International Journal of Computer Networks and Applications (IJCNA)
DOI: 10.22247/ijcna/2023/218514 Volume 10, Issue 1, January – February (2023)

RESEARCH ARTICLE

Security Model to Mitigate Black Hole Attack on Internet of Battlefield Things (IoBT) Using Trust and K-Means Clustering Algorithm

P. Rutravigneshwaran
Department of Computer Applications, Karpagam Academy of Higher Education, Coimbatore, Tamil Nadu, India.
rutra20190@gmail.com

G. Anitha
Department of Computer Applications, Karpagam Academy of Higher Education, Coimbatore, Tamil Nadu, India.
florenceanitha7@gmail.com

Received: 15 December 2022 / Revised: 30 January 2023 / Accepted: 07 February 2023 / Published: 26 February 2023

Abstract – The Internet of Things (IoT) acts an imperative part in the Battlefield Network (BN) for group-based communication. The new technology is called Internet of Battlefield Things (IoBT) that delivers intelligence services on the battlefield to soldiers and commanders equipped with smart devices. Though it provides numerous benefits, it is also susceptible to many attacks, because of the open and remote deployment of Battlefield Things (BTs). It is more critical to provide security in such networks than in commercial IoT applications because they must contend with both IoT networks and tactical battlefield environments. Because of restricted resources, an attacker may compromise the BTs. The BT that has been seized by the adversary is called a malicious BT and it may launch several security attacks on the BN. To identify these malicious BTs, the IoBT network requires a reputation-based trust model. To address the black hole attack or malicious attack over Routing Protocol for Low Power and Lossy Networks (RPL) is a key objective of the proposed work. The proposed work is the combination of both machine learning algorithm and trust management and it is named as KmCtrust model. By removing malicious BTs from the network, only BTs participating in the mission are trusted, which improves mission performance in the IoBT network. The simulation analysis of KmCtrust model has witnessed the better results in terms of various performance metrics.

Index Terms – IoBT, RPL, Trust, Black Hole Attack, Multiple Regression, K-Means Clustering Algorithm, Security.

1. INTRODUCTION

A rapidly developing framework, the Internet of Things (IoT) connects conventional networked objects with physical objects such as automated vehicles, agricultural devices, smart healthcare and more. Typically, those physical objects are embedded with sensors and they interact with the outside environment. They will exchange the collected data with the help of internet [1]. Introducing the IoT concept to the BN can have a number of benefits that can improve mission effectiveness [2]. In recent days, defense associations have been influenced by the advantages of the IoT to enhance efficiency in battle and dramatically monitor battle resources. The combination of both IoT and combat is called the Internet of Battlefield Things (IoBT) [3]. By leveraging smart devices, the IoBT enhances the capabilities and capabilities of soldiers on a single battlefield. It manages and controls a huge number of unmanned vehicles in combat against the opposite team. Despite this, the defense department has not assured security against cyberattacks [4]. The armed forces at various places are required to update their status to the central authority. Military troops and battlefield vehicles carrying smart devices can be moved from one location to another. They are required to transmit a large volume of information between battlefield devices and central authorities. When information has been transferred from one place to another, the adversary may modify the information and send incorrect information to the controller. It is challenging to ensure security in such networks. The adversary may perform various malicious actions, including both internal and external attacks. They transmit false information and devastate the performance of the whole network [5]. The BN allows coordination and organizes the capacity of the combat forces to enhance the efficiency of the mission on the battlefield. This network improves data sharing in both real-time (i.e., context awareness) and normal data traffic (i.e., file transmission). IoBT applications generally use a client-server architecture with bidirectional data transmission. Typically, it is exchanged between mobile devices (i.e., tanks, warships, armed vehicles, etc.) and those equipped with various sensors such as wearable sensors, active sensors, microelectronic mechanical systems, Nano sensors, infrared sensors, and

RESEARCH ARTICLE

camera sensors, as well as central stations (i.e., fixed stations). The architecture diagram in shown in the figure 1.

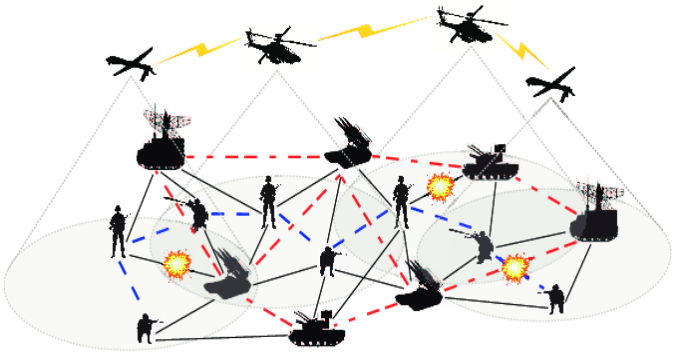

Figure1 The General Architecture Diagram of IoBT Environment [5]

Wearable sensors are the basis for the proposed model, and their properties are used in its implementation. For the application of IoBT in the battlefield network, many transmission technologies are used. A BN can be damaged by a variety of physical characteristics including the energy of the transmitted thing, the deployment locations, and the adaptability of message among different types of BTs [6], Jamming, attacks on BTs, and mobile node failures because of energy deprivation attacks or low energy, etc. Besides, another barrier to the BN is vulnerability to cyberattacks [6].

In order to analyze and make independent decisions on the BN, it is imperative to have real-time information provided by sensors attached to armed forces, vehicles, tanks, etc. The adversary aims to interrupt network connectivity by attacking IoBT devices and taking control of those devices. Security services like authenticity, confidentiality, integrity, availability, authorization and non-reputation can provide security using various cryptographic techniques but it requires key management. Traditional cryptographic techniques are not applicable in the IoBT network, because of the restricted resources of the BTs and the dynamically changing battlefield environment. Hence, the open and mobile BN, and lightweight BTs need a trust-oriented security mechanism to assure security in the IoBT network [7]. The KmCTrust model provides trust-oriented solutions for the IoBT network to ensure security. Each IoBT mobile node will select its corresponding one-hop neighbor nodes based on calculated trust values. As part of the mission, trusted BTs are used to maximize the chance of mission success. By the way, the proposed model ensures security in the battlefield environment.

1.1. Problem Statement

The IoBT environment usually consists of constrained BTs in relationships of their batteries, memory, and processing capabilities. Besides, the unique characteristics such as open and shared environment, dynamic environment, deployment environment of BTs, heterogeneous nature of various BTs, and lack of security in BTs. This is because manufacturing companies concentrate on productivity, not on security. Because of the reasons mentioned above, IoBT environments will damage by various security threats. One of the most notable attacks affecting the IoBT environment is the black hole attack. To address this, many security mechanisms have been proposed. These mechanisms are effective but they are not suitable for resource-constrained IoBT environments since they involve complex computational capabilities. This type of computing consumes a lot of memory and drains batteries quickly. Hence, applying those mechanisms again will lead to security violations. Many researchers have suggested trust-based security-based security mechanisms as alternative solutions to this problem. Thus, novel security model is called KmCTrust is proposed in this work.

1.2. Contribution

A trust security mechanism called KmCTrust is proposed to address the blackhole attack in the IoBT environment. Several machine learning concepts such as multiple linear regression and K-means clustering have been incorporated into the model. Additionally, BT behavior is observed based on direct and indirect mechanisms. To ensure security in the IoBT environment, both machine learning features and trust management are combined with each other to identify and eliminate the black hole attack.

1.3. Organization

The proposed research work is organized in the following manner. This paper has been organized as follows: in section 2, the background details, such as multiple linear regression and K-means clustering algorithms are discussed; in section 3, the related works is discussed, the proposed work is discussed in section 4; Section 5 deals with the results and discussion; conclusion and future work is presented in section 6.

2. BACKGROUND

In this section, the backbone of the research work such as RPL, K-means clustering algorithm and multiple linear regression algorithm is presented.

2.1. RPL Overview

In the networking, the exchange of information among the various network enabled devices are carried out by routing. Typically, it is defined as identifying the route from source device to destination devices. This routing is executed by various routing protocols. Among the routing protocols, RPL is considered as a suitable routing protocol for resource constrained devices. It supports point to point, multipoint to point and point to multipoint transmission methods. The RPL

RESEARCH ARTICLE

is constructed based on the graph called Destination Oriented Directed Acyclic Graphs (DODAG) [8]. According to IEEE 802.15.4 [9] it is called as distance vector routing protocol and it is correlated to IPv6 [10]. The graph is constructed from root node. RPL consists of instances and those are having different graphs. Besides, it is also having Objective Function (OF). The job of OF is to find the efficient route [10][11]. It also consists of various control messages [9]. The DODAG graph is formed as follows: At first, DIO messages will be received by neighbour nodes advertised by the border root. After getting the DIO message, nodes include the source of the DODAG Information Object (DIO) message in their parent's list. They estimate its rank by considering the OF mentioned in the DIO control message.

The estimation of nodes' rank is related to their location in the graph which corresponds to root node. The child node ranks must larger than parent node's rank which assures the non-cyclic feature of the DODAG graph. Afterward, updated DIO messages have been broadcast to their neighbour nodes. As a result, the node chooses the preferred parent, which becomes the default gateway, and all information is transmitted via the preferred parent to the DODAG root. Finally, every participating node in the graph has a default upward path to the root node; this path includes all the preferred parents. The control messages in RPL consist of routing information that is periodically broadcast to maintain network consistency. With the help of the trickle timer algorithm, periodic updates have been posted. IoT has a dynamic environment and therefore periodic updates are always expected. Because of weak security, the RPL is susceptible to routing attacks. Implementation of updated security mechanisms is always in demand to ensure security in all aspects of IoT applications [12].

2.2. Multiple Linear Regressions (MLR)

MLR is a Machine Learning (ML) technique; it defines the relationship between the dependent variable and multiple independent variables.

The MLR has computed based on equation 1:

$$Y = \beta_0 + \beta_1 . X_1 + \beta_2 X_2 \ldots + \beta_n . X_n \qquad (1)$$

In Eq. (1), where Y - dependent variable

β_0 - Constant value (It used to decrease the impact of modeling error)

X1, X2,..., Xn - Independent variable

$\beta_1, \beta_2, \ldots, \beta_n$ - Regression Coefficient for each independent variable [13].

MLR is an extension of simple linear regression. The primary merits of this technique are a clear and accurate understanding of the interrelationship of every independent variable with the dependent variable [14]. To detect BT's behaviour and identify which trust metrics have a high influence on trust, threshold-based models are appropriate.

2.3. K-Means Clustering Algorithm

This algorithm requires less computational overhead and also easy tom implement [15]. Here, the data is classified into K clusters. The centroids of these clusters have been depicted in [16]. The identified K-means cluster is a set of points which are closest to a certain centroid and away from all other centroids. This algorithm has some variations. The most widely used algorithm is Lloyd's algorithm. In this algorithm, the k number of clusters has been selected as input from a group of data points [17]. The algorithm begins with forming K-cluster centers. The selection of these centers was based on some heuristic procedures [18]. The prototype point is called the centroid (center). According to the closest prototype point, data points from the data set have been assigned to each cluster. The average points consist of a newly developed set of prototype points. Each data point has been assigned to a cluster of its closest prototype points. A K-means clustering algorithm iterates the above-described two steps (prototype point re-computation and cluster allocation) until the condition for concurrence (for instance, staying consistent across two consecutive repetitions) is satisfied. This stage of the cluster is the culmination of clustering results. This algorithm has several merits that make it very familiar. Simplicity and ease of implementation are the most crucial factors. Because of its linear complexity, this algorithm works very fast [18].

One of the most popular clustering methods is called K-means. This is an unsupervised machine learning technique that categorizes input data sets into several classes based on their Euclidean distance. It is a repetitive algorithm and begins with initial prototype points [19]. The Euclidean distance is defined as follows: (2):

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

3. RELATED WORK

The related works those are mainly focusing on ensuring trust in Internet of Battle Field environment are discussed in this section. In [20], the authors ensuring the security by SVM, a machine learning algorithm. Here, the black hole attacks are addressed with the help of trust metrics. In [21], the authors proposed extendable security in IoT using symmetric Datagram Transport Layer Security (DTLS) keys. They present a framework for resource-constrained mobile devices. This system is implemented with the client, server, and trusted authority to calculate the key that is derivative from its key management system. In [22], the authors proposed a security mechanism using the RSA cryptography algorithm. It

RESEARCH ARTICLE

is a two-way authentication mechanism to ensure security in the IoT-based DTLS. It has developed for 6LoWPANs of the IoT. The DTLS handshake and X.509 certificates with RSA keys has used for authentication to ensure message integrity and confidentiality in the IoT system. It provides an optimal security solution for IoT.

In [23], the exponential smoothing method to find the blackhole attack is proposed. The black hole attack by dropping received packets from its sub-tree's nodes, which are supposed to forward. By this, the malicious nodes disconnect the sub-tree from the remaining of the network. The authors developed an algorithm using exponential smoothing to identify the topological separation because of the black hole attack. This approach used exponential smoothing to compute the next data packet's delivery time at the root node. With the help of this estimation, the algorithm detects the malicious nodes impelling black hole attacks in real-time.

In [24], a new verification process to overcome the vulnerabilities in IoT is proposed. This model implemented ECDH cryptography, which is the vital agreement method. This approach accomplishes various security metrics like mutual authentication, ambiguously, confidentiality, data packet forwarding security, and location privacy. It was also resistant to various security attacks.

In [25], a strainer-based mechanism to detect and eliminate black hole attacks in IoT is proposed. It is an anomaly-based approach. In this model, suspicious nodes advertise high routing metrics that increase the possibilities to choose best parent. The SIEWE model identifies the node that advertises a higher routing metric than other adjacent nodes and adds their identity as a suspected list then its neighbor node verifies these nodes during the network operation. Finally, the root node discards malicious nodes. This model analyzes only malicious nodes. In [26], the authors proposed a hybrid anomaly-based approach. This model detects two popular routing attacks namely selective forwarding and sink. The intrusion detection agent has placed on the BR in the network that uses the optimum-path forest algorithm. It is depends on the MapReduce framework to employ in the distributed network for clustering models to detect malicious nodes using a global detection approach. The root node in this model used the voting method to decide malicious behavior. This model has deployed in a smart city network scenario. It also detects a wormhole attack.

In [27], the authors present an intelligent trust to counter black hole attack in the IoT network. They implemented their model in the AODV. In [28], an anomaly detection method in IoT for selective forwarding attacks is proposed. This model dynamically executes the support vector machines when identifying the suspected behavior of the wireless sensor nodes. The deep learning method has invoked when suspected behavior has identified in Gateway. This model combines the ML technique with a statistical method to identify attacks. In [29], the authors proposed an anomalous activity identification using two-levels in the IoT network. In level 1, network traffic has categorized as normal or abnormal. If any abnormal activity has been found, then it is transferred to level two for additional classification to identify the class or subclass of the identified anomaly. In [30], a secure architecture for an RPL-based industrial IoT network with resource-constrained devices is proposed. It has two phases: In the first phase, genetic programming has used to select the best features among all possible sets of features and the picked features has arranged in a standardized way. It is arranged as an in-order traversal with features output and its threshold value for every attack. In the second phase, the test features has evaluated when it meets the threshold value, and then it will be considered an attack in the network scenario.

In [31], a trust-based secure routing protocol in IoT networks to mitigate Sybil and rank attacks is proposed. This model evaluates neighbour node's trustworthy behaviour based on their services. This trustworthiness shows the reliability and dependability of the directly connected neighbour nodes. It has computed as a time-based successful data packets transmission among the nodes and positive acknowledgment with consistent monitoring of connected nodes. They use a fuzzy threshold to broadcast the trusted nodes to the whole network by maintaining efficient communication between nodes and assure broadcasting only trusted information to the neighbour nodes. In [32], the authors proposed a reputation-based approach to provide security for opportunistic IoT where the trust evaluation has done for each node based on its behaviour in the network. Suspicious nodes are discovered and excluded 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 [33], a trust-based solution for IoT is proposed. They used fuzzy logic to identify trusted nodes and selected the trusted routing path for successful data packet transmission. In [34], the authors present a security model to mitigate worm and gray hole attacks. DT computed from the trust properties is called forwarding check and ranking check. Total trust has estimated with the aggregation of DT and IT. The final trust forms in decreasing order and inserted into the RPL together with Rank and ETX. The data packets have forwarded via the trusted nodes by selecting high trust values nodes. Thus, suspicious nodes will be quarantined from the network. In [35], the authors present an energy-efficient trust computation model in a military IoT environment using stepwise tree-structured routing. In this model, only parent nodes do the trust computation process when they suspect the malicious behaviour of the child nodes. In [36], a security model which is based on combination of Machine Learning

RESEARCH ARTICLE

based Instruction detection system and Block chain Technologies is proposed. The main objective of the model is to address various internal attacks in IoT environment.

3.1. Drawbacks in the Existing Solutions

According to the review of the literature, most techniques and methods are based on cryptography algorithms and anomaly-based approaches. These techniques are effective for security attacks, however, applying these techniques in resource-constrained IoBT leads to security vulnerabilities. Furthermore, the internal attacker of the benevolent node could change its behavior at any time and turn it into a malicious node. Trust-based models can only identify these kinds of internal attacks. There has been notable progress in the field of trust management; however, they need to enhance the trust metrics for the IoBT network. The KmCTrust varies from the related research described above. It uses machine learning algorithms for trust computation. It detects malicious BTs accurately and removes them from the BN to ensure security. The trusted IoBT nodes only involve the battlefield to improve the mission's effectiveness.

4. K-MEANS CLUSTERING TRUST MODEL (KMCTRUST MODEL) – THE PROPOSED WORK

The KmCTrust uses multiple linear regressions and a K-means clustering algorithm to build the trust model. Nodes in 6LoWPAN have not authenticated before joining the network. Thus, malicious nodes can easily enter the network [35]. A malicious IoBT node may drop information in a highly distributed BN to disrupt its operation. The KmCTrust model aims to identify and discard malicious IoBT. Choosing the trust metrics is crucial to measuring the BT's trustworthiness based on past interactions. BT uses trust metrics to determine future behavior. The KmCTrust was primarily developed to mitigate blackhole attack.

4.1. Assumptions – Network Model

The assumptions are,

- The example network is an IoBT environment based on RPL. Sensors are attached to BTs, allowing them to communicate and collaborate with one another.
- It consists of many groups and assumes at least one BT is a non-constrained device. This root is a believe node and will not be seized by the adversary. All. All other BTs are resource-constrained devices that can be compromised by an attacker.
- The BTs can communicate only within the group.
- At any time, BT may enter or leave the group.
- There are various attacks that malicious BTs can perform. The BT that performs the black hole attack is called a malicious BT.
- Initially, all the BTs are healthy as far as energy and memory are concerned. A change in energy level may occur over time due to the involvement of network activities.
- The direct trust values, including the Packet Forwarding Ratio, Average Delay, Honesty and Closeness, will be calculated based on the satisfaction level of the network. Throughout the simulation, the level of satisfaction will be measured at regular intervals. Those values are calculated at 2.4 GHz frequency rate.
- Initially all the mobile nodes behave well. However, over time, they may behave as malicious nodes, such as black hole nodes.

4.2. Adversary Model

In the battlefield environment, mission-critical information has to be transferred from one place to another through an intermediate node. Malicious intermediate nodes may intentionally drop data packets. As a result, the destination IoBT node cannot receive the information that may lead to mission failure and risk to army forces.

4.2.1. Black Hole Attacks

The nature of this attack is to drop all the incoming packets that are intended to forward to others [35].

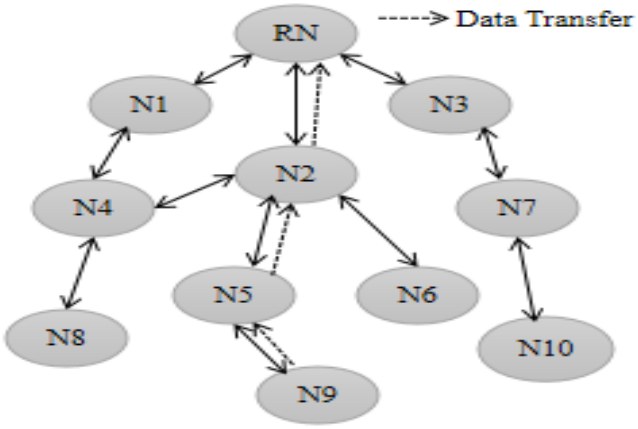

Figure 2 The RPL Network Without Any Attack

Figure 2 shows a sample network without any attacks. All nodes on the network are trusted and authenticated. For example, Node N9 transfers information to the BR through the intermediate Nodes N5 and N2. All nodes are trusted, so all the data packets will reach the BR without any data drop.

Figure 3 shows a work under attack by a black hole. The Node N2 launches the data drop attack. For example, Node N9 transfers information to the BR via intermediate Nodes N5 and N2. However, it will not reach the root node because malicious intermediate Node N2 drops the data packets.

RESEARCH ARTICLE

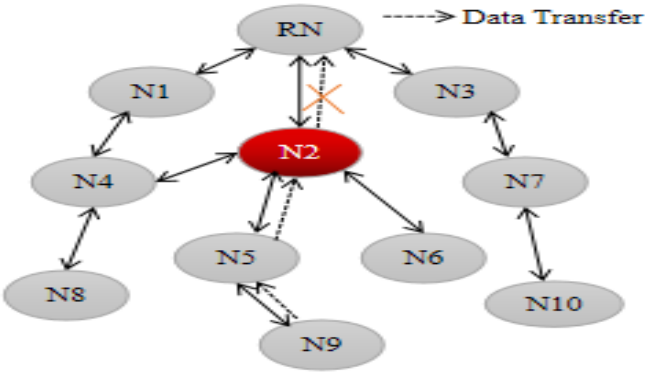

Figure 3 Example Network with a Black Hole Attack

4.3. Trust Management

Trust is a subjective possibility level that is shared by the two sensor nodes in the network. Direct experience or recommendations from other trusted nodes can be used to compute it. Generally, trust is computed by the degree of trust and it is explained by the trust relation [37]. Implementing and managing trust in IoT is essential for ensuring security and providing trustworthy communication among IoT devices [38]. The trust-oriented security model improves the security level in the IoT. In addition to that, the reputation-based trust model supports service management and enhances object cooperativeness in the IoT network [39]. Direct and indirect trust evaluations are involved in KmCTrust calculation. The Quality of Trust [40] metrics such as average delay, packet delivery ratio, packet dropping ratio and bandwidth are used to evaluate trust. Then, social trust metric is also used here. It consists of honesty, closeness and selfishness and etc [41].

4.3.1. Direct Trust Computation

The computation of DT depends on the trust evidence observed from the last interaction with the other node [42]. In DT computation, the node evaluates its neighbour node's trustworthiness using its direct experience. The subjective probability has been represented as the trust value [43]. As transferred data packets are dropped by malicious nodes, trust value of these nodes are relatively less compare with normal nodes. To aggregate the different trust values, multiple logistic regression is used. Several metrics are involved in trust calculation such as closeness, honesty, delay and forwarding ratio. Based on these metrics trust values can be calculated by the way black hole attacks will be detected.

For example, IoBT Node *'i'* computes the DT value of IoBT Node *'j'*. The DT value is computed using Equation (3).

$$DT(t) = \beta_0 + \beta_1.PCFR(t) + \beta_2.AD_{ij}(t) + \beta_3.C_{IJ}(t) + \beta_4.H_{ij}(t) \quad (3)$$

In Eq. (3), where, $DT_{ij}(t)$ - Direct trust (Dependent variable)

$PCFR_{ij}(t)$, $AD_{ij}(t)$, $C_{ij}(t)$, $H_{ij}(t)$ – Independent Variable (Trust Metrics)

B's - unknown regression coefficients

β_0 - constant

$DT_{i,j}(t)$ - Node *'i'* compute the DT for Node *'j'* from its direct experience.

The trust metrics used in the KmCTrust are explained as follows:

4.3.1.1. Packet Correctly Forwarding Ratio (PCFR)

It is the initial level of assessment and it is assessed by percentage of number of packets forwarded correctly and total packets received over the period of time. The word correctly forwarded refers to the transfer of data without any manipulation. For instance, a malicious node is located between the origin and target nodes. The origin node transfers data packets through malicious intermediate nodes to the target node. In this case, the malicious node may alter the data packets and send them to its malicious neighbour. Then it will not be considered as correctly forwarding behaviour and it directly affects the correctly forwarding ratio trust metric. This metric must be considered in order to ensure reliability. The PCFR is calculated as Equation (4):

$$PCFR_{ij}(t) = PCF_{i,j(t)}/TPR_{i,j}(t) \quad (4)$$

In the above equation, $PCF_{i,j}(t)$ represents no.of data packets forwarded correctly by the i^{th} node to j^{th} node at t time.

$TPR_{i,j}(t)$ represents total number of packets sent

$PCF_{i,j}(t)$ represents total number of packets forwarded [44].

4.3.1.2. Average Delay (AD)

AD denotes all possible delays caused by route detection, dissemination, re-transmission, and relaying. It has been computed using Equation (5):

$$AD_{i,j}(t) = \frac{(\sum_{k=1}^{n} PRT_k - PST_k)}{TNP} \quad (5)$$

In the above equation,

PRT_k denotes Packet Receive Time. It is defined as the time to attain the initial information of the '*k'* packet to the destination node *'j'*.

PST_k denotes Packet Sent Time. It is defined as the time to starting information of the *'k'* packet has sent by the origin node *'i'*. TNP denotes total amount packets forwarded [45].

4.3.1.3. Honesty (H)

It is an influential social trust metric that determines the level of trustworthiness. It helps to discover the adversary by examining the anomalous behaviour of the BT. Honesty is

RESEARCH ARTICLE

computed with the help of the number of successful and failed interactions. It can be computed using equation (6).

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

In the above equation, where, $\alpha_{i,j}(t)$ - successful interaction count

$\beta_{i,j}(t)$ - Failure interaction count

$\alpha_{i,j}(t)+\beta_{ij}(t)$ - sum of successful and failure interaction

i - Trustor

j - Trustee [46].

4.3.1.4. Closeness (C)

It is another one of the social metrics. It is calculated intimacy that is interaction counts between two nodes. if the node has high interaction counts, the closeness is high. The probability of the forwarding ratio from the node with the highest closeness is higher. Closeness is defined as;

$$C_{i,j}(t) = CF_{i,j}(t)/TCF_i(t) \quad (7)$$

In Eq. (7), where, $CF_{i,j}(t)$ - Contact frequency between Node *'i'* and Node *'j'*.

$TCF_i(t)$ – Contact frequency in summation evaluated by node 'i'. [47].

4.3.2. Indirect Trust Computation

IT calculations gather additional information to determine the trustworthiness of a node. It requests and receives recommendations from its peer nodes [48]. It is helpful to receive recommendations from nearby nodes to reduce the possibility of bias in direct experience. A malicious node may pretend to be a trusted node for some mobile nodes but may perform suspicious activities on some other mobile nodes. In IT calculation, every BT collects various recommendations from its nearby BTs for a given BT. In this model, when a BT has no previous direct experience with a certain BT, then the node uses only IT to select the node for routing operation. IT has computed equation (8).

$$IT_{x,y} = (\sum_{i=1}^{n}(DT_{x,mi} * DT_{mi,y}))/n \quad (8)$$

In Eq. (8), where, $DT_{x, mi}$ =: DT value of neighbour nodes 'mi' computed by Node *'x'*, who provides the recommendation trust for Node *'y'*.

$DT_{mi,y}$=: DT value of Node *'y'* computed by its *'mi'* neighbouring nodes.

n - Number of nodes provided the recommendation for Node *'y'*.

$IT_{x,y}(t)$ - Node *'x'* estimates the IT for Node *'y'* using recommendations.

Table 1 Indirect Trust Threshold Value

S. No	Threshold value	Meaning
1	If IT >= Th	T
2	If IT <Th	M

In table 1, where Th=Threshold value, T=Trusted, and M=Malicious. As shown in Table 1, the node's IT is above or equal to the threshold value then the BT is trusted otherwise the BT is malicious. Trusted BT will participate in the network operation, malicious BT's details are included in the blacklist, and it will be avoided by all BTs in the network.

4.3.3. Identifying Malicious IoBT Nodes Using K Means Clustering Algorithm

Each IoBT node in the BN maintains the previously communicated IoBT node's DT, IT, and its behaviour. The set of DT, IT, and node behaviour are training sets for the K-means clustering algorithm. Each tuple in the training data set contains of the DT and IT of a particular node and its previous behaviour. In the initial stage of node deployment, every BT learns the behaviour of neighbouring BT based on direct experience. The node uses both DT and IT for node selection. In this case, Node 'i' has the DT and IT of Node 'j'. When the DT and IT value of Node 'j' exceeds the pre-defined threshold, Node 'i' chooses the node 'j' for routing. Then the Node 'i' stores the trust behaviour of the Node 'j' for predicting the other node's behaviour.

The evaluated node can predict the evaluated node's behaviour using the K-means clustering algorithm.

Step 1: Select the K clusters (C1, C2, …., Ck) with null BTs.

Step 2: Prototype point (centroid) has randomly selected for every cluster.

Step 3: Repeat

Step 4: Select the BT_i (DT, IT, NB) from the training data set. Where $BT_i = \{BT_1, BT_2 \ldots BTn\}$.

Step 5: Compute the Euclidean distance between selected BT_i and all centroid.

Step 6: Assign BT_i to the closest centroid.

Step 7: Until all the BTs will assign to the cluster.

Step 8: Compute new centroids for every newly formed cluster.

Step 9: Until to satisfy any one of the criteria.

//Criteria1: Newly formed cluster's centroid remains the same.

//Criteria2: Newly formed cluster's BTs remain the same.

RESEARCH ARTICLE

//Criteria3: Certain number of iterations.

Algorithm 1 Training Phase (Clustering the BTs Based on their Behaviour Using K-Means Clustering Algorithm)

Algorithm 1 divides the BTs into two clusters: One cluster consists of malicious nodes (which is called a malicious cluster) and another cluster consists of a trusted node (which is called a trusted cluster).

Step 1: Evaluated BT computes DT and IT for evaluating BT. DT is derived from its direct experience and IT is derived from the recommendation that is received from the neighbour BT.

Step 2: The newly computed DT and IT has considered as a query point.

Step 3: Euclidean distance has computed between the query point and final centroid of each cluster. The final centroid has derived from Algorithm 1.

Step 4: Find the closest centroid.

Step 5: If the query point closest to the malicious cluster, then the BT is malicious; otherwise, the BT is trusted.

Algorithm 2 Predicting Phase (Predicting Node Behaviour)

The Euclidean distance between the two end points is computed in algorithm 2. One point is considered the centroid, and another point is the query point (DT and IT). In the actual environment, there is a point called BT (direct trust) and another point called the root node (indirect trust).

Malicious BTs cannot participate in a mission; they will avoid routing operations. As mentioned, the root node is controlled by the commander, who notifies other nodes about dangerous nodes. This makes other BTs aware of the malicious BT. Thus, malicious BTs are removed from the BN. Only trusted BTs are permitted to participate in the mission. To ensure security when operating on the battlefield. The design of the KmCTrust is shown in Figure 3. Initially, all the nodes construct the trust model using the K-means clustering algorithm from the sample data sets. Before communicating with the node, the sender node checks that they have had any previous interaction with the target BT. When yes, then the K-means clustering algorithm will be invoked to forecast BT's future behavior. Otherwise, it will consider it for node selection. The BT is stored on a blacklist and is excluded from network operation when it has been detected as malicious, and then the DODAG graph is updated.

4.3.4. Trust Value Update

The trust value update depends on the satisfaction level of neighbouring BTs. If BTs behave well with nearby BTs, then the satisfaction level will be high. For those BTs, the trust value will not be updated. Whenever neighbour BTs observe any behavior changes in any BT, the KmCTrust model will be invoked, and the trust value updates and with the help of this trust values, malicious nodes i.e., black hole nodes are disconnected from the network. Over time, those nodes will stop participating in network activities. Although those nodes have trust, they will disconnect based on the threshold values, which are listed in Table 1. Figure.4. illustrates the overall design of the KmCTrust.

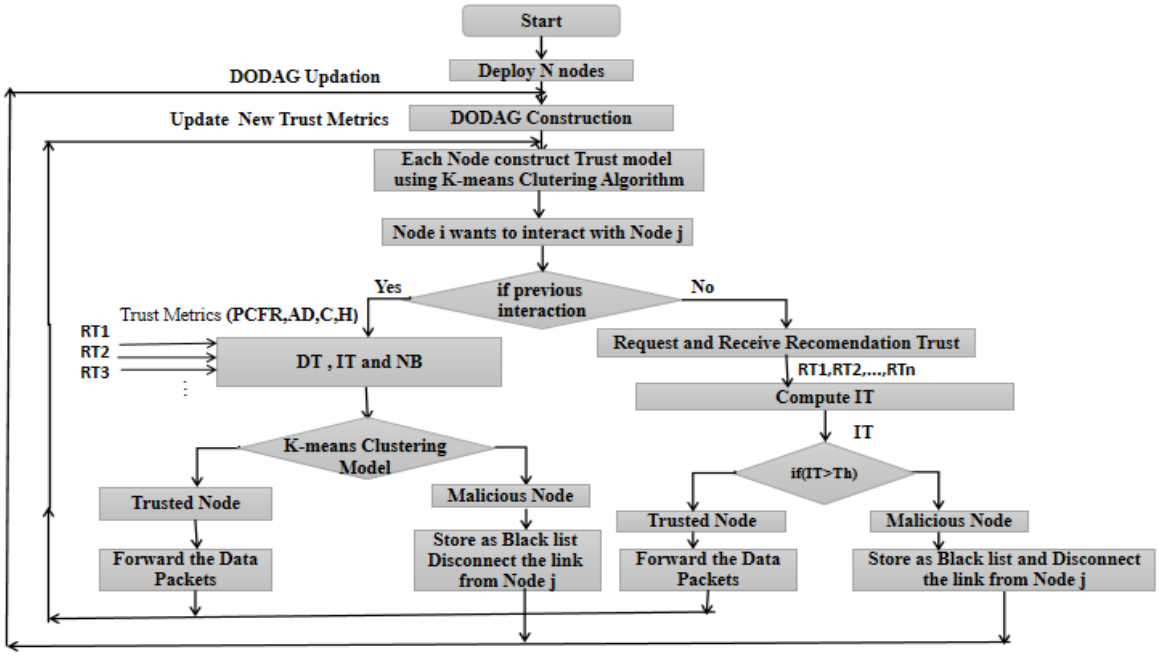

Figure 4 The Overall Design of the KmCTrust

RESEARCH ARTICLE

5. RESULTS AND DISCUSSION

The Contiki 2.7 OS and the network simulator called Cooja is used to implement the proposed model. The maximum number of mobile nodes involved in this simulation is 100. The coverage area is 300m x 300m. The nodes are deployed randomly. UDP is used for traffic. The communication distance of the sensors is 50 m. All nodes estimate the rank based on Min-Hop-Rank-Increase (256). As per the Cooja simulator, the proposed model incorporates wearable sensors. Those sensors are embedded in mobile nodes. The complete simulation parameters are shown in the following table 2.

Table 2 The Simulation Parameters

System Parameters	Values
Number of Nodes	100
Mote Type	TMote Sky
Simulation Time	3600Sec
Network Coverage Area	300mx300m
Data Rate	3072bps
Data Packet Size	64 byte
Traffic	UDP
Mac Layer	IEEE 802.15.4
Communication Range	50m
RPL Parameter	MinHopRankIncrease=256
Routing Protocol	KmCtrust, RPLand Trust based RPL [49]

The KmCTrust model has been analyzed and compared with the RPL- and Trust-based RPL [49] in terms of data drop ratio, PDR, throughput, and detection accuracy.

5.1. Packet Drop Ratio

Figure 5 depicts the packet loss ratio of KmCTrust, RPL and Trust – based RPL. The KmCTrust protocol's packet drop ratio is less than the other two protocols. In RPL, the packet drop ratio increases from 0.25 to 0.62 when the percentage of suspicious nodes is raised from 5% to 25%. Because it has no security mechanism against a black hole attack. The RPL protocol executes with malicious nodes and thus increases the data drop in the network. The KmCTrust model uses the K-means clustering ML algorithm to predict node behavior. Consequently, it identifies malicious nodes at least one step before Trust-based RPL [48] and ensures trustworthy communication between the source and target nodes. The proposed model decreases the data drop ratio and outperforms the other two protocols.

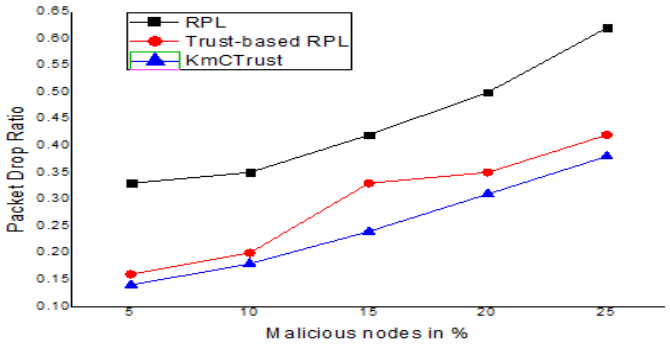

Figure 5 Packet Drop Ratio vs. Suspicious Nodes in Percentage

5.2. Packet Delivery Ratio

Figure 6 depicts the packet delivery ratio of KmCTrust, RPL and trust-based RPL [48] against the malicious nodes. When the network has no malicious nodes, all the protocols give around 97% of the delivery ratio. However, an increased percentage of malicious nodes affects the delivery ratio. However, the proposed KmCTrust model's PDR is higher than other protocols. The trust-based RPL [48] considers only single trust metrics to discover suspicious nodes, but KmCTrust considers multiple trust metrics to examine the node's trustworthiness. Generally, the RPL does not have any mitigation technique to identify suspicious nodes; the existence of malicious nodes decreases the delivery ratio. KmCTrust gives 80% PDR with 25% suspicious nodes.

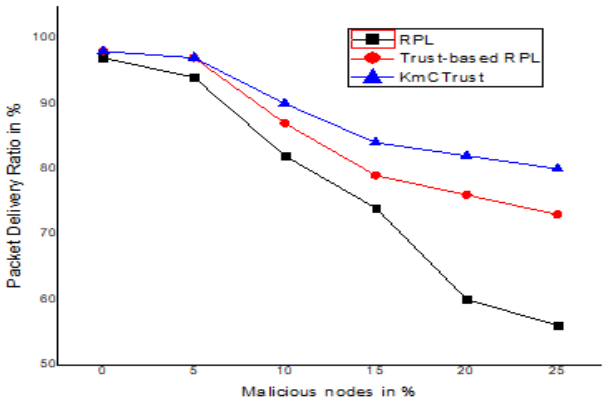

Figure 6 PDR vs. Suspicious Nodes in Percentage

5.3. Throughput

Figure 7 shows the proposed KmCTrust model throughput is around 3700bps with 25% of malicious nodes. While the RPL and Trust-based RPL [48] throughput rates are around 2100 and 3300 respectively. In the absence of suspicious nodes, the throughput of all protocols is almost the same. However, an

RESEARCH ARTICLE

increased number of suspicious nodes decreases network throughput.

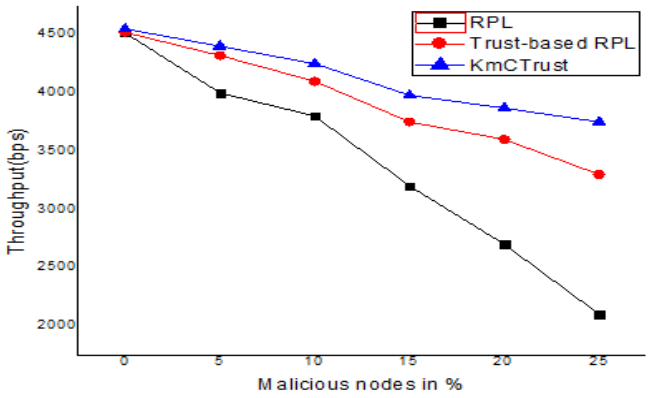

Figure 7 Throughput vs. Suspicious Nodes in Percentage

Suspicious nodes degrade network performance and reduce throughput. The KmCTrust uses multiple linear regressions to compute the direct trust and K-means clustering to discover suspicious nodes, while the existing model [48] uses fuzzy logic to identify the malicious node. The machine-learning algorithm predicts node behavior more accurately and faster than others. Thus, the KmCTrust model has the highest throughput compared to Trust-based RPL [48].

5.4. Detection Accuracy

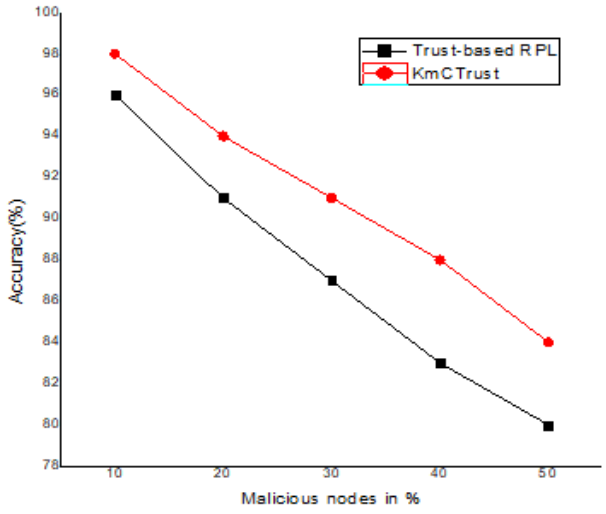

Figure 8 Detection Accuracy vs. Malicious Nodes in Percentage

In Figure 8, detection accuracy of trust-based RPL [48] and the proposed model has depicted. As RPL protocol does not have the ability to detect security attacks in its design itself, it is not considered in this scenario. When the malicious nodes increase, the detection accuracy decrease. The proposed is getting 84% accuracy in the presence of 50% of malicious nodes. Whereas the trust-based model [49] is only getting 80% of accuracy. As the proposed model use machine learning algorithm to effectively detect the malicious nodes hence this algorithm increases the detection accuracy. Whereas in trust-based model [49], as there is no such kind of algorithm, the detection accuracy rate is low compare with the proposed model.

5.5. Energy Consumption

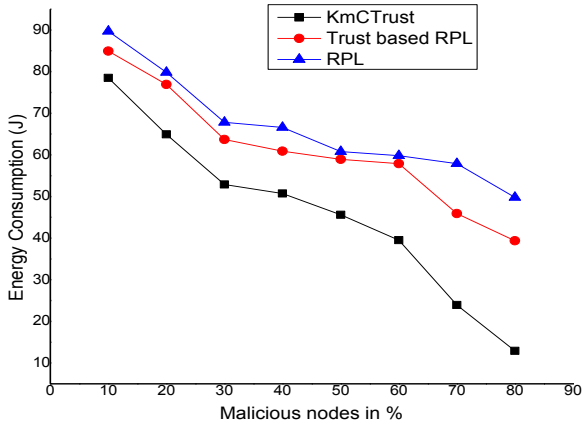

Figure 9 Energy Consumption vs. Suspicious Nodes in Percentage

In Figure 9, the energy consumption of PRL, KmCTrust and Trust-based RPL [48] are discussed. Since the IoBT environment is resource constrained when it comes to batteries, energy consumption is need to be analysed. The figure has shown clearly, the KmCtrust model consumes less energy. The multiple trust metrics involved in the proposed model hence energy consumption is less as suspicious nodes are identified and deleted from the network. Moreover, machine learning algorithm plays a major role in identifying the malicious nodes. all these mechanisms together leads less energy consumption in the proposed KmCTrust model. As no security mechanism in RPL, increasing energy consumption when number of malicious nodes increases. In trust-based RPL [49], weakest measurement in trust evaluation leads to increase energy consumption when no of malicious node increases. Finally, RPL has high energy consumption compare with other two models. Trust-based RPL has high energy consumption compare with proposed model and less than traditional RPL routing protocol.

6. CONCLUSION AND FUTURE WORK

Implementing the IoT concept in the battlefield environment brings various benefits to achieving a mission effectively;

RESEARCH ARTICLE

however, it introduces a distinct set of challenges. One of the most significant challenges is addressing security problems in the battlefield network. Providing security against various attacks on a battlefield network is a crucial task. Ensuring secure, reliable communication and avoiding adversaries from interrupting the mission is the primary concern in the BN. Thus, this paper provides a trust-oriented security model to withstand black hole attacks in the battlefield network. The KmCTrust model relies on trust to ensure trustworthy data transmission among battlefield things. It is implemented in the OF of the RPL, the performance of the network on the battlefield has improved. The DT has been computed using a multiple regression-supervised ML technique. Then, the K-means clustering algorithm uses the DT and IT to discover suspicious BTs in the battlefield network. A BT with suspicious behavior is removed from the battlefield network. Trusted BTs are involved in the routing process, improving mission effectiveness. The KmCTrust model has been implemented and analyzed using a COOJA network simulator. The experiment results captured the efficiency of the KmCTrust model with different numbers of suspicious nodes. In the future, KmCTrust will implement to identify various security attacks. Moreover, the KmCTrust model will be adapted for use in some other applications as well.

REFERENCES

[1] Burrell, D. N. (2021). Creating Diverse and Religiously Inclusive Workplace Cultures in Hyper-Connected, Technical, and cyber-Driven Organizations. International Journal of Sociotechnology and Knowledge Development, 13(3), 17–32. doi:10.4018/ IJSKD.2021070102

[2] 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. 198(10813), 1-20, 2021

[3] Farooq, M. J., & Zhu, Q. "Secure and Reconfigurable Network Design for Critical Information Dissemination in the Internet of Battlefield Things (IoBT)". 15th International Symposium on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks (WiOpt). doi:10.23919/wiopt.2017.7959892, 2017.

[4] Ferrara, P., Mandal, A. K., Cortesi, A., & Spoto, F. (2021). Static analysis for discovering IoT vulnerabilities. International Journal of Software Tools for Technology Transfer, 23(1), 71–88. doi:10.1007/s10009-020-00592-x

[5] Nobre, J., Rosario, D., Both, C., Cerqueira, E., & Gerla, M, "Toward Software-Defined Battlefield Networking". IEEE Communications Magazine, 54(10), 152–157. doi:10.1109/mcom.2016.7588285, 2016.

[6] K.Prathapchandran and T.Janani, "Decision Tree Trust (DTTrust)-Based Authentication Mechanism to Secure RPL Routing Protocol in Internet of Battlefield Thing (IoBT)", International Journal of Business Data Communications and Networking (IJBDCN), 1(17), pp.1-23, 2021.

[7] Pongle, P., & Chavan, G, "A Survey: Attacks on RPL and 6LoWPAN in IoT". International Conference on Pervasive Computing (ICPC). doi:10.1109/pervasive.2015.7087034, 2015.

[8] Kamble, A., Malemath, V. S., & Patil, D, "Security Attacks and Secure Routing Protocols in RPL-Based Internet of Things: Survey", International Conference on Emerging Trends & Innovation in ICT (ICEI). doi:10.1109/etiict.2017.7977006, 2017.

[9] Winter, T., "RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks", https://tools.ietf.org/html/rfc6550, 2012.

[10] Glissa G, Rachedi, A, & Meddeb, A, "A Secure Routing Protocol-Based on RPL for Internet of Things" . 2016 IEEE Global Communications Conference (GLOBECOM). doi:10.1109/glocom.2016.7841543,2016.

[11] Li, S., Iqbal, M., & Saxena, N. (2022). Future industry internet of things with zero-trust security. Information Systems Frontiers, 1-14.

[12] Koohang, A., Sargent, C. S., Nord, J. H., & Paliszkiewicz, J. (2022). Internet of Things (IoT): From awareness to continued use. International Journal of Information Management, 62, 102442.

[13] Marill, K. A, "Advanced Statistics: Linear Regression, Part II: Multiple Linear Regression. Academic Emergency Medicine" , 11(1), 94–102. doi: 10.1197/j.aem.2003.09.006, 2004.

[14] Ng, H. P., Ong, S. H., Foong, K. W. C., Goh, P. S., & Nowinski, W. L. (n.d.). "Medical Image Segmentation Using K-Means Clustering and Improved Watershed Algorithm", IEEE Southwest Symposium on Image Analysis and Interpretation. doi:10.1109/ssiai.2006.1633722, 2006.

[15] Shanmugam, S., V., M. G., K., P., & T., J. (2022). Mitigating Black Hole Attacks in Routing Protocols Using a Machine Learning-Based Trust Model. International Journal of Socio technology and Knowledge Development (IJSKD), 14(1), 1-23. http://doi.org/10.4018/IJSKD.310067

[16] Nidheesh, N., Abdul Nazeer, K. A., & Ameer, P. M. " An Enhanced Deterministic K-Means Clustering Algorithm for Cancer Subtype Prediction from Gene Expression Data" . Computers in Biology and Medicine, 91, 213–221. doi: 10.1016/j.compbiomed.2017.10.014, 2017.

[17] Cui, H., Ruan, G., Xue, J., Xie, R., Wang, L., & Feng, X, " A Collaborative Divide-and-Conquer K-means Clustering Algorithm for Processing Large Data", Proceedings of the 11th ACM Conference on Computing Frontiers - CF '14. doi:10.1145/2597917.2597918, 2014.

[18] Kavitha, A., Reddy, V. B., Singh, N., Gunjan, V. K., Lakshmanna, K., Khan, A. A., & Wechtaisong, C. (2022). Security in IoT Mesh Networks based on Trust Similarity. IEEE Access, 10, 121712-121724.

[19] S. Raza, L. Seitz, D. Sitenkov, G. Selander, "S3K: Scalable Security with Symmetric Keys − DTLS Key Establishment for the Internet of Things" , IEEE Trans. Autom. Sci. Eng. 13 (2016) 1270–1280, http://dx.doi.org/10.1109/TASE.2015.2511301, 2016.

[20] Rutravigneshwaran, P., Anitha, G. & Prathapchandran, K. "Trust-based support vector regressive (TSVR) security mechanism to identify malicious nodes in the Internet of Battlefield Things (IoBT)". Int J Syst Assur Eng Manag. https://doi.org/10.1007/s13198-022-01719-w, 2022

[21] Hassan, T., Asim, M., Baker, T., Hassan, J., & Tariq, N. (2021). CTrust-RPL: A control layer-based trust mechanism for supporting secure routing in routing protocol for low power and lossy networks-based Internet of Things applications. Transactions on Emerging Telecommunications Technologies, 32(3), e4224.

[22] Sahay, G. Geethakumari, B. Mitra and V. Thejas, "Exponential Smoothing-Based Approach for Detection of Blackhole Attacks in IoT," IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS), Indore, India, 2018, pp. 1-6, doi: 10.1109/ANTS.2018.8710073,2018.

[23] Alamr, A. A., Kausar, F., Kim, J., & Seo, C, "A Secure ECC-Based RFID Mutual Authentication Protocol for Internet of Things". The Journal of Supercomputing, 74(9), 4281–4294, 2018.

[24] Patel, H. B., & Jinwala, D. C, " Blackhole Detection in 6LoWPAN-Based Internet of Things: An Anomaly Based Approach". TENCON 2019 - 2019 IEEE Region 10 Conference (TENCON). doi:10.1109/tencon.2019.8929491,2019.

[25] Bostani, H., & Sheikhan, M, " Hybrid of Anomaly-Based and Specification Based IDS for Internet of Things Using Unsupervised OPF Based on MapReduce Approach". Computer Communications, 98, 52–71. doi:10.1016/j.comcom.2016.12.001, 2017.

[26] Seyedi, B., & Fotohi, R, "NIASHPT: A Novel Intelligent Agent-Based Strategy Using Hello Packet Table (HPT) Function for Trust Internet of Things". The Journal of Supercomputing. doi:10.1007/s11227-019-03143-7,2020.

[27] Yahyaoui, A., Abdellatif, T., & Attia, R, "Hierarchical Anomaly-Based Intrusion Detection and Localization in IoT" 15th International Wireless Communications & Mobile Computing Conference (IWCMC). doi:10.1109/iwcmc.2019.8766574, 2019.

RESEARCH ARTICLE

[28] Ullah, I., & Mahmoud, Q. H, "A Two-Level Flow-Based Anomalous Activity Detection System for IoT Networks". Electronics, 9(3), 530. doi:10.3390/electronics9030530, 2020.
[29] Qureshi, K. N., Rana, S. S., Ahmed, A., & Jeon, G, "A Novel and Secure Attacks Detection Framework for Smart Cities Industrial Internet of Things". Sustainable Cities and Society, 102343. doi: 10.1016/j.scs.2020.102343,2020.
[30] Airehrour D, Gutierrez JA, Ray SK , "SecTrust-RPL: a secure trust-aware RPL Routing protocol for Internet of Things" . Future Generation Computer System. https://doi.org/10.1016/j.future.2018.03.021., 2018
[31] Kandhoul, N., Dhurandher, S. K., & Woungang, I. T_CAFE: "A Trust based Security approach for Opportunistic IoT"., IET Communications. doi:10.1049/iet-com.2019.0657.2019.
[32] Airehrour D, Gutierrez JA, Ray SK , "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.v5n1.88,2017.
[33] Mehta, R., & Parmar, M. M, " 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, 2018.
[34] Lim, J., Ko, Y.-B., Kim, D., & Kim, D, " A Stepwise Approach for Energy Efficient Trust Evaluation in Military IoT Networks". International Conference on Information and Communication Technology Convergence (ICTC). doi:10.1109/ictc.2018.8539353, 2018.
[35] Kamble, A., Malemath, V. S., & Patil, D. "Security Attacks and Secure Routing Protocols in RPL-Based Internet of Things: Survey", International Conference on Emerging Trends & Innovation in ICT (ICEI). doi:10.1109/etiict.2017.7977006, 2017.
[36] Kaur, J., Singh, G., "A Blockchain-Based Machine Learning Intrusion Detection System for Internet of Things" . In: Daimi, K., Dionysiou, I., El Madhoun, N. (eds) Principles and Practice of Blockchains. Springer, Cham. https://doi.org/10.1007/978-3-031-10507-4_650,2023.
[37] Sun, Xi., Chang, G., & Li, F, "A Trust Management Model to Enhance Security of Cloud Computing Environments" , Second International Conference on Networking and Distributed Computing. doi:10.1109/icndc.2011.56. 2011.
[38] Alshehri, M. D., Hussain, F., Elkhodr, M., & Alsinglawi, B. S, "A Distributed Trust Management Model for the Internet of Things (DTM-IoT)" . EAI/Springer Innovations in Communication and Computing, 1–9. doi:10.1007/978-3-319-99966-1_1, 2019.
[39] Abdalla Ahmed, A. I., Ab Hamid, S. H., Gani, A., Suleman khan, & Khan, M. K, " Trust and Reputation for Internet of Things: Fundamentals, Taxonomy, and Open Research Challenges". Journal of Network and Computer Applications, 102409. doi:10.1016/j.jnca.2019.102409, 2019.
[40] 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, pp. 562-583. 2011.
[41] Guo, J., Chen, I.-R., & Tsai, J. J. P.," 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, 2017.
[42] Liqin, T., Chuang, L., & Tieguo, J. " Quantitative Analysis of Trust Evidence in Internet" , International Conference on Communication Technology. doi:10.1109/icct.2006.342023, 2006.
[43] Tripathy, B. K., Jena, S. K., Bera, P., & Das, " An Adaptive Secure and Efficient Routing Protocol for Mobile Ad Hoc Networks". Wireless Personal Communications. doi:10.1007/s11277-020-07423-x ,2020.
[44] Wang, B., Chen, X., & Chang, W. "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, 2014.
[45] Wang, Y., Tian, Y., Miao, R., & Chen, W, "Heterogeneous IoTs Routing Strategy Based on Cellular Address" . IEEE International Conference on Smart Internet of Things (SmartIoT). doi:10.1109/smartiot.2018.00021,2018.
[46] Shabut, A. M., Kaiser, M. S., Dahal, K. P., & Chen, W, " A Multidimensional Trust Evaluation Model for MANETs", Journal of Network and Computer Applications. doi:10.1016/j.jnca.2018.07.008, 2018.
[47] Liang, W., Long, J., Weng, T.-H., Chen, X., Li, K.-C., & Zomaya, A. Y. " TBRS: A trust based recommendation scheme for vehicular CPS network". Future Generation Computer Systems. doi:10.1016/j.future.2018.09.002, 2018.
[48] Iltaf, N., Ghafoor, A., & Zia, U. " A Mechanism for Detecting Dishonest Recommendation in Indirect Trust Computation" . EURASIP Journal on Wireless Communications and Networking, 2013(1). doi:10.1186/1687-1499-2013-189,2013.
[49] Airehrour, D., Gutierrez, J., & Ray, S. K, " Securing RPL Routing Protocol from Blackhole Attacks Using a Trust-Based Mechanism" , 26th International Telecommunication Networks and Applications Conference (ITNAC). doi:10.1109/atnac.2016.7878793, 2016.

Authors

P. Rutravigneshwaran received his Post Graduation from Bharathiar University, Coimbatore in 2013 and completed his M. Phil. Computer science in 2014. He is pursuing the Ph.D degree at karpagam Academy of higher education, Coimbatore. His research interests include Internet of Things, Network Security.

G. Anitha received her Post Graduation from Madurai Kamaraj University, Madurai in 2005 and M. Phil. from Bharathiar University in 2007. She also completed her PhD in Computer Science from Bharathiar University during 2018. She is presently working as Associate Professor in Department of Computer Applications at Karpagam Academy of higher education, Coimbatore. She has more than two decades of teaching and research experience. Her research interests on Computer Applications and Optimization Techniques, Intrusion Detection System, Internet of Things.

How to cite this article:

P. Rutravigneshwaran, G. Anitha, "Security Model to Mitigate Black Hole Attack on Internet of Battlefield Things (IoBT) Using Trust and K-Means Clustering Algorithm", International Journal of Computer Networks and Applications (IJCNA), 10(1), PP: 95-106, 2023, DOI: 10.22247/ijcna/2023/218514.