Semiconductor Optoelectronics
ISSN: 1001-5868

A NOVEL SECURITY MECHANISM FOR INTERNET OF BATTLEFIELD THINGS USING TRUST AND K-NEAREST NEIGHBOR ALGORITHM

[1]P. Rutravigneshwaran and [2]G.Anitha
[1]Research Scholar, [2]Associate Professor,
[1,2] Department of Computer Applications
Karpagam Academy of Higher Education
Coimbatore -641021 , Tamilnadu State, India
[1]rutra20190@gmail.com, [2]florenceanitha7@gmail.com,

Abstract
IoBT (Internet of Battlefield Things) is one of the most significant application domains in the field of IoT to enhance mission effectiveness on the battlefield. A key function of IoBT is to connect various IoBT nodes in order to communicate with each other. The special characteristics of IoT, suitable for group-based communication like battlefield networks. The Routing Protocol for Low Power and Lossy (RPL) is for the most part utilized in everyday IoT as well as in the IoBT networks. It consumes fewer resources; however, it is highly susceptible to various internal attacks. Therefore, the information that has been exchanged in the IoBT environment is unsafe. Black hole and selective forwarding attacks are the two internal attacks that harm the IoBT environment seriously. The proposed security mechanism aims to detect and eliminate those attacks with the help of trust management along with machine learning algorithm is called K-Nearest Neighbor Algorithm (KNN). Here, the trustworthiness of nodes will be assessed with the help of both direct and indirect trusts. After that, KNN algorithm will be used to classify the nodes into malicious or not. The proposed security model will be assessed by various performance metrics including delivery ratio, detection accuracy, average delay and routing overhead and also compared with existing similar models. The results has witnessed the effectiveness of the proposed model.

Keywords—Internet of Battlefield Things, RPL, Security, Trust, Blackhole and selective forwarding attacks, K-Nearest Neighbor algorithm.

1. INTRODUCTION

The advancements of smart devices and extraordinary network facilities leads to promising technology called Internet of Things (IoT). It is getting popularity as they have resource constrained resources. It is defined as the collection of smart devices or objects or things or entities and those are connected together over a public or private network to provide a seamless service to the users. The smart devices are embedded with sensors to sense the information from outside environment by the way it will react based on the situation [1]. IoT offers many application domains including Agriculture, Transport, Education sector, Hospitals, Smart cities, Logistics, Industries and etc. Among the applications, battled field environment is adopting the features of IoT to provide high level operations efficiency and it becomes Internet

of Battlefield Things (IoBT) [2].

In an existing military network, sensors and IoT devices are attached to the applications which provide accurate and full information about the battlefield and also enable situation awareness decision making by the commander and soldier. The integration of IoT with the existing military networks creates the Internet of Battlefield Things(IoBT)[3].

The future battlefield will consist of massive heterogeneous smart things such as Planes, Drones, Wearable devices, Ships, Cameras, Military Tropes and etc and most of them are highly intelligent and rest are minimal intelligence. The Battlefield things will include sensors, weapons, vehicles, robots, munitions, and wearable devices [4].They are performing various activities such as sensing the outside environment with the help of embedded sensors, making communication with other smart devices, reacting based on the environmental conditions and cooperating with other smart things [2]. The task of the IoBT devices is to selectively collect and process the information, sense-making, coordinate-ally take decisions for a certain action, and discharge different types of effects on the attacker.

In addition to physical attack with soldiers and the IoBT devices, the adversary also attacks the information that is transferred between IoBT nodes [4].

In general, IoBT is highly susceptible when compared to the commercial IoT, because of the adversarial feature in the battlefield environment [5].

In a real-time implementation, the IoBT application has to be overwhelmed for a new set of challenges. For instance, interaction among IoBT nodes has to be adaptable and flexible to a promptly changing environment and mission. Besides the advantages of the IoBT application on the battlefield environment faces numerous problmes because of the following factors; resource constrained nature of IoBT nodes, dynamic battlefield surroundings, unpredictable environmental conditions, open and shared environment, security threats from both internal and external attacks, blindness communication with participating battlefield things and etc. The adversary threatens the integrity, confidentiality, and availability of the information in the IoBT via malware and eavesdropping. They may perform the following illegal activities, obtaining mission-critical information in the battlefield (violates its confidentiality), attempt to modify the obtain information through the malware (violates the integrity of the messages), inserting unauthorized IoBT devices, interrupt and corrupt the IoBT devices, and sending wrong information to the data acquiring devices in the battlefield. With the massive density of IoBT devices in the battlefield requires an efficient lightweight security mechanism. To identify the attacks, machine learning-based approaches are required to deal with the huge amount of data in the IoBT environment [4].

Ensuring trustworthiness in group-based communication is always a trivial task as things in the environment are communicating with each other without prior knowledge and interactions. To accomplish mission related tasks, cooperation and team work among the participating devices are important. This can be achieved by ensuring trustworthiness among the participating devices. The proposed model ensures the trustworthiness among the participating devices by eliminating the internal attacks such as Blackhole and Selective forwarding attacks. It can be entrenched through traditional RPL routing protocol to ensure secure routing.

In battlefield environment, both Quality-of-Service and social trusts are important to achieve a mission. Therefore, the proposed trust-based solutions consider both QoS and Social trust. Each IoBT node selects the one-hop neighbor nodes based on direct and indirect trust. Then,

the KNN algorithm will be applied to predict the future behavior of the nodes.

Depending on this prediction each node selects its one-hop neighbor for forwarding the data packets. Trusted nodes are most effective and concerned with inside the mission and malevolent nodes are eliminated from battlefield zone organization to improve mission's effectiveness. Eliminating malicious nodes and selecting trusted identity for missions can ensure the authentication and provide security on the battlefield network environment.

Contribution

The contributions of the proposed KNNTrust model as follows;

- The Routing Protocol for Low power and Lossy Network (RPL) will be examined initially followed by adversary model on RPL protocol will be discussed.
- Presented the fundamental introduction of the K-Nearest Neighbors (KNN) Algorithm.
- Trust evaluation will be done with the help of direct and indirect trusts then how the KNN algorithm can be used to classify the IoBT node's behavior will be explained. In addition, the role of KNN algorithm in future prediction of the nodes also explained.
- Presented the new filtering algorithm to filter the dishonest recommendation.
- A proposed model involves trust calculation among the IoBT nodes by means of both Direct Trust (DT) and Indirect (IT). Social trust and QoS trust are taken into considered to estimate the DT of the IoBT nodes. It uses the simple weighted average technique to aggregate of the trust metrics. A new filtering algorithm used to filter the unfair recommendation and indirect trust is calculated only from honest recommendation by taking a simple average. KNN algorithm takes these direct and indirect trust as contributions and guesses nodes future behavior such as Trusted or Malicious.
- With the help of KNNtrust model attacks of the black hole and selective forwarding are identified and eliminated from the network. So that authentication i.e trustworthiness of individual nodes will be ensured.
- The efficiency of the KNNTrust model is compared to similar existing works with different performance metrics.

2. RELATED WORK

The following section discusses the related work. Many researchers have been addressed the security related issues by providing various security solutions in terms of cryptographic based solutions, repudiation-based solutions, Intrusion Detection System (IDS) based and trust-based solutions. Here, some of the notable works are discussed herein.

In[6] authors(Patel, H. B et al.,2019) present a strainer based mechanism for intrusion detection in 6LoWPAN for the IoT to counter black hole attack on RPL. This model first creates a suspect list from the behavior of the node then these nodes are verified by its neighbor node during the network operation. Finally, the root node discards malicious nodes from the network. This model analyzes malicious nodes only. In[7] authors(Kandhoul, N., et al.,2019) proposed a reputation-based approach to provide security for opportunistic IoT where the trust evaluation is done for each node based on its behavior in the network. Malicious nodes are detected and avoided from the routing. Every node in the network maintains two lists: one is a trusted nodes list that is used to involve the message transmission and another one is a malicious

nodes list that is avoided from the transmitting messages.

In [8] authors (Airehrour D et. al.,2017) suggested a trust solution used for addressing selective forwarding attack, black hole attack in IoT network. fuzzy logic to identify trusted nodes and selected the trusted routing path for successful data packet transmission. In [9] authors (Conti et. al.,2017) aimed a harmless and extendible routing protocol in the IoT networks. Here, a lightweight attestation tool to ensure the honesty of the node. Piggyback's attestation is evaluated by the switch messages of RPL and ensures security in the IoT network. In [10] authors presented a distributed approach based on trust for IoT against black hole attack. Every node computes the trust measures of its close nodes in IoT network, which are collected by the border router or the cluster head to compute the reputation score. Finally, those values are used to find the black hole attack in the network.

In [11] authors (Mehta.R & Parmar.M. M. (2018)) present a trust related model used secure RPL to mitigate wormhole attack and gray hole attack. Direct trust computed from the trust properties called forwarding check and ranking check. Total trust is estimated with the aggregation of the DT and IT. The final trust forms in downward order are inserted into the RPL together with Rank and ETX.The data packets are forwarded through the trusted nodes by selecting high trust values nodes. Thus, malicious nodes are separated in the network. (Lim, J., et al., 2018) [12] present an energy-efficient trust computation model in a military IoT environment using stepwise tree-structured routing. In this model trust computation process done only by parent nodes when they suspect the malicious behavior of the child nodes. The trust computation process is done in two phases: the child node inquires to its parent node and local calculation of the trust value. Liang Liu et al., 2019 [13] proposed perceptron detection approach to evaluate the trust worthiness of IoT nodes. Both k-mean algorithm and perceptron are used to evaluate the trust worthiness of the nodes. The aim of the proposed approach is to detection of multiple mix attack that harm the IoT environment. Mohamed Tahar Hammi et al., 2017 [14] proposed a blockchain based security system for IoT devices. The aim of the proposed work is to ensure the authentication along with it ensures the availability and data integrity. It uses the concept called “Bubble of Trust” where collection of secure IoT things to form a virtual zone. King-Hang Wang et al., 2017 [15] proposed a security scheme for IoT based on the key agreement and aim is to ensure the authentication among IoT devices. Yasmine Harbi et al., 2019 [16] proposed a key management based secure protocol to address the issues of authentication. This work addresses the multiple attacks such as denial of service attack, impersonation attack, replay attack.

The proposed research work varies from the existing research work mentioned above. This model uses a KNN machine learning algorithm to identify malicious and trusted nodes. The trusted(authenticated) IoBT nodes only selected for communication and malicious nodes are disconnected in the network. Authentication in the IoBT environment can be succeeded using this approach.

3. BACKGROUND

This section represents an overview regarding the RPL protocol and a brief representation of the K-Nearest Neighbor Algorithm.

3.1 RPL Overview

Routing Protocol for Low Power Lossy Network (RPL) has developed for resource restricted devices within the network position. Resource constrained in relationships of memory storage,

limited power and processing resources. Typically, this Lower Power Lossy Networks (LLN) are embedded with sensor and connected by minimal power Wi-Fi or IEEE 802.115.4. RPL is based on source routing protocol and distance vector protocol. The source routing refers the sender node will hold the entire or partial entire network address by the way it enables to discover all the possible routes in the network. Distance vector routing refers a node has vector of distances to another nodes in network. The information about the topology changes will update periodically. Hence, RPL organizes topology as a Directed Acyclic Graph (DAG). It rooted with single Destination Oriented Directed Acyclic Graph (DODAG root) and it has no outgoing edges. A combination more than one DODAGs is called RPL example that shared the same RPL Instance ID. The instances are used to identify and maintain the network topologies. Then, the RPLInstanceID is an exclusive identifier within the network. DODAG Version number is an iteration of a DODAG with given DODAGID. The root node will increment the sequential counter to form a new version number. RPL performs two mode of operations such as storage mode and non-storage mode. In storage mode, it keeps track of download routing table at each node in the network. Whereas, in non-storing mode, it leads over all the circulation to the root node afterward root node purposes of the source routes and send traffic to all leaf nodes in the network. In RPL, the following control messages are used such as ICMPV6, DODAG Information Solicitation (DIS) and DODAG Information Object (DIO), Destination Advertisement Object (DAO), Destination Advertisement Object Acknowledgement (DAO-ACK). Another important function used in RPL is Objective Function (OF). It acts a most important role in how the nodes are selecting their parent nodes, how the RPL nodes transfer one or more functions into a rank and how the best and optimal routes are selected in RPL.

3.2 Overview of k-Nearest-Neighbours (kNN)Algorithm

K-Nearest Neighbors algorithm is quite simple yet effective machine learning technique for classification. Due to less computation time and easy interpretation, the KNN algorithm is widely used[19]. It is a traditional non-parametric classifier[20].

It is used to classify the entities, depending on the nearest sample instance in the feature space[22]. It holds all the sample data for classification[21]. This algorithm is a lazy learning algorithm because all the calculations of the KNN algorithm are rough and stored locally and it may be changed at any time before the classification. It requires a training data set, but it does not learn or build any model from the training phase. It aggregates the training data set of the search space with a known class of the objects. During the testing phases, only all the training data sets are required, it does not generate any generalization in the training phase. The unknown class object given for testing, the KNN algorithm calculates its K- closest neighbors, and the class of the new object is determined based on the voting of these neighbors. The training phase of these algorithms is rapid but the testing phase is expensive.

There are two phases in the KNN algorithm: Training and classification phase. In the training phase, the sample training instances are vectors(each instance assigns a class label) in the feature space. Feature vectors and class labels of sample instances are saved in this training phase. In the classification phase, a user-defined constant k is an examination data(unknown vector) is categorized and assigned by a label, which is often repeated in association with k training instances closest to that examine data. It means the KNN algorithm correlates the examine data or a query point with the stored training vectors, and the examine data is labeled

with the closest class of saved training vectors. This technique of classifying examination data depending on its interval to data in the training vectors is simple, however, this is an efficient technique of categorizing unknown data. The main advantage of the KNN algorithm needs only some metric: distance metric and parameter K are enough to achieve high accuracy in classification. Typically, selecting the highest K value decreases the impact of noise on the classification.

Thus, the selection of K value and distance metric for estimating the closest distance is a difficult task in the KNN based application[22].

The K-NN algorithm uses different measures of distance, but popularly used measures are Euclidean distance and the Manhattan distance Various measures for distance can be used in k-NN[19].

The Euclidean distance is represented as follows

$$d(x,y) = \sqrt{\sum_{i=1}^{n}(x_i - y_i)^2} \quad (1)$$

The Manhattan distance is represented as follows

$$d(x,y) = \sum_{i=1}^{n} |x_i - y_i| \quad (2)$$

In this proposed work, euclidean distance is used, it can be affordable, satisfies the performance of prediction, and computation is also relatively easy.

4. KNNTrust Model (K-Nearest Neighbor Trust)

The main aim of the proposed KNNTrust is to perceive and mitigate block hole attacks and selective forwarding attacks in the battlefield network surroundings. This model evaluating the reliability of node's behavior based on their previous interaction to detect malicious nodes. Even though malicious nodes may perform several malicious activities, this paper focused on the most common two attacks that occur on the battlefield environment including black hole attack and selective forwarding attack.

Although lightweight authentication protocol and some encryption methods may prevent external attacks, it is difficult to defend against internal attacks, these attacks are performed by the internal nodes with legal identity[23]. Therefore, the trust aware model to detect node behavior is very effective in network security. Identifying these attacks on the battlefield network and discard the malicious IoBT nodes from the network can ensure security. This model assures the authenticity of the data packets by selecting only trusted(authenticated) IoBT for the routing process on the battlefield environment.

4.1 Network Model Suppositions

The KNNTrust model has the following suppositions;

1. The proposed method assumes the network nature as Internet of Battlefield Thing (IoBT) environment. This network consists of various IoBT nodes that are attached to the soldiers and military vehicles. To successful mission completion, these IoBT nodes should communicate and collaborate.
2. Dynamic Topology: Devices involved in IoBT actions from one network to another environment.
3. Heterogeneity: The devices involved in IoBT are differing in their resources such as process-speed, memory, storage capacity, energy and involving technologies.

4. A node with high capacity will be treated as a border origin node and this node is held by the commander.
5. Decentralized Network: there is no central administration in IoBT hence every node will play as ordinary node as well as forwarding node.
6. Malicious IoBT nodes perform data packet drop attacks or selective forwarding attacks to interrupt the mission.

4.2 Adversary Model

In this paper, the behavior of the IoBT nodes is considered malicious, when the node completely or selectively drops the data packets. In the battlefield environment, these attacks cause severe problems. For example, soldiers may transfer the mission-critical information to the commander through the intermediate nodes, malicious nodes may completely drop or selectively drop the information thus leading to failure in mission or even risk to the soldier's life. The nodes which are compromised by an attacker are called malicious nodes and aim of these nodes to degrade the routing protocol performance and interrupt the mission.

4.2.1 Blackhole Attack

In this kind of attack, the misbehaving nodes drop all the data packets that are supposed to forward to their neighbor nodes [24].

4.2.2 Selective Forward Attack

The intention of selective forwarding is to collapse the routing path by intruder the data packets selectively to the target nodes.[25].

Figure 1. A Typical RPL Network without any attacks

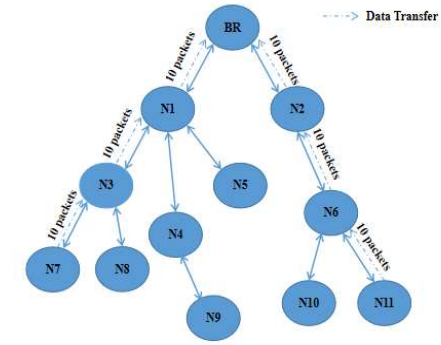

Figure 2. A Typical RPL network with Blackhole and selective forward attacks.

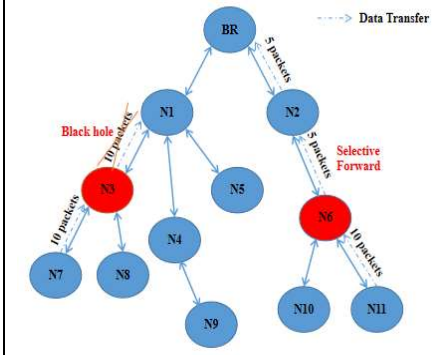

Figure.1 shows the example RPL network scenario without any attacks. Where nodes N7 and N11 conversion the data packets to the Borderline Root though intermediate node, without any loss, data packets are reached to the Border Root because of all the nodes in the RPL network are trusted and authenticated.

Figure.2 shows the example RPL network scenario with the black hole and selective forward attacks. Node N7 and N11 transfer the data packets through node N3 and Nod N6. bWhere node N3 launches the black hole attack which drops all the data packets that are supposed to forward to its neighbor node N1. Node N6 launches the selective forwarding attack which selectively drops the data packets that are transferred through these nodes.

These two attacks are very dangerous on the battlefield network which leads to failure in mission. Mission-critical information may transfer from soldier to commander or from

commander to soldier through intermediate nodes. If anyone of the intermediate nodes (malevolent nodes) can completely or selectively abandon the data packets then the information cannot be reached to the target person, it leads to risk in a soldier's life or increases the chance of failure in mission.

The primary aim of the KNNTrust model is to find the block hole and selective forward attacks and identify the malicious nodes which perform these attacks and then discard these nodes from the network.

4.3 Trust Management

The important task of trust management is to collect various needed information for trust estimation.[26]. Typically, Trust is described by Quality of Service(QoS), honesty, availability, risk, and other factors. It is characterized as a satisfied level on one node by another node based on the observation from the past behavior. [27]

The proposed trust model is specially designed for the IoBT application. Each IoBT node in the battlefield network estimates the direct trust of its nearby nodes. Also, this direct trust value transfers to other nodes as a recommendation value to compute indirect trust. Recommendation trust managers collect various recommendation values and filter the dishonest recommendation then compute the indirect trust form the honest recommendation. By using these two trust KNN algorithms predict the node behavior.

4.3.1 KNNTrust Model

The trust computation in KNNTrust can be done with both direct and indirect trusts. To execute direct trust method, the subsequent trust methods are used such as forwarding reliability, contact intimacy, and honesty are aggregated using the weighted average method. In indirect trust computation, trusted node requests and receives recommendation values from common neighbors about trustee nodes. To avoid dishonest recommendations, a filtering technique is used in this mechanism. Finally, Indirect trust is intended from the honest node's recommendation. KNN algorithm to analyze and predict the node's performance basis on the previous set of direct and indirect trust value. In the battlefield environment, as soldier’s life also must be considered hence social trust metrics also considered along with social trust metrics are evaluate the honesty of the node. Therefore, KNNTrust model uses both societal trust and QoS(Trust) properties for estimate the trustworthiness of the node in battlefield environment.

QoS trust indicates to the forwarding reliability in the particular node that is whether a particular node correctly forwarding the packet or not to the destination node. Otherwise, it also denotes the belief of the node [28]. Social relationship between the owners of IoT represented by social trust. It includes honesty, intimacy, centrality and etc. [29]. In this proposed model, trust metrics such as honesty and intimacy are used as the social trust metrics.

4.3.1.1 Direct Trust: It is estimated based on the observation from the direct experience. It shows the relationship between the nodes based on their trust[27]. This calculation depends on many trust properties for a particular node based on the several interactions that occur in the network [26]. It is derived from the neighbor nodes, it is first-hand information and it can be obtained easily and reliably as a source of information.[30].

Computation of direct trust in KNNTrust model depends on forwarding reliability, contact intimacy, and honest trust methods are used. It is established on the impact of the black hole and selective forwarding attacks; the trust metric is preferred in proposed model.

IoBT node i evaluates the direct trust value of IoBT node j as follows.

$DT_{i,j}(t)=w1.FR_{i,j}(t)+w2.CI_{i,j}(t)+w3.H_{i,j}(t)$ (3)

w1+w2+w3=1

$FR_{i,j}(t)$ - Forwarding Reliability at 't' time.

$CI_{i,j}(t)$ -Contact Intimacy at 't' time

H(t)- Honesty at 't' time (based on number of positive and negative interaction in node i and node j)

$DT_{i,j}(t)$ - Node i compute direct trust for node j based on the experience.

The following trust methods are used in this model;

Forwarding Reliability

This metric is used to measure the QoS trust. It is defined as forwarding the data packets correctly without any loss or modification. Higher-level packet loss or data modification refers to a lower level of reliability. Selfish nodes will abandon the data packets are supposed forwarded to their neighbor for energy saving. Malicious nodes abandon or modify the data packets to disturb the operation and degrade the network performance. The forwarding reliability can be used to differentiate the trusted node from the malicious or selfish node. It is defined as follows

$$FR_{i,j}(t)= CFP_{i,j}(t)/RP_{i,j}(t) \quad (4)$$

$CFP_{i,j}(t)$ - represents overall collection of correctly forwaded data packets through the node i with respect to node i at 't' time.

$RP_{i,j}(t)$ - signifies the amount of received packets by the node j with respect to node i at 't' time.

$FR_{i,j}(t)$-Forwarding Reliability of node j measured by node i.

After every communication, node i measure the forwarding reliability of its neighbor node j through acknowledgment [31].

Contact Intimacy

It is essential trust metrics to compute the social trust. It measures the intimacy between two nodes using the interaction count. When the node has the highest number of contact frequencies with the particular node, then the contact intimacy between these nodes also will be high. The probability of forwarding ratio from the node with the highest contact intimacy is higher. Contact Intimacy is estimated as follows.

$$CI_{i,j}(t)= CF_{i,j}(t)/TCF_i(t) \quad (5)$$

$CF_{i,j}(t)$ - Contact frequency in node i , node j at 't' time.

$TCF_i(t)$ - Total number of contact frequency with all other nodes by node I[32].

Honesty

It is also one of the important social trusts in estimating the trustworthiness of the participating nodes. The abnormal behavior of the nodes are analyzed with the help of this trust metric. The analyzes can be done with total number of both positive and negative communications between two nodes. Hence, the following beta function will be handled evaluation the honesty measured of two nodes. The honesty trust measured is described as follows.

$$H_{i,j}(t) = \alpha_{i,j}(t)/\alpha_{i,j}(t)+\beta_{ij}(t) \quad (6)$$

$\alpha_{i,j}(t)$- number of positive communication within node i and node j.

$_{i,j}(t)$ - number of positive communication within node i and node j.

$\alpha_{i,j}(t)+\beta_{ij}(t)$ - It denotes the overall positive communication between node i and node j.

i -Evaluated node

j- Evaluating node[33]

4.3.1.2 Indirect Trust

Some certain cases direct trust is not enough to evaluate the trust worthiness of the particular node. In that case indirect trust will be used and it is also called secondhand information [26]. It is derived from other trustworthy third party nodes. Recommendation trust is an essential feature in any trust computation system[30]. In the KNNTrust model, the evaluated node requests the recommendation trust for evaluating nodes to its neighbor nodes. The evaluated node receives a huge number of responses from its neighbor nodes. These responses from both honest and dishonest third party nodes. Due to the distributed network, there is possible to many malicious nodes, it intentionally provides the wrong recommendation. To differentiate the dishonest recommendation from the network, the proposed model uses the following filtering algorithm.

Algorithm 1 Indirect Trust Computation

Step 1: Evaluated node request recommendation trust to its neighbor nodes about evaluating node.

Step 2: Evaluated node receives recommendation trust from its neighbor nodes for evaluating nodes.

Step 3 : $RT_i = \{ RT_1, RT_2, RT_{3,\ldots..}, RT_n\}$

Step 4: Find the median m from the Recommendation trust set.

Step 5: Find the distance between recommendation trust and median using the one-dimensional Euclidean equation.

Step 6 : for i =1 to n

Step 7 : $d_i = | RT_i - m|$ //RT_i - Recommendation Trust of i^{th} recommender node

Step 8 : sum = sum+d_i

Step 9 : end of loop

Step 10 : mean= sum/n

Step 11 : for i = 1 to n

Step 12 : if(d_i <= mean)

Step 13 : TRT = TRT+ RT_i // Total Recommendation Trust from honest nodes

Step 14 : j = j +1 // Total Number of honest node

Step 15 : endif..

Step 16 : endofloop…

// Indirect Trust calculation

Step 17 : IT = TRT / j

Step 18 : End

This algorithm filters out the dishonest recommendation using mean, median, and Euclidean distance equations. From the set of recommendation trust(RT_i), the median is calculated, then the Euclidean distance is calculated between each recommendation trust and median. The mean value is computed for a set of distance values (d_i). when the distance value is above the mean value then the recommendation is dishonest that is filtered from the recommendation set. Indirect trust is calculated only from the honest recommendation using a simple average.

4.3.1.3 Identifying Malicious nodes

Implementation of KNN Algorithm

Each IoBT node in the battlefield network maintains the direct and indirect trust of neighbor nodes. In the training segment of the KNN algorithm, each IoBT node realizes the node's behavior from the collection of direct and indirect trust. These previous sets of data are also known as training sample data. The evaluated node can guess the evaluating nodes actions using direct trust and indirect trust value in the classification segment of the KNN algorithm.

Algorithm 2: Classifying and predicting node's activities (Trusted or Malicious)

Step 1: Compute the similarity between current data and all the training data based on the distance function (Euclidean distance).

Step 2: Decide the K value (K= number of nearest neighbors)

Step 3: Assign a rank to the distance and find k nearest neighbors based on the k value. (From the least distance rank is assigned)

Step 4: Distance with greater than the k value is ignored.

Step 5: Based on the majority of the node behavior from the selected nearest neighbors, a new node's trust behavior is predicted.

As malicious nodes are disconnected beginning from the network environment. So, it will not be involved in the network environment. As already mentioned, the IoBT root node is held by the commander who will notify the details about malicious nodes to other nodes. Hence, genuine nodes remove the links from the malicious nodes as per the commander notification. Because of this reason only honest nodes concerned within the network and malevolent nodes discarded from the network. Thus, ensures authentication in the battlefield environment. The following figure 3 explains the general design of the KNNTrust model.

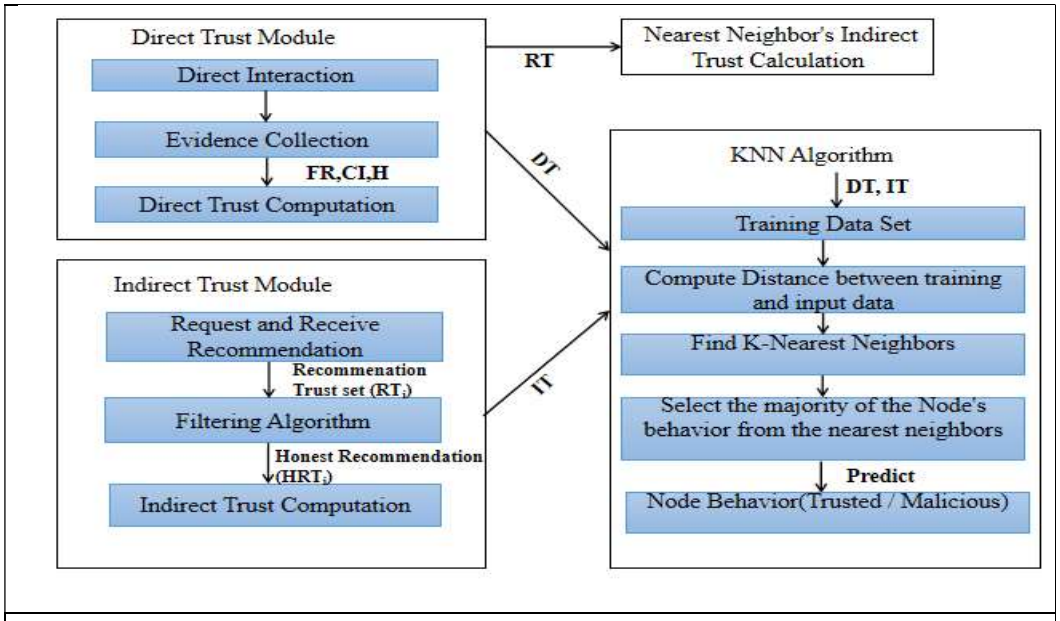

Figure 3. The overall design of the KNNTrust Model

5. SIMULATION RESULTS AND DISCUSSION

5. 1. Performance Evaluation Metrics

The proposed trust model implemented and analyzed in the Contki 3.0 OS and the Cooja

simulator. The mote type model used in this model is TMote Sky(Sensor nodes). The following simulation parameters will be used for the proposed KNNTrust model.

Table 4. The Simulation Parameters of the Proposed KNNTrust Model

System Parameters	Values
Maximum of no.of nodes	75
Mote Type	TMote Sky
Simulation Time	3600Sec
Network Coverage Area	500mx500m
Data Rate	3072bps
Data Packet Size	128 byte
Traffic	UDP
Mac Layer	IEEE 802.15.4
Communication Range	50m
RPL Parameter	MinHopRankIncrease =256
Routing Protocol	KNNTrust, RPL, David et al., 2017

5.2 Simulation Results

The following test cases are used in the proposed KNNTrust model.

1. The main objectives of the KNNTrust model are to detect and eliminate the block hole attack and selective forwarding which perform malicious activities. Hence, it is required to recognize the impact of them. Thus, it can be analyzed by increasing the number of malevolent nodes and evaluate the data packet abandoning ratio.
2. The efficiency of the KNNTrust is assessed with the RPL and David e al., 2017[8] in relations of several performance metrics such as forwarding Ratio of data packet, Average Delay, and Routing Overhead.
3. The detection accuracy of KNNTrust with David et al., 2017 will be measured with increasing percentage of malicious nodes.

Scenario 1: This is the first experiment and it is operated to know the impact of malicious nodes in the network environment. Whenever, malicious nodes are increasing the packet dropping ratio has also increased gradually. This can be done with standard RPL routing protocol. The figure 5. Clearly shows the impact of malicious nodes and it clearly depicts

whenever the malicious nodes growth the packet drop also increases.

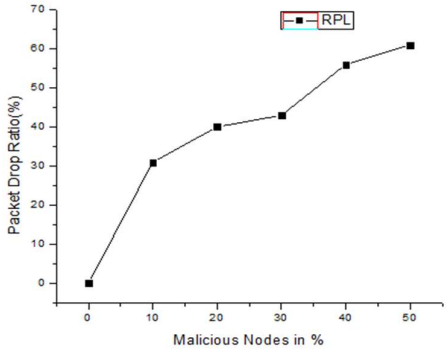

Figure 5. Effect of the Malicious nodes under normal RPL routing protocol

Scenario 2: In this scenario, the performance metrics such as packet forwarding ratio, average delay and routing overhead will be analyzed. As mentioned earlier, the proposed KNNTrust model has compared with traditional RPL and David et al., 2017.

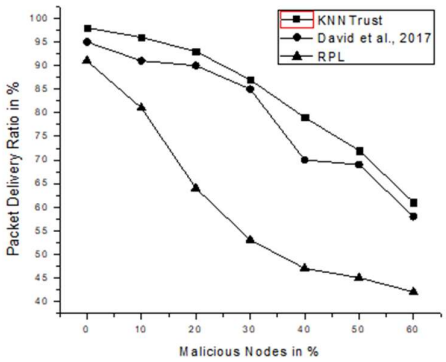

Figure 6. Packet Delivery Ratio

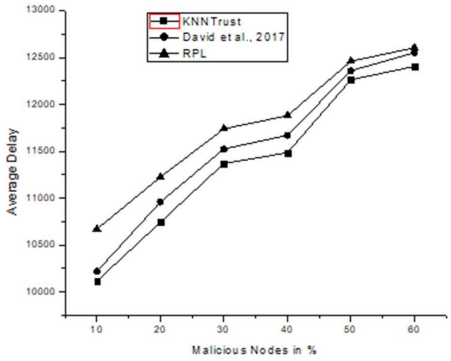

Figure 7. Average Delay

Packet delivery ratio: This metric has high impact in analyzing the performance of the network. It is classified as the entire of both data and control packets progressed by the source node and both control packet and also data packets are received by the destination node. Packet delivery ratio of single node as well as the entire network will be analyzed with the help of this network. This metric can be analyzed with varying number of malevolent nodes therefore the malevolent nodes can be upgraded ranging from 0 to 60 percentage. The Figure. 6 depict the forwarding ratio of KNNTrust, RPL, and David et al., 2017. Results describe the KNNTrust model has a greater forwarding ratio than the other two protocols. The intention is, that the proposed model considers correctly forward ratio instead of packet delivery ratio for trust computation. The David et al., model considers a single trust metric(packet delivery ratio) to assess the credibility of the node, but the proposed method deliberates manifold trust metrics (FR, CI, H) to calculate the honesty of the node. So, this manifold trust metric, the proposed method can find and eliminate misbehaving nodes which perform the black hole and selective forwarding attacks. The malicious nodes have not selected for routing, only trusted nodes involved for routing the data packets, thus increasing the packet delivery ratio. RPL routing protocol does not have any detection mechanism of malicious nodes, so it consequences in a

less forwarding ratio.

Average delay: This metric depends on the schedule management of network operations that will be involved in the network environment. It denotes an average time taken by the source node to transfered a particular packet to the destination node. The presences of malicious nodes will increase the delay. The Figure 7 represents the average delay of separate protocols such as KNNTrust, RPL, and David et al., 2017. It can be analyzed with differing number of malicious nodes. The average delay of KNNTrust model is relatively low compare with other two models. The proposed model handles the KNN machine learning algorithm to detect node behavior. It is a fast and reliable algorithm for classification. It identifies the malicious nodes using a limited number of training samples and those nodes are removed in the network. Simply trusted IoBT nodes are selected for routing operation, therefore average delay also reduced in the proposed system. The RPL has no such detecting mechanism, due to the misbehaving nodes, the delay also increased in such protocols.

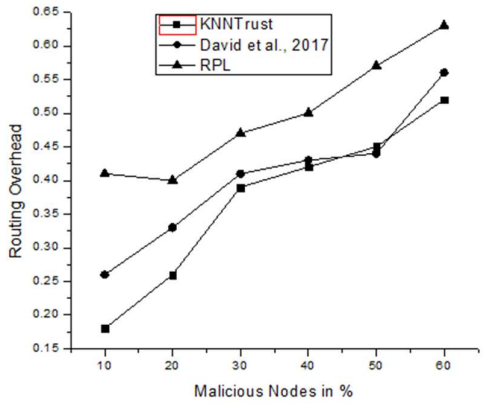

Figure 8. Routing Overhead

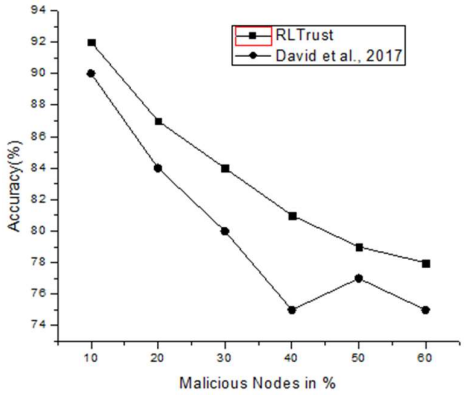

Figure 9. Accuracy

Routing overhead: It is a metric that create impact on routing. If the routing overhead is high, it affects the performance of the entire network operations. It is explained as the proportion in between the total route control packets and data packets. The Figure 8 illustrates the routing overhead of the proposed KNNTrust, RPL, David et al., 2017 with varying number of malicious nodes. The figure clearly shows that the routing overhead of KNNTrust model is low compare with other routing protocols. The black hole and selective forward attacks can degrade the functionality of the network. The selfish or malicious nodes drop the data packets; therefore, the routing overhead increases and makes the network unstable. KNNTrust model effectively identifies and avoids both black hole and selective forwarding attack nodes from the network. Therefore, routing overhead of the suggested KNNTrust model is low.

Scenario 3: This is the final performance evaluation metric that defines how the malicious nodes are being detected. The Figure .9 the detection accuracy of the proposed KNNTrust model and David et al., model.

The detection accuracy of both RPL and David et al., 2017 are low in the presence of malicious nodes. Also, the detection accuracy of the KNNTrust model is more than the differing two. As a result of the proposed method uses the new filtering algorithmic rule to avoid dishonest recommendation. Indirect trust metric is considered only from the honest recommendation and

direct trust is calculated using the trust metrics such as forwarding reliability, contact intimacy, and honesty, thus these trust values are highly reliable. Further KNN algorithm effectively predicts the node behavior thus increases the detection accuracy. David et al., 2017 model considers only forwarding behavior for trust computation thus the detection accuracy is low.

6. CONCLUSION

Future IoBT will be controlled by cyber warfare and artificial intelligence. Authentication is an essential security requirement in all applications to assure the right identity of the nodes, especially IoBT because it includes the soldier's life. Due to the restricted resources of IoBT devices, it is easily compromised by an attacker. The most common attacks that happened in the IoBT network is blackhole and selective forwarding attack. Traditional security requirements are not feasible, because it consumes more resources and requires fixed infrastructure for key management. In a distributed network like the IoBT environment, providing security using the trust mechanism will be suitable. The proposed KNNTrust model designed to detect and remove the malicious nodes in the battlefield network to provide good security and ensure authentication. To establish trust among IoBT nodes requires experience and opinion from neighbor nodes. This model uses the weighted-average method to compute direct trust. The new filtering algorithm was developed to filter the dishonest or unfair recommendation. Indirect trust is calculated only from an honest recommendation. Finally, the KNN algorithm used to guess the node performance using the computed direct trust and indirect trust. Every node has maintained the interacted nodes direct, indirect trust and their corresponding node' s behavior. These are the sample training data, based on this information evaluated node predicts the node's trust behavior. The primary merit of the KNN algorithm is it requires limited training data to predict the query data and it is a simple, fast, and effective classifier. The proposed KNNT trust model has embedded in the traditional RPL routing protocol and the performing of the KNNTrust is implemented and evaluating with the help of Cooja simulator. From the performance metrics, observed that the proposed KNNTrust is showing better results compare with other two models.

REFERENCES

[1] Aggarwal, R. and Lal Das, M. (2012) RFID Security in the Context of “Internet of Things”. First International Conference on Security of Internet of Things, Kerala, 17-19 August 2012, 51-56. http://dx.doi.org/10.1145/2490428.2490435.

[2] Glowacka, J., Krygier, J., &Amanowicz, M. (2015). A trust-based situation awareness system for military applications of the internet of things. 2015 IEEE 2nd World Forum on the Internet of Things (WF-IoT). doi:10.1109/wf-iot.2015.7389103.

[3] Prathapchandran Kannimuthu & Janani Thangamuthu. (2021). Decision Tree Trust (DTTrust)-Based Authentication Mechanism to Secure RPL Routing Protocol on Internet of Battlefield Thing (IoBT). Int. J. Bus. Data Commun. Netw. 17(1), 1-23.

[4] Prathapchandran, K & Janani, T. (2021). A Trust-Based Security Model to Detect Misbehaving Nodes in Internet of Things (IoT) Environment using Logistic Regression. Journal of Physics: Conference Series, 1850.

[5] Abuzainab, N., & Saad, W. (2018). Dynamic Connectivity Game for Adversarial Internet of Battlefield Things Systems. IEEE Internet of Things Journal, 5(1), 378–

390. doi:10.1109/jiot.2017.2786546.
[6] Patel, H. B., &Jinwala, D. C. (2019). Blackhole Detection in 6LoWPAN Based Internet of Things: An Anomaly Based Approach. TENCON 2019 - 2019 IEEE Region 10 Conference (TENCON). doi:10.1109/tencon.2019.8929491.
[7] Kandhoul, N., Dhurandher, S. K., &Woungang, I. (2019). T_CAFE: A Trust based Security approach for Opportunistic IoT. IET Communications. doi:10.1049/iet-com.2019.0657.
[8] Airehrour D, Gutierrez JA, Ray SK (2017) A trust-aware RPL routing protocol to detect black hole and selective forwarding attacks. J Telecommun Digital Econ 5(1):50–69. https://doi.org/10.18080/ jtde.v5n1.88.
[9] Conti M, Kaliyar P, Rabbani MM, Ranise S (2018) SPLIT: a secure and scalable RPL routing protocol for Internet of Things. In: 2018 14th International Conference on Wireless and Mobile Computing, Networking, and Communications (WiMob). IEEE, pp 1–8.
[10] A. Khan and P. Herrmann, "A trust based distributed intrusion detection mechanism for internet of things," in Advanced Information Networking and Applications (AINA), 2017 IEEE 31st International Conference on. IEEE, 2017, pp. 1169–1176.
[11] Mehta, R., & Parmar, M. M. (2018). Trust based mechanism for Securing IoT Routing Protocol RPL against Wormhole &Grayhole Attacks. 2018 3rd International Conference for Convergence in Technology (I2CT). doi:10.1109/i2ct.2018.8529426
[12] Lim, J., Ko, Y.-B., Kim, D., & Kim, D. (2018). A Stepwise Approach for Energy Efficient Trust Evaluation in Military IoT Networks. 2018 International Conference on Information and Communication Technology Convergence (ICTC). doi:10.1109/ictc.2018.8539353.
[13]T.Winter, "RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks",https://tools.ietf.org/html/rfc6550, 2012.
[14]Le, A., Loo, J., Luo, Y., &Lasebae, A. (2011). Specification-based IDS for securing RPL from topology attacks. 2011 IFIP Wireless Days (WD). doi:10.1109/wd.2011.6098218.
[15] Mathur, A., Newe, T., & Rao, M. (2016). Defence against Black Hole and Selective Forwarding Attacks for Medical WSNs in the IoT. Sensors, 16(1), 118. doi:10.3390/s16010118
[16]Hatzivasilis G, Papaefstathiou I, Manifavas C (2017) SCOTRES: secure routing for IoT and CPS. IEEE Intern Things J 4(6):2129–2141
[17]Mabodi, K., Yusefi, M., Zandiyan, S., Irankhah, L., &Fotohi, R. (2020). Multi-level trust-based intelligence schema for securing of internet of things (IoT) against security threats using cryptographic authentication. The Journal of Supercomputing. doi:10.1007/s11227-019-03137-5
[18] A. Dvir, T. Holczer, and L. Buttyan. Vera - version number and rank authentication in rpl. In 2011 IEEE Eighth International Conference on Mobile Ad-Hoc and Sensor Systems.
[19]Ao Li, Lirong Wang, Yunzhou Shi, Minghui Wang, Zhaohui Jiang, &Huanqing Feng. (2005). *Phosphorylation Site Prediction with A Modified k-Nearest Neighbor Algorithm and BLOSUM62 Matrix. 2005 IEEE Engineering in Medicine and Biology 27th Annual Conference.* doi:10.1109/iembs.2005.1615878.
[20]Hu, L.-Y., Huang, M.-W., Ke, S.-W., & Tsai, C.-F. (2016). The distance function effect on k-nearest neighbor classification for medical datasets. SpringerPlus, 5(1). doi:10.1186/s40064-016-2941-7.
[21]Guo, G., Wang, H., Bell, D., Bi, Y., & Greer, K. (2003). KNN Model-Based Approach in Classification. Lecture Notes in Computer Science, 986–996. doi:10.1007/978-3-540-39964-

3_62.
[22]Saini, I., Singh, D., & Khosla, A. (2013). *QRS detection using K-Nearest Neighbor algorithm (KNN) and evaluation on standard ECG databases. Journal of Advanced Research, 4(4), 331–344.* doi:10.1016/j.jare.2012.05.007.
[23] Denko, M. K., Sun, T., &Woungang, I. (2011). Trust management in ubiquitous computing: A bayesian approach. Computer Communications, 34(3), 398–406.
[24] K. Prathapchandran and T. Janani,A trust aware security mechanism to detect sinkhole attack in RPL-based IoT environment using random forest – RFTRUST,Computer Networks, Volume 198,2021,108413,ISSN 1389-1286,
[25] A.Pongle, P., & Chavan, G. (2015). *A survey: Attacks on RPL and 6LoWPAN in IoT. 2015 International Conference on Pervasive Computing (ICPC).* DOI:10.1109/pervasive .2015.7087034.
[26]Babu, S. S., Raha, A., &Naskar, M. K. (2011). *Geometric mean based trust management system for WSNs (GMTMS). 2011 World Congress on Information and Communication Technologies.* doi:10.1109/wict.2011.6141286.
[27] Jiang, J., Han, G., Wang, F., Shu, L., &Guizani, M. (2015). *An Efficient Distributed Trust Model for Wireless Sensor Networks. IEEE Transactions on Parallel and Distributed Systems, 26(5), 1228–1237.* doi:10.1109/tpds.2014.2320505
[28] J. H. Cho, A. Swami, and I. R. Chen, "A Survey on Trust Management for Mobile Ad Hoc Networks," IEEE Communications Surveys & Tutorials, vol. 13, no. 4, 2011, pp. 562-583.
[29] Guo, J., Chen, I.-R., & Tsai, J. J. P. (2017). A survey of trust computation models for service management in internet of things systems. Computer Communications, 97, 1–14. doi:10.1016/j.comcom.2016.10.012.
[30] Xia, H., Jia, Z., Li, X., Ju, L., & Sha, E. H.-M. (2013). Trust prediction and trust-based source routing in mobile ad hoc networks. Ad Hoc Networks, 11(7), 2096–2114. doi:10.1016/j.adhoc.2012.02.009.
[31] Wang, B., Chen, X., & Chang, W. (2014). A light-weight trust-based QoS routing algorithm for ad hoc networks. Pervasive and Mobile Computing, 13, 164–180. doi:10.1016/j.pmcj.2013.06.004
[32] Liang, W., Long, J., Weng, T.-H., Chen, X., Li, K.-C., &Zomaya, A. Y. (2018). TBRS: A trust based recommendation scheme for vehicular CPS network. Future Generation Computer Systems. doi:10.1016/j.future.2018.09.002
[33] Shabut, A. M., Kaiser, M. S., Dahal, K. P., & Chen, W. (2018). *A multidimensional trust evaluation model for MANETs. Journal of Network and Computer Applications.* doi:10.1016/j.jnca.2018.07.008