Artificial Intelligence Inspired Intelligent Trust Based Routing Algorithm for IoT

Kajol Rana[1†], Ajay Vikram Singh[2] and P. Vijaya[3],
kajolau07@gmail.com
Amity University, Noida, India
Waljat, College of Applied Science, Oman

Summary
Internet of Things (IoT) is a relatively new concept that has gained immense popularity in a short period of time due to its wide applicability in making human life more convenient and automated. As an illustration: the development of smart homes, smart cities, etc. However, it is also accompanied by a substantial number of risks and flaws. IoT makes use of low-powered devices, so secure, less time-consuming and energy-intensive transmission (routing) of messages due to the limited availability of energy is one of the many and most significant concerns for IoT developers. The following paper presents a trust-based routing scenario for the Internet of Things (IoT) that exploits the past transmission record from the cupcarbon simulator's log files. Artificial Neural Network is used to quantify knowledge of trust, calculate the value of trust, and share this information with other network devices. As a human behavioural pattern, trust provides a superior method for making routing decisions. If there is a tie in the trust values and no other path is available, the remaining battery power is used to break the tie and make a forwarding decision; this is also seen as a more efficient use of the available resources. The proposed algorithm is observed to have superior energy consumption and routing decisions compared to conventional routing algorithms, and it improves the communication pattern.

Keywords:
ANN, Routing Algorithm, Sensors, Low Power Devices..

1. Introduction

Internet, which emerged in the early 1950s, is a method for connecting systems across the globe that uses TCP/IP to transmit data. The Internet has evolved to a point where all types of physical objects will be able to identify themselves and communicate with other devices over the internet. IoT enables Internet protocol-based network communication by eliminating human interference. IoT employs scale-free networking, meaning that the data can range from tiny data blocks to high-quality video. It has zero tolerance for any form of delay. IoT networking [6] utilises Radio-Frequency identification [3] and Near-field communication [4], low energy Bluetooth [5], wireless, LTE-A, and Wifi-direct. To accommodate a large number of devices, IPv6 addressing is utilised [7].

Manuscript received November 5, 2023
Manuscript revised November 20, 2023
https://doi.org/10.22937/IJCSNS.2023.23.11.19

1.1 Routing in IoT

IoT is defined as a collection of adhoc devices, sensors, and heterogeneous natured devices that communicate with each other in a harmonious manner; therefore, constructing such a system and enabling the devices to communicate with one another is a laborious task. IoT employs the 6LoWPAN protocol [8] to simplify the sending and receiving of IPv6 packets over IEEE 802.15.4 [9].

IoT devices typically have low-power applications, which results in a lossy network because the devices lack the power to support traditional data routing; consequently, data flow is restricted and highly ordered. The flow of data can be point-to-point, point-to-multi-points, or multi-point-to-point [10].

Cluster-based routing is used to improve the performance of nodes in an energy-poor environment in order to conserve energy. Certain Cluster-based routing protocols, such as LEACH (Low Energy Adaptive Clustering Hierarchy), are utilised by network nodes to overcome power shortage issues. Clusters of wireless sensor nodes are assigned. A message is then transmitted over short distances. A cluster head is chosen at random to collect data from the nodes and transmit it to the base station [12] [13]. The Cluster head is selected by SEP (Stable Election Protocol) using the weighted probability of nodes. On this basis, the nodes are separated into two categories: Advanced and Normal. Typically, advanced nodes are selected as cluster heads [14]. This is why this protocol is considered stable; [15] HEED (Hybrid Energy Efficient Distributed Protocol) creates groups of nodes, selects a cluster head from the nodes, and uses the residual energy for CH selection [17]. TEEN (Threshold Sensitive Energy Efficient Sensor Network Protocol) utilises threshold for data transmission and is data-centric. According to reports, data sensing consumes less energy than data transmission [18-20].

1.2 Security Requirements For IoT

The Internet of Things is distinguished by characteristics such as heterogeneity, connectivity and

ubiquity, limited resources, self-organization, mobility, and scalability. To achieve IoT full deployment, however, the following security requirements must be met [21][22]:

- **Authentication:** It ensures that each entity in the Internet of Things is uniquely identified; therefore, each entity must identify itself and mutual authentication is required between IoT entities. Therefore, impersonating nodes must be identified.
- **Authorization / Access Control:** These specifications guarantee that only authorised users can access IoT entities. Because unauthorised access to IoT entities will jeopardise network security, it is essential that only authorised parties have access to data and routing information.
- **Availability:** It states that IoT entities, networks, and services must be accessible and functional at all times, regardless of exposure to malicious attacks or failures due to IoT characteristics.
- **Confidentiality:** It ensures that only authorised entities are able to access and modify data and routing information securely. In other words, IoT application data exchanges should be concealed from intermediaries and unauthorised parties.
- **Integrity:** It ensures that data and routing information have not been altered by an intermediary or malicious entity while in transit. Consequently, it is imperative to detect any alteration in the data being exchanged.
- **Privacy:** It ensures that the identities of IoT entities are highly protected against unauthorised access by, for example, defining the rules under which data pertaining to specific entities may be accessed. According to Kumar and Patel (2014), privacy must be considered on the IoT device itself, during storage, communication, and processing.
- **Trust:** Due to the characteristics of the Internet of Things, there is a need to architect the IoT in a reliable manner that allows for automatic adaptation to an unanticipated security breach. In actuality, numerous security solutions exist to satisfy the aforementioned requirements. For example, Transport Layer Security mechanisms such as TLS or VPN should be utilised to ensure privacy. Message Integrity Codes (MIC) may be utilised to ensure message integrity. Communication between IoT entities could be secured using certificate-based authentication. Context-based access control could be used to control access based on the requirements of IoT applications. For availability security, Intrusion Detection Systems (IDS) and firewalls could be utilised. Solutions that strike a balance between the anonymity requirements of some applications and the localization and tracking needs of others could be used to preserve privacy. In reality, trust management systems must detect untrustworthy behaviour, isolate untrusted entities and zones, and redirect IoT functionality to trusted zones in all circumstances.

1.3 ANN Classification For IoT

Artificial Neural Network functions similarly to the human brain in that it is comprised of a large number of interconnected processing elements that work together to perform the perfect solution for specific problems that are extremely costly to solve using conventional methods. Several applications have successfully implemented ANN algorithms, including Recognition, Classification, and Feature Extraction. And classify and detect security threats using various supervised ANN algorithms, namely:

- **Learning Vector Quantization (LVQ):** LVQ is one of the supervised ANN classification algorithms based on the Kohonen model. It is also known as the supervised version of the unsupervised learning algorithm Self-Organizing Map networks (SOM). LVQ employs vector quantization architecture in conjunction with vector labelling and supervised training. There are several improved versions of the LVQ algorithm, including LVQ1, LVQ2.1, LVQ3, OLVQ1, OLVQ3, and LVQ3. And use all versions of LVQ to determine which version has the highest classification accuracy and performance in terms of time.
- **Radial Basis Funcion (RBF):** The RBF is one of the neural network learning methods based on radial basis function utilised by ANN. This algorithm has three layers: an input layer, a single hidden layer, and an output layer. The RBF algorithm has a straightforward structure and numerous outstanding performances. In this paper, we classified IoT security threads using RBF.
- **Multilayer Perceptron (MLP):** Algorithms Multilayer Perceptron (MLP) is a well-known artificial neural network (ANN) algorithm utilised in numerous fields, including recognition and classification. Input, one or more hidden, and output layers comprise the MLP. Through nonlinear function, it is possible to map input parameter to output parameter.

2. Related Research Work

This section compares various related works in the field of IoT and trust management. A recent study states that for election of a leader in IoT, dominating tree routing

algorithm [23] gives an efficient and fault tolerant environment, with low energy consumption of about 85% [24]. We know that IoT faces the challenge of memory management, so telescopic view is used to generate less network traffic volume with excellent latency [25]. When talking about routing in IoT, a cluster based hierarchy protocol called DEEC-VD is used for heterogeneous network which makes use of clusters and forms active cluster head [26] and to find the shortest path between the active cluster heads, it makes use of the Dijkastra algorithm [27] that gives better results as compared to other routing algorithms like DEEC, LEACH & SEP [28][29]. Another technique is known as Redundancy based WEP routing technology, which does query-driven data reporting and provides a coverage area of Machine to Machine mode and also ensures maximum stability period [30]. Another routing protocol which is focused on energy consumption is divided into two phases: The first phase, known as initialization phase, in which, each sensor node needs to find its neighbor nodes and form a cluster, whereas, the second phase is known as, maintenance phase, wherein, all the nodes maintain their information matrix and share these details with all the other nodes, on receiving a cluster head rotation control message.

AOMDV [31] makes a connection between the internet and ordinary nodes within a network. Each node has to maintain two tables: Internet Connecting table & Routing table. It can also be called a reactive protocol [32] as it only works on demand. Does not provide any security, not context aware, finds the best route with regards to minimal hop count and do not consider energy efficiency and it only shortlists one path, so there are high chances of failure and delays: [33]. Optimized link state routing protocol works as a table operated protocol and shares the details of the topology with the other participating nodes on a regular basis. Each node has to select a set of multipoint relays to make communication possible. These MPR's should be only one hop neighbors to the node and must contain bi-directional linkages; [34] For NDN IoT in smart cities creation, we have a Light weight authentication and secured routing protocol, which provides deployment densities of 40,000 nodes/km^2 and also involves three stages, Network discovery and authentication, Sensor Node authentication & key delivery and Path advertisement; [35] Secured Multi-hop routing enables the IoT devices to combine the procedures of authentication and routing without creating any notable overheads with added features that enable it to segregate IoT devices based on their unique identifications and re- conceptualize logical networks previously formed inside the network by the IoT devices. It performs better than OLSR protocol [36] by inculcating four layers, known as, Application layer, transport layer, User controllable multi-layer(UML) and Data link layer, wherein, the routing task is provided to the UML layer along with ANDL module to secure the communication [37]; RPL is another routing algorithm introduced by IETF whose work is to develop a topological structure by consuming the energies provided by the intelligent devices and compute the required resources. A modification of RPL also called Multiparent-RPL works on the same phenomenon but considers two way routing and makes a hierarchical clustering topology, in which, many clusters cross path and ensures data arrival rates against common routing attacks. It has been proven to prevent black and wormhole attacks; [38][39] EARA is a bio-inspired algorithm. It considers the hop count as well as the energy efficiency. It also maintains data about the average energy of nodes and the lowest residual energy value; PAIR includes information about: Residual energy and the amount of power consumption, Buffer space and the active load, and Distance between the node and neighbor [40]. It is a context aware as well as multi-hop protocol. Security parameters are not considered and memory requirements are high. It makes the heterogeneous networks cooperate; [21] REL only makes decisions based on the Link Quality indicators and stores all the possible routes. Best route is found out by considering the following factors: quality of the wireless links, Residual energy, and Hop Count [41].

2.1 Issues Associated With IoT

IoT is a developing area and so it still has a lot of issues which need to be considered before enjoying the actual benefits of IoT. As per the study of HP, it is found that 80% of IoT devices are failing to provide personal privacy to its users and 60% are still having security issues, that makes the system highly vulnerable to attacks. IoT still lacks interoperability of applications making the system not fulfilling its main goal and requiring a mechanism to develop standards and inculcating the made standards into every device to be a part of IoT system. Although the growth of sensors and chipsets are on an increase but still we lack good objects to sense the environment and generate good quality of data. Security and privacy is a big concern of IoT, as we still do not have a good authentication and reliable algorithm through which we can send our data with 100% guarantee of safe delivery to the destination node. Maintenance of connectivity in an ad-hoc network is a highly challenging task. As IoT has a feature of connecting a large number of objects, the scalability of objects in here becomes a problem. There is a limited supply of energy to run the IoT devices, so we need a system wherein consumption of energy is minimum with maximum output. Management of memory space in small objects, where data collected is very high makes it hard for the user to accept the system. No device can give 100% CPU power to run the IoT application, no system can provide such high power to any applications due to their own dedicated tasks [42].

2.2 Routing Issues

Routing is a great issue as when talking about IoT, we require devices working on low power, links should be lossy in nature, IoT follows mesh topology with multiple-hop principle and the network conditions are vastly changing from device to device. On top of it IoT works on moving as well as stationary objects, requiring different protocols, for making an IoT we have to combine these protocols into a single protocol which works more efficiently, which is again a tedious task. So considering these situations, routing has large number of issues to be handled, such as, devices communicating, suppliers of devices may be same or different; existence of the source node and destination node may be on different networks; connection between the devices may be consistent or may not be; resource availability may be a challenge and devices of different kinds may not cooperate well along with each other due to the unavailability of resources; devices not utilizing the universally accepted addressing mechanism; varying communication range between devices creates a lot of chaos; environmental conditions highly affect the routing, due to breakage of various links, signal quality degradation, reaching server becomes an issue.; estimated delay in communicating the huge amount of data should always be less than the expiry time of the data; duplicate data must be removed before transmitting onto the network; energy requirement should be less, so that even very small devices are able to function properly and require less network lifetime; context creation, validation, accuracy of the data should be well maintained and with constrained memory we also need to maintain the context in such a way that storage is maintained [42].

2.3 Factors Affecting Trust

Trust keeps on growing at a rapid pace, till the devices are interacting continuously. Denial of service, whether from the intermediate node or destination node, can change the value of trust disastrously. If such an event occurs, we need to negate all the values, so we keep the value of the bias to be a very high negative value. Just like the real world, in the IoT world value of trust obtained in the past may not matter much, if the contact time is high. Record of the success rate and time difference between the last contact and current contact must be kept, for the proper working of Trust as a routing algorithm for making forwarding decision in an IoT environment [48].

3. Trust For IoT Security

It is the starting point for developing any type of relationship. Trust is a feeling, or a flow of hormones, that induces reliance, a sense of security, and confidence in the other individual. Trust is a complex phenomenon because its evaluation is entirely dependent on the other party's response. Responses can be in the form of the instilling of confidence, the person's beliefs (which are bound to differ from person to person), the expectations one has of the other, the person's reputation (which is easily derived from prior knowledge and past experience), cooperation, and honesty. Trust can be cultivated in a variety of ways, including direct trust (involvement of the individual), indirect trust, or both (when we have trust on a person and that person trusts some third person, we automatically develop a level of trust on the third person). The reason for trust, the environment of trust, and the imminence of trust determine the strength of a relationship built on trust. Privacy is an additional trust factor [43].

Real-world examples include the relationship between a buyer and seller or the trust between family members. There are two types of trust in a buyer-seller relationship: calculated and relational. It is said that the value of calculated trust is predictive in nature. The buyer always bestows calculated trust upon the seller, whereas the seller may bestow both relational and calculated trust upon the buyer. The level of trust between the two parties will depend on the level of risk involved, the quality of the item sold, and the presence of continuous values. In contrast, calculating trust in a family may involve the behaviour and participation of family members. In a family (Figure 1.), the level of trust is observed to increase with age and experience. A general pattern indicates that children have a higher level of trust for their parents/grandparents, whereas parents/grandparents may not have the same level of trust for their children; therefore, it can be concluded that trust is context-dependent and asymmetric in nature.

For example, Hari and Ram, members of the IJK family may or may not trust each other. In a framework where decision is to be made about the careers Hari may not trust Ram, whereas when it comes to the selection of a dress Hari may trust Ram. Thus, we can say that trust constitutes continuous values. For example, Hari and Ram, members of the IJK family may or may not trust each other. In a framework where decision is to be made about the careers Hari may not trust Ram, whereas when it comes to the selection of a dress Hari may trust Ram. Thus, we can say that trust constitutes continuous values.

If we Consider T(v) as the function for trust and obtaining values between -1 to 1, we can say that, T(v) = -1 - Untrustworthy, 0 - Evenhanded, and 1 - Trustworthy.

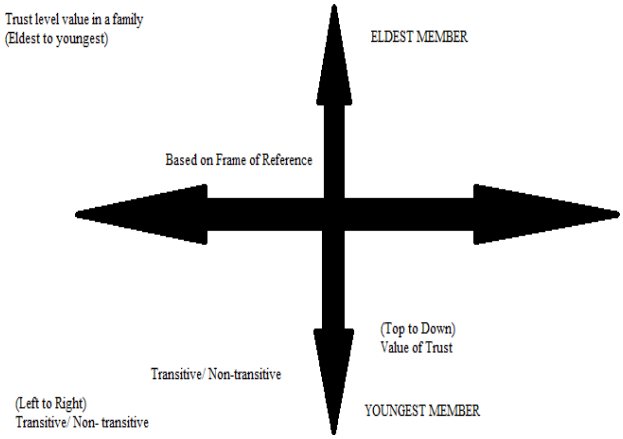


Fig. 1 Illustrating level of trust in a family.

Due to the heterogeneity of IoT components, the nature of communication channels, and other factors, the Internet of Things is susceptible to a number of security issues relating to each layer of the IoT architecture. These vulnerabilities must be addressed so that all entities participating in the IoT ecosystem can be trusted. Moreover, uncertainty and risk are crucial concerns for the deployment of IoT, as entities may be untrustworthy and thus security can be easily compromised. In this context, trust management is crucial for reliability, privacy, and data security, allowing IoT users to be more certain and confident in IoT services.

The sensed and exchanged data must be trusted; therefore, solutions to protect these data can be categorised as trust management systems. In addition, entities within an IoT network must communicate using trusted relationships; thus, identity controls and authorization systems must be implemented to build trust between entities in order for them to reliably share information. Moreover, data and applications must only be accessible to trusted parties. Therefore, solutions for access control must be based on trustworthiness. Consequently, identification, authentication, and authorization, in addition to access control systems and other existing security protocols, could be a part of or the entirety of a trust management system [44].

3.1 Trust Definitions

Different disciplines and domains, including social sciences, economics, philosophy, and cyberspace, have conducted extensive research on the concept of trust. In accordance with some existing definitions:

Definition 1: According to Mayer, Davis, and Schoorman, trust is the willingness of one party to be exposed to the actions of another party in the anticipation that the other will carry out a specific action that is significant to the trustor, regardless of the capability of the trustor to monitor or control the other party [44].

Definition 2: Online trust, according to Kimery and McCord's definition from 2002, is a customer's willingness and ability to accept an online transaction in accordance with their expectations for their future online shopping behaviour [44].

Definition 3: Additionally, online trust was defined by [45] as "an attitude of confident expectancy in an online environment of risk that one's weaknesses will not be exploited.

Definition 4: According to [46], trust is the confidence a person has in another person's willingness and capacity to provide a high level of service in a certain situation and at a specific moment.

Definition 5: According to [47], trust is based on one's capacity to anticipate another party's actions.

Definition 6: [48] defined trust as the willingness of the trustor to rely on a trustee to accomplish what is promised in a specific situation, regardless of the ability to monitor or control the trustee, and even though unfavourable outcomes might result.

Definition 7: In the context of the Internet of Things, [47] defined trust as device trust, entity trust, and data trust; device trust could be established through trusted computing and computational trust. The expected behaviour of participants, such as people or services, is referred to as entity trust. Additionally, trusted data may be created through IoT services where data needs to be assessed for trust or it may be derived from unreliable sources through aggregation.

The definitions of trust actually encompass a number of ideas, including dependence, confidence expectations, vulnerability, comfort, utility, context-specificity, risk attitude, and lack of control. Since there is no universally accepted definition of trust, it is clear that the major objective of trust management is to leverage security by supporting decision-making.

3.2 Trust Models and Classification

One remedy for concerns with loT security is trust management. The distinction between trust management and trust modelling is actually necessary. As a result, the trust models help to specifically build and realise trust management for IoT. In fact, trust modelling describes the trust establishment and computation approaches. “Trust modelling is a practical method for determining the degree of device reliability inside a system. It pinpoints the problems which could damage the trust of a system while assisting to identify areas where a low value of trust could

degrade a system's operational efficiency and usability". As opposed to this, "Trust management is a service mechanism that self-organizes a set of things depending on their trust status to take an informed choice" [25].

Different trust models may exist because the concept of trust depends on the aforementioned characteristics as well as the context and purpose of its use. A collection of characteristics, guidelines, and techniques are used to build trust between entities in trust models. They do, in fact, rely on one or more techniques for extracting, analysing, and transmitting trust information in addition to the decision-making mechanism. Various trust models have been put forth. In 2016, Airehrour et al., [44] developed many trust model types based on techniques for assessing trust. For instance, the methods used to assess trust for safe routing include Bayesian statistics, game theory, entropy, fuzzy, probability, neural network, swarm intelligence, directed/undirected graph, arithmetic/weighting, and Markov chain.

Although the majority of trust models in use today evaluate trust values using analytical techniques, other approaches have been utilised as well, including evolutionary algorithms, ant colony-based algorithms, machine learning, and social networks. New classes of trust models based on physiologically and sociologically based trust techniques as a result. Thus, writers divided trust models into three categories: analytical, bio-inspired, and socio-inspired (See Figure 2). According to Figure 2, the various techniques in the analytical class are [44].

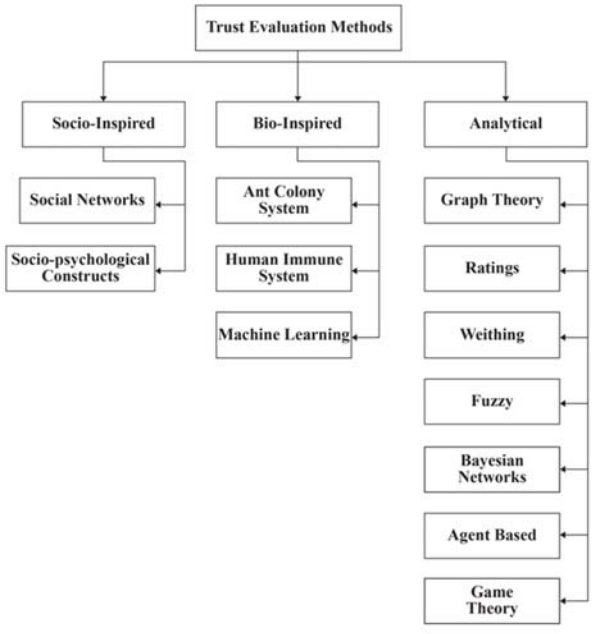


Fig. 2 Trust Models according to [42].

A different taxonomy, including two categories: decision models and assessment models. Policy models and negotiation models are included in the first class, and propagation (flow), reputation, and behaviour models are included in the second class [48 - 51].

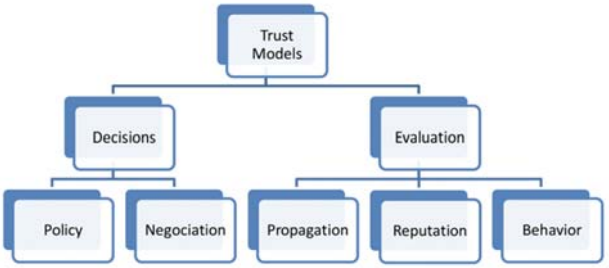


Fig. 3 Trust Model.

- **Trust Decision Models**: These approaches combine the management of the authentication and authorization process with access control decision-making to provide unified solutions.
- **Trust Evaluation Models**: Computational trust models are another name for these models. The evaluation models, in contrast to the decision models, quantify trust through measurement. To determine an entity's trustworthiness, they assess and quantify traits including dependability, honesty, and integrity.
- **Composition models:** In these models, entities need to understand which trust attributes to employ when calculating trust. Social and Quality of Service (QoS) trust models are examples of composition models.
- **Aggregation models:** These models provide the most effective technique to combine trust data that has been assessed directly by the entity or indirectly by other entities (Bao et al., 2012). There are numerous methods for aggregating trust, including regression analysis, fuzzy logic, weighted sum, belief theory, and Bayesian inference.
- **Update models:** These models show when trust values should be updated. After a transaction or occurrence that may have an impact on the quality of service, the trust information can be updated either immediately or on a regular basis (Time-driven).
- **Formation models:** These models show whether trust computation is based on the usage of many properties or just one trust property (single-trust) (Multi-trust). Additionally, models for trust formation should specify how much importance to give to social and QoS trust features.

4. Proposed Work

IoT nodes contain the combination of sensors and actuators which hold the responsibility of catching data and taking required actions. IoT is constructed on three building blocks, namely, hardware, platform and software. Sensors, gateways and actuators are a part of hardware. In IoT we talk about Device to Device Direct calculation, wherein, we need to be aware about the kind and sort of past experiences, without having the need of a trusted third party. We need to build a trust metric, on basis of which the credibility of a node can be recognized. So for making the forwarding decision, trust value are computed for each and every node along with the distance between each node, to find the nodes in the range of the source node.

Assumption Mode

IoT works with the coordination of all the sensors and gateways and thus it is assumed that all the sensors and gateways work in a coordinated manner. IoT works on real time and does not accept any sort of delays. In case of delays the error code is generated and the bias is activated. The value of trust is calculated at each and every node and flows continuously. All the nodes used are indistinguishable. Routing decisions are only taken on the basis of the value of trust computed and the propinquity of all the nodes.

4.1 ANN Based Trust Model

Artificial Neural Networks are modelled after the human nervous system and learn how to operate by mimicking human beings' learning from previous experiences. It does a decent job of handling variations. Mobility patterns are more frequently found by researchers. In order to evaluate the importance of trust and improve the functionality of IoT, we will be quantifying the log files values in this section, such as time, message repetition, and total message delivery time.

Trust value can be calculated by using Trust Metric only after we successfully map the log_file with the IoT Routing variables.

Let us consider the nodes to be as $s_1, s_2, s_3, \ldots, s_n$. So, we would define the initial value of trust to be zero, that is, $t(s_1) = t(s_2) = t(s_3) = \ldots = 0$. It is done to get a better understanding of trust. Destination node is found by routing the first message from the source node. For each sensor the value of remaining power is stored using p1, p2, p3…..pn. The initial value of all the power for every sensor is set to 100%. So, $p_1 = p_2 = p_3 = \ldots = p_n = 100$.

4.2 Computation and Learning

For computing the value of each node we need a function to quantify the variables:-

f(s1) = <Difference between time of the current and last messages trasnmitted f1, repetition of messages f2, total time taken to deliver a message f3>.

To build a neural network we assign weights w1, w2, w3 to f1, f2, f3 to erect the Binary Activation Function (Figure 4). Assigning the value of b (bias) = -999 (High negative value). Setting the null weight w0 = 1, fi = trust parameter and wn = weight allocated to each variable.

f1 = Difference between time of the current and last messages trasnmitted (i.e Time of current message - Time of Last message transmitted).

f2 = Repetition of messages (i.e Frequency) f3 = Total time taken to deliver a message.

$$w^1 - w^2 = w^3 \quad (1)$$

Where, w = 1, 2, 3…… ∞ .

For each node of wn function will be calculated for the other node that are, w1, w2, ... wn-1, wn, wn=1, wn+2, ... and so on. For each node wn a power value is generated and stored in the variable w=1, 2…. ∞ , which will be responsible for storing the battery power dynamically. The initial value for power for all the sensors will be set to 100.

$$f(v) = \Sigma\_(w=1),$$

$$y = v + b \; z = \text{ø}(y),$$

$$z = \begin{cases} 0 < 0 \; 1 \\ >=0 \end{cases} \quad (2)$$

The proposal of w2 and w3 to be equal to one is kept to find the correct values of f2 and f3 . Under any unwanted condition the value of bias is owned. Trust is computed for each device by each device for the trust metric construction. Since, w1 is the value of trust becomes inversely proportional to the value of f1. So if the time difference is low the value of trust will be high and contrariwise All the computed values of trust are kept in the cache. No negative or fraction value is considered. All the results must be absolute.

Notation:- Real Time variables are mentioned in Table I.

Sensors: s1 to sn.

Battery Power: p1 to pn.

t(old) = Trust value of the sensor on the last connection.

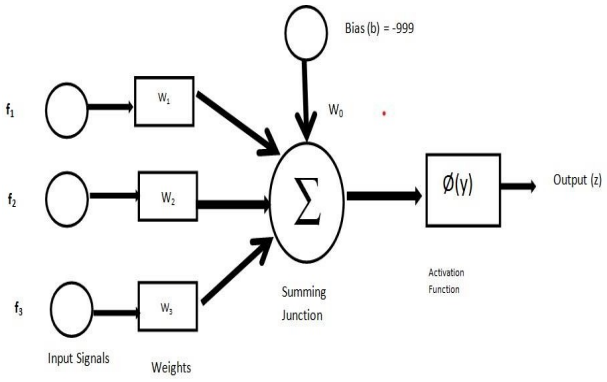
t(new) = Current value of trust

log_file = Data of Past Transmissions

Table 1: Real Time Variables

S.No.	*Real Time Variables*	*Variables Recognized*
1	Transmitting Sensor	Source
2	Battery power	Battery power value
3	Receiving Sensor	Destination
4	Start Time of message transmission	Start_Time
5	Time taken for message to reach from source to destination	Total_time
6	Event of calling	COM_SEND, COM_RECIEVE, COM_UNKNOWN, COM_BREAK or COM_DELAY
7	Route from which transmission of message started	Check trust metric
8	Route from which message left the exchange	Check trust metric
9	Fault event	Bias is activated, so b = -999

Fig. 4 Binary Activation Function using variables of trust.



5. Meta Physical Illustrations

5.1 Illustration 1

The initial values of all the sensors in the transference radius is set to be 0. The algorithm will work without the evaluation of trust values for the first time. The value of trust for all the sensors s1, s2, s3, s4 persists to be 0. Trust values for sensors s5, s6will be assigned as -∞. (Table II and Figure 5). Both the sensors are way apart from the other sensors and do not fall in the communication range of any other sensor.

So, t(s1, s2) = t(s1,s3) = t(s1, s4) = 0 and t(s1,s5) = t(s1,s6) = -∞.

Similarly t(s2,s5)=t(s3,s5)= t(s4,s5)= t(s2,s6)= t(s3,s6)= t(s4,s6)= -∞.

So the initial trust metric will be similar to the following table :-

Table 2: Trust Values of Sensors at Initial State

Sensor Node	*Receiver Node*	*Trust Value*
s1	s1	-
s1	s2	0
s1	s3	0
s1	s4	0
s1	s5	-∞
s1	s6	-∞

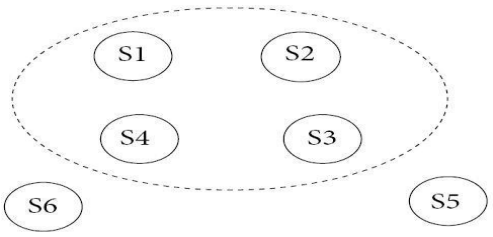


Fig. 5 Initial State

5.2 Illustration 2

Suppose that sensor s1 communicates with sensor s3 then the value of trust is calculated using the Artificial neural network and so, t(s1,s3) = t(s1,s3)+1. The table entries will

change accordingly in the following way. (Table III and Figure 6).

Table 3: Trust Values of Sensors for making forwarding decision

Sensor Node	*Receiver Node*	*Trust Value*
s1	s1	-
s1	s2	0
s1	s3	t(s1,s3)+1
s1	s4	0
s1	s5	-∞
s1	s6	-∞

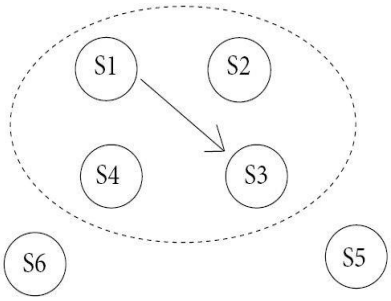


Fig. 6 Forwarding Decision

5.3 Illustration 3

Supposing that sensors s5 and s6 come in the communication range of sensor s1 at a given point of time, then,

t(s1, s2) = t(s1, s4) = t(s1,s5) = t(s1,s6) = 0 and t(s1,s3) = t(s1,s3)+1. (Table IV and Figure 7)

Table 4: Trust Values when all sensors are in communication range

Sensor Node	*Receiver Node*	*Trust Value*
s1	s1	-
s1	s2	0
s1	s3	t(s1,s3)+1
s1	s4	0
s1	s5	0
s1	s6	0

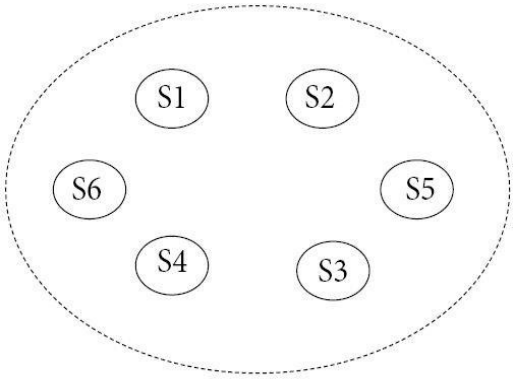


Fig. 7 All the sensors in communication range

5.4 Illustration 4

Assuming that sensor s1 is obtaining the same highest value of trust for two sensors, for example s3, s4then in that case, the path is identified using the most recent connection time, in case the value of f1 is also equal for both the sensors. (Table V and Figure 8).

Table 5: Equal Trust Values for two or more sensors

Sensor Node	*Receiver Node*	*Trust Value*
s1	s1	-
s1	s2	0
s1	s3	4
s1	s4	4
s1	s5	0
s1	s6	0

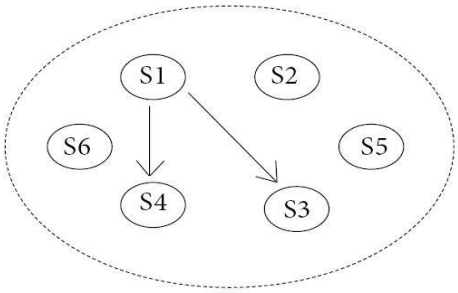


Fig. 8 Two paths for communication from a particular sensor

5.5 Illustration 5

Assuming that the most recent connection time and the value of f1 is also equal for both the sensors, which can be a case in big networks working with thousand's and lakh's of sensors, then we utilize the remaining battery power as a variable. The router will find the sensor with the highest amount of battery power remaining using the value of p and will direct the message towards that particular sensor. (Table VI and Figure 9).

Table 6: Equal Trust Values and most recent connection time for two or more sensors

Sensor Node	*Receiver Node*	*Trust Value*	*Most Recent Connection Time*
s1	s1	-	-
s1	s2	0	0
s1	s3	4	12.03
s1	s4	4	12.03
s1	s5	0	0
s1	s6	0	0

In this case the remaining battery power for both nodes s3 and s4 will be checked and the forward decision will be based upon the sensor which has the highest amount of battery power remaining.

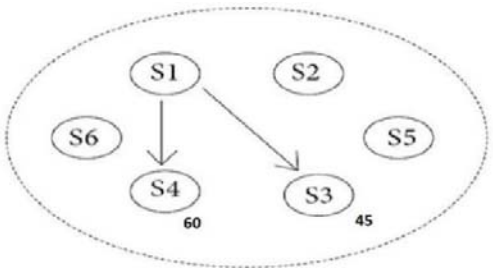


Fig. 9 Two paths for communication from a particular sensor along with their remaining battery power

7. Performance Computation

The proposed algorithm has been simulated using the cup-carbon simulator of IoT using five sensors with the maximum energy of 19160 J and having sensor radius of 20m. The algorithm also proceeds with the shortest path model.

Cup-carbon is used for the development of a smart city, which includes the validation and debugging of the algorithms and collection of data for all kind of IoT applications like smart homes, smart city, etc. It works on geographical locations by making use of Open Street Maps. One can easily program the working of the sensors by making use of Senscript (algorithm for sensors, routers, mobiles, etc.). On each and every simulation two types of files are generated namely, log file (contains all the events executed by a sensor in the particular simulation) and rst file (contains the energy level of a sensor during the simulation). It contains three scenarios: Wireless sensor network simulation, Multi agent simulation environment and mobile simulation. Cupcarbon is a growing tool and is advantageous for researchers, academicians and enthusiastic students.

The proposed algorithm makes use of sensors to demonstrate the communication channel of real time devices. It also makes use of the battery consumption feature of cup carbon simulator for breaking the tie in case the value of trust and value of last connection time for the sensors are equal. The performance is evaluated by using two routing protocols, LASER (Lightweight Authentication and Secured Routing Algorithm) and REL (Routing Protocol Based on Energy & Link Quality) with comparison to the proposed algorithm. LASER is used as it provides high deployment density of 40,000 nodes/km2 and is a reliable algorithm in terms of security and message delivery. RPL allows the use of energy accumulated from the smart devices and makes use of distance vector algorithm, while the proposed algorithm makes use of the remaining battery level of the nodes.

Performance is evaluated based on the variables simulation time (Figure 10), sent messages (Figure 11), received messages (Figure 12), lost/aborted messages (Figure 13) and the delivery probability (Figure 14). It is seen that the proposed algorithm has larger number of sent messages and also surpasses the other algorithms in the number of received messages and also takes very less time to simulate.

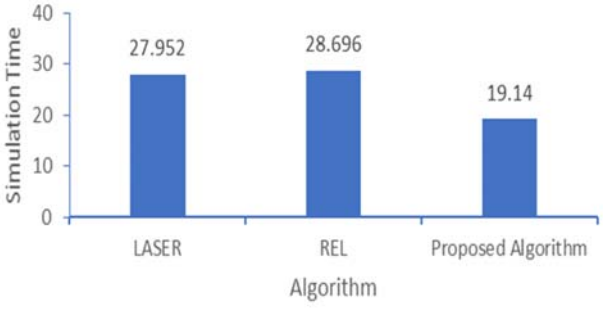


Fig. 10 Total time taken for simulation

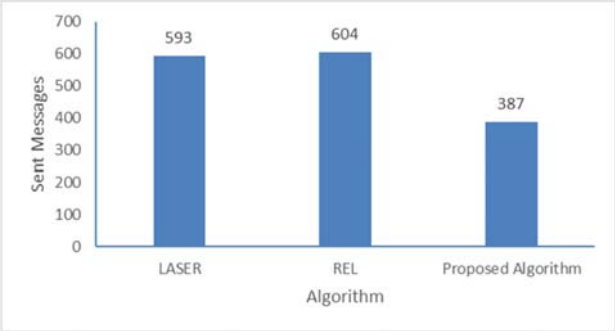


Fig. 11 Total number of message sent

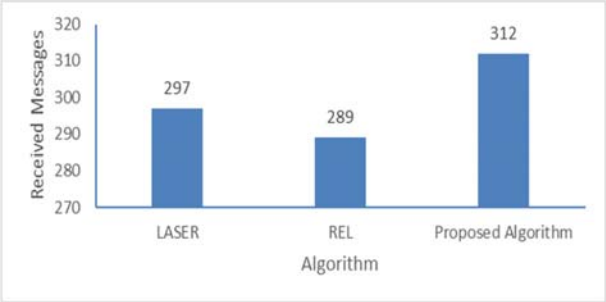


Fig. 12 Total number of Received messages

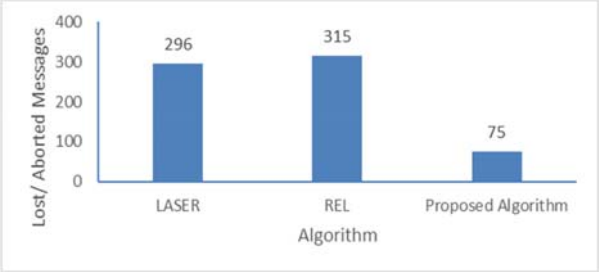


Fig. 13 Total number of Lost/Aborted messages

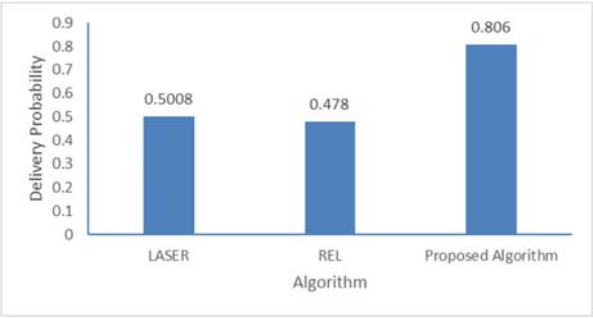


Fig. 14 Delivery Probabilities

8. Conclusion

IIn this paper, has made use of a trust based ANN. Trust is taken as a tool to guide for the forwarding decision. Trust is found to be a very practical approach for making routing decision, low routing overheads and is seen to be saving the evaluation time and also it does not require any form of authentication as compared to the other algorithms and thus it is said to have low security aloft. The implementation of trust in the practical world will lead IoT to greater heights, as it has low routing overheads, making the concept or emotion of trust to be quantified and also training the neural network to work according to this human behavior. The proposed algorithm works well, with more number of messages sent and received in comparison to the other algorithms namely, LASER and REL used in the paper. A certain amount of energy reduction and a skillfull use of energy as a variable is also achieved as the proposed algorithm makes use of the remaining battery power as a variable to sort out the tie in case the value of trust and the last communication time both result into equivalent value, which can occur in the real time network which involves large number of sensors, which is not a part of the traditional routing algorithms.

Acknowledgments

This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

References

[1] D. Meyer and G. Zobrist, "TCP/IP versus OSI," in IEEE Potentials, vol. 9, 1990, pp. 16-19.

[2] Tetsuya Yokotani, “Requirements on the IoT communication platform and its standardization”, IEEE, 2017, p.p:- 1-4.

[3] X. Jia, Q. Feng, T. Fan and Q. Lei, "RFID technology and its applications in Internet of Things (IoT)," 2012 2nd International Conference on Consumer Electronics, Communications and Networks (CECNet), Yichang, 2012, pp. 1282-1285.

[4] I. Turk, P. Angin and A. Cosar, "RONFC: A Novel Enabler-Independent NFC Protocol for Mobile Transactions," in IEEE Access, vol. 7, 2019, pp. 95327-95340.

[5] A. R. Chandan and V. D. Khairnar, "Bluetooth Low Energy (BLE) Crackdown Using IoT," 2018 International Conference on Inventive Research in Computing Applications (ICIRCA), Coimbatore, 2018, pp. 1436-1441.

[6] M. Condoluci, L. Militano, A. Orsino, J. Alonso-Zarate and G. Araniti, "LTE-direct vs. WiFi-direct for machine- type communications over LTE-A systems," 2015 IEEE 26th Annual International Symposium on Personal, Indoor, and

Mobile Radio Communications (PIMRC), Hong Kong, 2015, pp. 2298-2302.

[7] N. S. Zarif, H. Najafi, M. Imani and A. Q. Moghadam, "A New Hybrid Method of IPv6 Addressing in the Internet of Things," 2019 Smart Grid Conference (SGC), Tehran, Iran, 2019, pp. 1-5.

[8] RFC 8138 [Online]. Available: https://tools.ietf.org/html/rfc8138. 802.15.4 [Online]. Available:standards.ieee.org/content/dam/ieeestandards/standard/web/documents/erratas/802.15.4-2015-errata.pdf.

[9] M. Lukić, Ž. Mihajlović and I. Mezei, "Data Flow in Low-Power Wide-Area IoT Applications," 2018 26th Telecommunications Forum (TELFOR), Belgrade, 2018, pp. 1-4.

[10] N. Nasser, L. Karim, A. Ali, M. Anan and N. Khelifi, "Routing in the Internet of Things," GLOBECOM 2017 - 2017 IEEE Global Communications Conference, Singapore, 2017, pp. 1-6.

[11] Behera TM, Samal UC, Mohapatra SK, "Energy efficient modified LEACH protocol for IoT applications", IET wireless sensor systems, 2018, p.p:- 223-228.

[12] M. N. Jambli, M. I. Bandan, K. S. Pillay and S. M. Suhaili, "An Analytical Study of LEACH Routing Protocol for Wireless Sensor Network," 2018 IEEE Conference on Wireless Sensors (ICWiSe), Langkawi, Malaysia, 2018, pp. 44-49.

[13] Liu, X. A Survey on Clustering Routing Protocols in Wireless Sensor Networks. *Sensors* **2012**, pp. 11113- 11153.

[14] S. Iqbal, S. B. Shagrithaya, Sandeep Gowda G.P and M. B.S, "Performance analysis of Stable Election Protocol and its extensions in WSN," 2014 IEEE International Conference on Advanced Communications, Control and Computing Technologies, Ramanathapuram, 2014, pp. 744-748.

[15] K THOMAS, Aby; R, Vallikannu; ADVAIT NARAYANAN, Sai. Minimizing the energy consumption of WSN by using modified hybrid energy efficient distributed clustering protocol. **International Journal of Engineering & Technology**, [S.l.], 2018, pp. 758-763.

[16] O. Younis and S. Fahmy, "HEED: a hybrid, energy-efficient, distributed clustering approach for ad hoc sensor networks," in IEEE Transactions on Mobile Computing, 2004, pp. 366-379.

[17] Manjeshwar, Arati & Agrawal, Dharma. (2001). TEEN: ARouting Protocol for Enhanced Efficiency in Wireless Sensor Networks.. Intl. Proc. of 15th Parallel and Distributed Processing Symp.

[18] Galshetwar V.M., Jeyakumar A., "Energy efficient and reliable clustering algorithms HEED and ADCP of wireless sensor network : A comparative study", IEEE, 2014, p.p:- 1979-1983.

[19] Neha Rani, Pardeep Kumar, "Energy efficient hierarchical routing protocols for IoT", IJEAT, 2019, p.p:- 2122- 2125.

[20] Xue X., Leneutre J., Ben-Othman J. (2005) A Trust-Based Routing Protocol for Ad Hoc Networks. In: Belding-Royer E.M., Al Agha K., Pujolle G. (eds) Mobile and Wireless Communication Networks. MWCN 2004. IFIP International Federation for Information Processing, vol 162. Springer, Boston, MA, p.p : 251- 262.

[21] Ajay Vikram Singh, Vandana Juyal, Ravish Saggar, "Trust based Intelligent routing algorithm for delay tolerant network using Artificial Neural Network", Springer, 2016.

[22] Bounceur, Ahcene, et al. "A new dominating tree routing algorithm for efficient leader election in IoT networks." Consumer Communications & Networking Conference (CCNC), 2018 15th IEEE Annual. IEEE, 2018.

[23] Ahcene Bounceur, Madani Bezoui, Massinissa Lounis, Reinhardt Euler, Ciprian Terodorov, "A new dominating tree routing algorithm for efficient leader election in IoT network", IEEE, 2018, p.p:- 1-2.

[24] Hessam Mocini, I-Ling Yen, Farok Bastani, "Routing in IoT network for dynamic service discovery", 2017, IEEE, p.p:- 360-367.

[25] L. Qing, Q. Zhu and M. Wang, "Design of a distributed energy-efficient clustering algorithm for heterogeneous wireless sensor networks", *Comput. Commun.*,2006, pp. 2230-2237.

[26] S. Skiena, "Dijkstra's algorithm" in Implement. Discret. Math. Comb. Graph Theory with Math. Reading, MA:Addison-Wesley, 1990, pp. 225-227.

[27] T. Sharma, B. Kumar and G. S. Tomar, "Performance Comparision of LEACH SEP and DEEC Protocol in Wireless Sensor Network", *Proc. of the Intl. Conf. on Advances in Computer Science and Electronics Engineering*, 2012.

[28] T M Behera, SK Mohapatra, Proshikshya Mukherjee, HK Sahoo, "Work in Progress: DEEC-VD: A Hybrid energy utilization cluster based routing protocol for WSN for application in IoT", International Conference on Information Technology, 2017, p.p:-97-100.

[29] K Anusha, "Redundancy based WEP routing technology (IoT-WSN)", IEEE, 2015, p.p:-407-410.

[30] Bilal R. Al-Kaseem ; Hamed S. Al-Raweshidy, "Scalable M2M routing protocol for energy efficient IoT wireless applications", IEEE, 2016, p.p:- 30-35.

[31] R. Ahuja, "Simulation based Performance Evaluation and Comparison of Reactive Proactive and Hybrid Routing Protocols based on Random Waypoint Mobility Model", *International Journal of Computer Applications*, 2010, pp. 20-24.

[32] Yicong Tian, Rui HOU, "An improved AOMDV Routing

protocol for Internet of Things", CiSE, 2010, p.p:-1- 4.

[33] RFC 3626 [Online]. Available: https://tools.ietf.org/html/rfc3626.

[34] Travis Mick, Reza Tourani, Satyajayant Misra, "LASeR: Lightweight authentication and secured routing for NDN IoT in Smart cities", IEEE.

[35] RFC3626 [Online]. Available: https://tools.ietf.org/html/rfc3626.

[36] Paul Lon Ruen Chze, Kan Siew Leong, "A secure multi hop routing for IoT communication", IEEE, 2014, p.p:- 428-432.

[37] Wallgren, Linus, Shahid Raza and Thiemo Voigt. "Routing Attacks and Countermeasures in the RPL-Based Internet of Things." *International Journal of Distributed Sensor Networks* 9 ,2013.

[38] Guojun Ma, Xing Li, Quingqu Pei, Zi li, "A security routing protocol for Internet of Things based on RPL", International conference on networking and network applications, p.p:- 209-213.

[39] Michael Frey, Friedrich Grose, Mesut Gunes, "Energy aware ant routing in wireless multi hop network", IEEE, 2014, p.p:- 190-196.

[40] Sharief M.A. Otcafy, Fadi M al-Turjman and Hossam S. Hassancin, "Pruned adaptive roputing in the Heterogeneous Internet of Things", IEEE, 2012, p.p:- 214-219.

[41] Amol Dhumane, Rajesh Prasad, Jayshree Prasad, "Routing issues in Internet of Things: A survey", IMECS, 2016.

[42] Prasad P. Lokulwar, Dr. Hemant R. Deshmukh, "Threat analysis and attacks modeling in routing towards IoT", IEEE, 2017, p.p:-721-726.

[43] Abderrahim, Oumaima Ben, Mohamed Houcine Elhedhili, and Leila Saidane. "DTMS-IoT: A Dirichlet-based trust management system mitigating On-Off attacks and dishonest recommendations for the Internet of Things." In 2016 IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA), pp. 1-8. IEEE, 2016.

[44] Airehrour, David, Jairo Gutierrez, and Sayan Kumar Ray. "Secure routing for internet of things: A survey." Journal of Network and Computer Applications 66 (2016): 198-213.

[45] Nabil, D., D. Tandjaoui, I. Romdhani, and F. Medjek. "Trust-based defence model against mac unfairness attacks for iot." (2017).

[46] Gonzales, Dan, Jeremy M. Kaplan, Evan Saltzman, Zev Winkelman, and Dulani Woods. "Cloud-trust—A security assessment model for infrastructure as a service (IaaS) clouds." IEEE Transactions on Cloud Computing 5, no. 3 (2015): 523-536.

[47] Guo, Jia, Ray Chen, and Jeffrey JP Tsai. "A survey of trust computation models for service management in internet of things systems." Computer Communications 97 (2017): 1-14.

[48] Khan, Zeeshan Ali, Johanna Ullrich, Artemios G. Voyiatzis, and Peter Herrmann. "A trust-based resilient routing mechanism for the internet of things." In Proceedings of the 12th International Conference on Availability, Reliability and Security, pp. 1-6. 2017.

[49] Medjek, Faiza, Djamel Tandjaoui, Imed Romdhani, and Nabil Djedjig. "A trust-based intrusion detection system for mobile RPL based networks." In 2017 IEEE international conference on Internet of Things (IThings) and IEEE green computing and communications (GreenCom) and IEEE cyber, physical and social computing (CPSCom) and IEEE smart data (SmartData), pp. 735-742. IEEE, 2017.

[50] Truong, Nguyen Binh, Hyunwoo Lee, Bob Askwith, and Gyu Myoung Lee. "Toward a trust evaluation mechanism in the social internet of things." Sensors 17, no. 6 (2017): 1346.

[51] Wu, Tao, Qiusong Yang, and Yeping He. "A secure and rapid response architecture for virtual machine migration from an untrusted hypervisor to a trusted one." Frontiers of Computer Science 11, no. 5 (2017): 821-835.