamat, R. González Crespo, Comparative study on ant colony optimization (ACO) and K-means clustering approaches for jobs scheduling and energy optimization model in Internet of Things (IoT). *Int. J. Interact. Multimed. Artif. Intell.* **6**(1) (2020)
16. R. Amuthavalli, R.S. Bhuvaneswaran, Detection and prevention of Sybil attack in wireless sensor network employing random password comparison method. *J. Theor. Appl. Inf. Technol.* **67**(1) (2014)
17. E.H.S.C. Bedi, Prevention of Sybil attack on LEACH protocol in WSN using BCO. *Int. J. Electr. Electron. Res.* **3**(1), 103–109
18. L. Xiao, L.J. Greenstein, N.B. Mandayam, W. Trappe, Channel-based detection of Sybil attacks in wireless networks. *IEEE Trans. Inf. Forensics Secur.* **4**(3), 492–503 (2009)
19. J.F. Herrera-Cubides, P.A. Gaona-García, C. Montenegro-Marín, D. Cataño, R. González-Crespo, Security aspects in web of data based on trust principles. A brief of literature review. *Int. J. Commun. Networks Inf. Secur.* **11**(3), 365–379 (2019)
20. P. Sarigiannidis, E. Karapistoli, A.A. Economides, Detecting Sybil attacks in wireless sensor networks using UWB ranging-based information. *Expert Syst. Appl.* **42**(21), 7560–7572 (2015)
21. R. Singh, J. Singh, R. Singh, TBSD: a defend against Sybil attack in wireless sensor networks. *Int. J. Comput. Sci. Netw. Secur.* **16**(11), 90 (2016)
22. N. Alsaedi, F. Hashim, A. Sali, F.Z. Rokhani, Detecting sybil attacks in clustered wireless sensor networks based on energy trust system (ETS). *Comput. Commun.* **110**, 75–82 (2017)
23. P.R. Vamsi, K. Kant, Detecting Sybil attacks in wireless sensor networks using sequential analysis. *Int. J. Smart Sens. Intell. Syst.* **9**(2) (2016)
24. Palak, Fuzzy based Sybil attack detection in Wireless Sensor Network. *Int. J. Comput. Sci. Eng.* **5**(11) (2017)
25. U.S.R.K. Dhamodharan, R. Vayanaperumal, Detecting and preventing Sybil attacks in wireless sensor networks using message authentication and passing method. *Sci. World J.* **2015** (2015)
26. R. Singh, J. Singh, R. Singh, A novel Sybil attack detection technique for wireless sensor networks. *Adv. Comput. Sci. Technol.* **10**(2), 185–202 (2017)
27. M.A. Jan, P. Nanda, X. He, R.P. Liu, A Sybil attack detection scheme for a centralized clustering-based hierarchical network. *Trustcom/BigDataSE/ISPA, 2015 IEEE* **1**, 318–325 (2015)
28. S. Abbas, M. Merabti, D. Llewellyn-Jones, K. Kifayat, Lightweight Sybil attack detection in MANETs. *IEEE Syst. J.* **7**(2), 236–248 (2013)
29. S.T. Patel, N.H. Mistry, in *Electronics and Communication Systems (ICECS), 2017 4th International Conference on*. A review: Sybil attack detection techniques in WSN (2017), pp. 184–188
30. M. Usman, I. Ahmed, M.I. Aslam, S. Khan, U.A. Shah, Sit: a lightweight encryption algorithm for secure internet of things. *arXiv Prepr. arXiv1704.08688* (2017)

Publisher's Note

Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.