Received: August 6, 2023. Revised: September 16, 2023. 600

International Journal of
Intelligent Engineering & Systems

http://www.inass.org/

Conflicting Behaviour Attack Prediction using Machine Learning for Mobile Adhoc Network

Vijay Anand Krishnan[1]* **Abel Thangaraja Ganesan[2]**

[1]*Department of Computer Science, SNMV College of Arts and Science, Coimbatore, India*
[2]*Department of Computer Technology, Sri Krishna Adithya College of Arts and Science, Coimbatore, India*
* Corresponding author's Email: vijayanandphd123@gmail.com

Abstract: Mobile adhoc network (MANET) is a type of wireless configuration that features self-organizing wireless mobile nodes and adaptive network connection. Security is a key concern for MANETs due to their dynamic nature and continually changing topology. To improve security, an adaptive trust threshold-aware secure energy-efficient protocol was designed, which adaptively predicts the threshold value using an artificial neural network (ANN) to evaluate the node's trust for detecting and preventing the suspected nodes. In contrast, it fails to detect and mitigate conflicting behavior (CB) attacks, in which the suspected node may behave well towards a specific group of nodes and badly towards another group of nodes. Therefore, this article proposes a CB attack prediction using the shared learning-based ANN (CBAP-SLANN) algorithm to predict CB attacks in different nodes as well as different timeslots within the same node. The trust calculation should then take into account the consistency of behavior when employing different node-based observations along with the proposed different time-based observations. Initially, nodes are divided into overlapping clusters, and the trust and various network parameters of each node are observed for every group individually. Then, the ANN algorithm is trained in each group using the observed parameters and the trained model for each group is combined to get the global decision, which helps to predict the CB attack nodes in the network. At last, the simulation outcomes show that the CBAP-SLANN algorithm attains 93.1% accuracy when deploying 300 nodes compared to the trust-based routing algorithms.

Keywords: MANET, Trust management, Routing protocol, Adaptive trust threshold, ANN, CB attacks.

1. Introduction

MANET is a modern communication system that uses peer-to-peer data transfer and multi-hop paths. It can be used in various situations, such as target tracking and disaster response [1]. Nodes depend on each other for data transmission, requiring specific collaboration methods and routing algorithms [2]. Its key features include interoperability, node mobility, and cost limits. MANET's versatility exposes nodes to various threats, jeopardizing their reliability. To address this, reliable routing algorithms must be designed [3, 4].

Self-organized MANET's adaptability poses data breaches, as nodes lack prior understanding. Establishing trust between unknown nodes is crucial to ensure reputable access to services. MANET transmission relies on adhoc on-demand distance vector (AODV) [5-7] and dynamic source routing (DSR) [8, 9] protocols, ensuring trustworthiness and cooperation. However, these protocols increase vulnerability to routing failures caused by disruptive non-cooperative nodes. The application of trust-based routing algorithms appears to be a possible solution to this issue [10]. The potential of many elements for evaluating confidence opens up a wide range of study prospects. This motivates the scholars to contribute by creating and implementing a trust-based routing system in the AODV framework [11].

Trust is crucial in MANET for handling uncertainty and unpredictability, but trust analysis and regulation are complex due to computation cost requirements and individual node autonomy. In a MANET, unstable nodes can limit data throughput and pose risks [12-13]. Trust evaluation enhances

user interaction reliability and protects hostile nodes from the routing path in data transmission.

Trust-based communication systems, linked to misbehavior classification models, help locate offending nodes by computing and storing trustworthiness values about others [14-15]. These values are compared to a pre-defined threshold, indicating a node's maximum tolerable misconduct. An honest node successfully relays a certain fraction of data packets in compliance with 802.11 standards.

According to this fact, trust-based secure power-effective routing in MANETs has been established by considering the cat slap single-player algorithm (C-SSA) [16] to enhance confidentiality and power utilization. At first, the CHs were determined using the fuzzy clustering technique in association with each node's highest trust value. Next, depending on the preset threshold, suspected nodes were discovered and excluded from the routing path across the origin and target nodes. Further, the optimal paths were determined by the C-SSA method, which was based on the desired characteristics and several criteria such as path efficiency, bandwidth utilization, and communication. But a preset threshold may influence the network efficiency since all nodes pose distinct mobility and node degrees. Also, it tends to high false-positive rate for detecting the suspected nodes. When the threshold was kept at a very minimum, the loss value increased since suspected nodes were eliminated from the route immediately. When the threshold was kept at a very maximum, the loss value was less; yet, some nodes were permitted to engage in the data transfer since many nodes were seen as misconduct. Additionally, a sophisticated suspected node may modify its misconduct policy based on the constant threshold to evade the detection process. So, a proper threshold has to be selected depending on the network parameters.

To combat this problem, an adaptive threshold-aware secured energy-efficient protocol has been developed [17], which uses the different network parameters to dynamically decide the threshold for trust analysis. Initially, various network parameters including the rate of link changes, node degree, connectivity, node stability, mobility, residual power, pause time and mean neighborhood trustworthiness were determined for each node. After that, the values of all parameters were learned by the ANN to obtain the optimum threshold for predicting the node's proper trust value. By using these trust values, the suspected and typical nodes were identified accurately and timely. Nonetheless, this protocol fails to identify the suspected nodes, which creates CB attacks. In CB attacks, the suspected node may behave well towards a specific group of nodes and badly towards another group of nodes.

As a result, this paper proposes the SLANN model that improves the trust evaluation to be resistant to a CB attack in various nodes as well as different timeslots with the same node. The trust computation should include the consistency of behavior when using various node-based observations in addition to the suggested varied time-based observations. Initially, nodes are grouped into overlapping clusters and the trust of each node is assessed independently for each group. As well, the different network parameters are calculated for each node in each group at different periods. The ANN algorithm is then trained for each group using the obtained parameter and trust values. Further, the trained model for all groups is combined to obtain the global decision, which is used to predict the CB attack in the network at various periods. Thus, the CB of a malicious node in a network is predicted effectively by the trust modeling, without using the predetermined threshold values.

The rest of the portions are arranged as: Section 2 presents recent studies associated with the safe and reliable routing systems for MANETs. Section 3 discusses the CBAP-SLANN algorithm, while section 4 proves its effectiveness. Section 5 summarizes the study and recommends solutions to enhance it.

2. Literature survey

The trust-based secure multipath routing (TBSMR) protocol [18] was presented to boost MANET efficiency. However, the packet loss ratio (PLR) was high and the network throughput was less. An efficient trust-based routing scheme (ETRS) [19] was presented to avoid misbehaving nodes and establish secret data transfers in MANET. This ETRS was used to provide an explicit diagnosis to each intermediary node participating in the network transmission, to prevent the distribution of fake data prepared intentionally by suspected nodes, and to define a specific category of trusted path control scheme upon identification of the suspected node. However, the end-to-end delay was high and PDR was less.

A novel hybrid technique, namely the data-driven zone-based routing protocol (DD-ZRP) [20] was presented for resource-limited MANETs, which integrates abnormality identification methods. In this protocol, a dynamic threshold value was determined based on the different quality-of-service (QoS) parameters to choose the cluster head and identify the suspected node behavior. But the detection rate was low because of the predefined threshold value.

The base station controlled secure routing protocol (BSCSRP) [21] was developed to identify the anti-nodes from protected nodes based on the trust strategy, which prevents fake information insertion and offers a stable path. To increase security, data drop trust and quality trust were incorporated. But the average throughput and residual energy were not efficient.

An improved trust-based efficient energy-balanced routing (TER) algorithm [22] was developed to choose the forwarding nodes according to the residual energy, distance, occupied buffer space and the node speed. Conversely, the network throughput was affected when increasing the node densities.

A hybrid trust-based reputation mechanism (HTRM) [23] was developed to determine the node's trust value for a reputed optimal routing in MANET. However, the throughput and energy consumption were not satisfactory. A machine learning and trust-based AODV protocol [24] was presented to prevent flooding and blackhole attacks in MANET. The node with the highest trust value were selected as trusted relay forwarders. Also, the ANN and support vector machine (SVM) classifiers were applied to find the best routes. But the PLR was high while the node density was high.

A selfish node-aware trustable and optimized clustering-based routing (SN-TOCRP) [25] was developed to generate node clusters. The CH was chosen by the fuzzy-based crow search algorithm. Selfish node recognition was performed by using the authentication scheme. Also, bandwidth-aware trust-based routing protocol (BTRP) was used to detect and prevent misbehaving nodes from the network. But energy consumption was very high.

3. Proposed methodology

This part describes the CBAP-SLANN algorithm. In MANETs, secure energy-efficient routing ensures that information is securely forwarded between the origin node and the target nodes and avoids packet loss during transmission. The block diagram of the proposed study is shown in Fig. 1. Table 1 lists the notations used in this study.

3.1 Network and adversary model

First, the MANET is constructed as a graph $G(V, E)$ in which V is the group of nodes and E is the group of edges, $E \subseteq V \times V$. Let every node comprise a homogeneous communication area r_0. The wireless connection $(i, j) \in E$ while the Euclidean distance D_E between nodes i and j is lower than r_0. For 2-hop connectivity of i, the sub-graph G_i is assumed, which contains only the 1-hop and 2-hop neighbours of i. This is defined in Eq. (1):

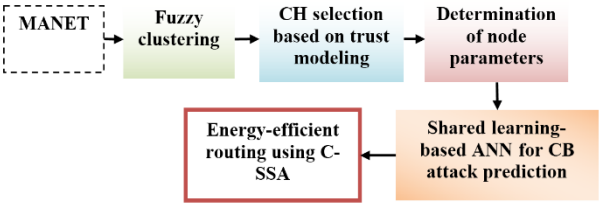

Figure. 1 Block diagram of the proposed study

Table 1. Lists of notations

Notations	Description
G	Graph
V	Group of nodes
E	Group of edges
r_0	Homogeneous communication range
(i, j)	Wireless connection between node i and j
D_E	Euclidean distance
G_i	Sub-graph
$2hop(i)$	2-hop neighbors of i
ξ	Dynamic threshold
t	Trust
dt	Distrust
u	Uncertainty
(α, β)	Parameters of the beta probability distribution
p, q	Number of positive and negative behaviour, respectively
α_{MF}, β_{MF}	Fading variables applied to validate the concept that trust is an entity
$f(\cdot)$	Function used to update the trust value
α_{rec}, β_{rec}	Parameters of the beta probability associated with the referral trust
X	Suspected packet dropper
A	Evaluator node
τ_α, τ_β	Trust fading variables
α_{fwd}^y, β_{fwd}^y	Value of positive and negative behavior of node y about the data transfer, respectively
$\alpha_{rperiod}^y$, $\beta_{rperiod}^y$	Value of positive and negative transfer/referral behavior of node y within the present period, respectively
β_{newf}^y	Penalty variable included in the recommendation trust of node y
$\tau_\alpha^y(t)$, $\tau_\beta^y(t)$	Interval-based fading variable for node y for the parameter α and β, respectively
N	Number of nodes
C	Number of clusters
t	Total time
e	Epochs

$$2hop(i) = \{w \in V, k \in V : (i,k) \in E \wedge (k,w) \in E\} \quad (1)$$

As well, let the dynamic threshold range is $\xi \in [0,1]$, where 0 denotes the minimum and 1 denotes the maximum.

Because the CB attack uses a malicious packet dropper that exhibits on and off behaviour with different nodes, it may exhibit good behaviour and bad behaviour, degrading the trust and increasing the number of false positives when declaring a node as a conflicting node. Such contradicting behaviour by attackers can be sorted out by the right design of the trust update mechanism.

3.2 Calculation of network parameters and trust updates

First, the number of nodes is partitioned into small groups based on fuzzy clustering to find the malicious and CB nodes. Then, various network parameters are determined independently for each node in each group along with the different intervals.

The considered network parameters [17] are the node degree, 2-hop connectivity, rate of link alterations, mobility, stability, residual energy and mean neighbourhood trustworthiness. After obtaining all parameters for each node in each group, the trust value of each node is calculated in the different periods depending on the uncertainty factor.

To achieve this, the trust is denoted as the tuple (t, dt, u), where t, dt and u are the 3 elements of trust, distrust and uncertainty. Initially, all nodes in each group maintain the path of many data sent or dropped by its adjacent via the Timeout Acknowledgement Message (TAM) strategy. The parameters (α, β) of the beta probability distribution are mapped to the number of positive and negative behavior, correspondingly associated with the different node operations such as data transfer and offering trust recommendations.

In the situation of data transfer, the parameters define the quantity of data transmitted and the quantity of data dropped, correspondingly. Such parameters are utilized to determine the values for trust, distrust and uncertainty as:

$$t = \frac{\alpha}{\alpha+\beta}(1-u) \quad (2)$$

$$dt = \frac{\beta}{\alpha+\beta}(1-u) \quad (3)$$

$$u = \frac{12\alpha\beta}{(\alpha+\beta)^2(1+\alpha+\beta)} \quad (4)$$

$$t + dt + u = 1 \quad (5)$$

Eqs. (2-5) can determine the trust defining the data transfer behavior. This data is utilized in the creation of a secure path to forward the data from an origin node to the target node. In the determination of trust, the TAM considers not only its direct observations; but, indirect observations acquired from adjacent nodes, which serve as recommenders. This is useful because the node in the MANET may not contain a sufficient number of direct observations on a freshly created adjacent node.

The parameters (α, β) of the beta probability distribution must be updated either regularly at constant periods of interval. The freshly updated values of α and β are acquired as a function of prior values, the present measure of good/bad behavior and a reduction variable called aging/fading variable determined by the trust recovery method applied in the TAM. The updated variables α and β are denoted by

$$\alpha_{new} = f(\alpha_{old}, p, \alpha_{MF}) \quad (6)$$

$$\beta_{new} = f(\beta_{old}, q, \beta_{MF}) \quad (7)$$

In Eqs. (6-7), p and q are the number of positive and negative behavior, correspondingly, α_{MF} and β_{MF} are the fading variables applied to validate the concept that trust is an entity, which fades away with interval. The function $f(\cdot)$ is utilized to update the trust value. The calculation of p and q, which particularly define the behavior in the present time is achieved by the TAM to transmit the trust update whereas the update of referral trust is achieved by considering the quantitative variance between the trust measure of the recommender and the evaluator node. So, transferring trust is applied to discourage the CB or malicious attacks and referral, or recommendation trust discourages the distrust recommenders' attacks.

A CB attack is a type of malicious packet-dropping attack that tries to distort the computation of forwarding and referral trust. The use of recommenders to compute a trust value provides the opportunity for the other kind of attacker called deceptive recommenders, who want to deliver fake suggestions to compromise the trustworthiness assessment. As a result, this model includes a new aspect of trust known as referral/recommendation trust, which shows the degree of trustworthiness of a neighbor node in offering truthful suggestions.

The evaluator node computes the referral trust on a neighbor using the dissimilarity metric between its

direct trust value on a target node calculated over time and the indirect trust value received through the neighbor. The referral trust is used in the selection of recommenders to offer indirect trust estimations. Those recommenders who have a greater referral trust are favored since they provide truthful suggestions.

It is essential to analyze the referral traits of a node to remove distrust recommenders. It is achieved using referral trust values, which are updated at constant intervals called trust update periods. This task is depending on the variance between the indirect trust values received in the prior trust update period and the direct trust values determined in the present trust update period. For each trust update, a count of good and false recommendation actions must be kept, representing the genuine and deceptive referral behavior, correspondingly. The count of false referral actions is mapped to the parameter α_{rec} and the count of distrust referral actions is mapped to the parameter β_{rec} of beta probability distribution associated with the referral trust.

An evaluation of the CB attack finds that it affects the trust assessment in such a way that it generates false positives for fraudulent recommenders while decreasing the referral trust of truthful recommenders. A suspected packet dropper *X* having on and off behavior shows signs of false behavior with a particular group of nodes and malevolent behavior with the other group of nodes. Especially, the nodes with whom *X* exhibits suspected packet dropping can evaluate it and provide it a less trust value. But, the nodes which observe the malicious behaviour of *X* can allocate it a greater trust value. This provides a variance in the analyses of the evaluator node *A* belonging to the particular group and the other node *Y* belonging to the other group.

So, the node *A* reduces the referral trust of node *X* and thus the false positives are increased during the identification of false recommenders. This issue is observed via a robust trust determination strategy, which tries to create a probability-based prediction of CB attack and false recommender attack. Particularly, all nodes accumulate the information associated with those subject nodes, which causes the development of false recommendation incidences of all recommenders. For example, when a similar subject node *X* has been involved in a rise in the value of β_{rec} of a recommender, there is a better opportunity that the subject node is a suspected packet dropper having a CB attack model.

The major challenge associated with the accumulation of the information regarding all recommender-recommended pairs is the inadequate storage of a MANET node. So, the demand for a memory-effective information pattern arises, so this trust determination method uses the ANN model. It comprises the information regarding the recommender-recommended pair nodes along with the count of the number of times the recommended contributed towards a rise in the value of β_{rec}.

The strategy applied for the design of the defensive scheme to enable the trust update in the occurrence of a CB attack needs the evaluator (the node concerned with determining the referral trust for all recommender neighbors) to make the ANN of all recommender nodes. The data structure stores data associated with the recommended who is responsible for increasing the number of unfavorable referral occurrences. As well, it contains information regarding the number of such occurrences, which is used to detect a conflicting attacker's activity.

Because of applying a probability-based prediction of a CB attack, trust in 2 dimensions must be updated. The trust updates are based on a temporal fading method in which the trust in any dimension is updated at regular intervals by using a composite measure of its behavior collected during previous periods and the behavior shown in the current period. The previous behavior is discounted by the variable called trust fading variable defined by τ_α and τ_β, correspondingly. For CB attack identification, the present period's behaviour is also discounted to consider the probabilities of the recommended being a deceptive recommender or the recommender being a CB attacker.

Trust updates without considering CB attack are defined as the following Eq. (8):

$$trust(t+1) = trust(t) \times fading\ variable + trust(present\ time) \quad (8)$$

Trust updates considering CB attack are defined as the following Eq. (9):

$$trust(t+1) = trust(t) \times fading\ variable + trust(present\ time) \times conflicting\ behavior\ discount\ variable \quad (9)$$

For the recommender node x, both the referral and forwarding trust updates are performed as the following Eqs. (10-27):

1) Referral trust updates without CB attack:

$$\alpha_{rec}(t+1) = \alpha_{rec}(t) \times \tau_\alpha(t) + \alpha_{rperiod} \quad (10)$$

$$\beta_{rec}(t+1) = \beta_{rec}(t) \times \tau_\beta(t) + \beta_{rperiod} \quad (11)$$

$$\tau_{\alpha}(t) = \gamma \times \frac{\alpha_{rec}(t)}{\alpha_{rec}(t)+1} \quad (12)$$

$$\tau_{\beta}(t) = \mu \times \frac{\beta_{rec}(t)}{\beta_{rec}(t)+1} \quad (13)$$

2) *Referral trust updates with CB attack*:

$$\alpha^{x}_{rec}(t+1) = \alpha^{x}_{rec}(t) \times \tau^{x}_{\alpha}(t) + \alpha^{x}_{rperiod} \times \left(\frac{n}{n+1}\right) \quad (14)$$

$$\beta^{x}_{rec}(t+1) = \beta^{x}_{rec}(t) \times \tau^{x}_{\beta}(t) + \beta^{x}_{newr} \quad (15)$$

$$\beta^{x}_{newr} = \frac{\sum_{1 \le i \le n}\left(1+\frac{\beta^{x}_{rec}(t)}{\beta^{x}_{rec}(t)+\beta^{y}_{fwd}(t)}\right)}{n} \times \beta^{x}_{rperiod} \quad (16)$$

$$\tau^{x}_{\alpha}(t) = \gamma \times \frac{\alpha^{x}_{rec}(t)}{\alpha^{x}_{rec}(t)+1} \quad (17)$$

$$\tau^{x}_{\beta}(t) = \mu \times \frac{\beta^{x}_{rec}(t)}{\beta^{x}_{rec}(t)+1} \quad (18)$$

3) Forwarding trust updates without CB attack:

$$\alpha(t+1) = \alpha(t) \times \tau_{p}(t) + \alpha_{rperiod} \quad (19)$$

$$\beta(t+1) = \beta(t) \times \tau_{q}(t) + \beta_{rperiod} \quad (20)$$

$$\tau_{p}(t) = \gamma \times \frac{\alpha(t)}{\alpha(t)+1} \quad (21)$$

$$\tau_{q}(t) = \mu \times \frac{\beta(t)}{\beta(t)+1} \quad (22)$$

4) Forwarding trust updates with CB attack:

$$\alpha^{y}_{fwd}(t+1) = \alpha^{y}_{fwd}(t) \times \tau^{y}_{\alpha}(t) + \alpha^{y}_{rperiod} \times \left(\frac{|X|}{|X|+1}\right) \quad (23)$$

$$\beta^{y}_{fwd}(t+1) = \beta^{y}_{fwd}(t) \times \tau^{y}_{\beta}(t) + \beta^{y}_{newf} \quad (24)$$

$$\beta^{y}_{newf} = \frac{\sum_{\forall x | x \in X}\left(1+\frac{\beta^{y}_{fwd}(t)}{\beta^{y}_{fwd}(t)+\beta^{x}_{rec}(t)}\right)}{|X|} \times \beta^{y}_{rperiod} \quad (25)$$

$$\tau^{y}_{\alpha}(t) = \gamma \times \frac{\alpha^{y}_{fwd}(t)}{\alpha^{y}_{fwd}(t)+1} \quad (26)$$

$$\tau^{y}_{\beta}(t) = \mu \times \frac{\beta^{y}_{fwd}(t)}{\beta^{y}_{fwd}(t)+1} \quad (27)$$

In the above equations, α^{y}_{fwd} is the value of positive behavior of node y about the data transfer, β^{y}_{fwd} is the value of negative behavior of node y about the data transfer, $\alpha^{y}_{rperiod}$ is the value of positive transfer/referral behavior of node y within the present period, $\beta^{y}_{rperiod}$ is the value of negative transfer/referral behavior of node y within the present period, β^{y}_{newf} is the penalty variable included in the recommendation trust of node y, $\tau^{y}_{\alpha}(t)$ is the interval-based fading variable for node y for the parameter α and $\tau^{y}_{\beta}(t)$ is the interval-based fading variable for node y for the parameter β.

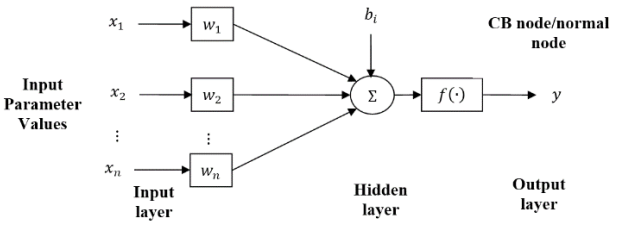

Figure. 2 Structure of ANN for CB node prediction

Algorithm for the proposed CBAP-SLANN-C-SSA

Input: N number of nodes, C number of clusters, t periods, training database for each cluster (network parameters and trust update variables)

Output: CB node

1. **Begin**
2. ***for***$(each\ cluster\ c\ in\ t)$
3. Get the corresponding training database;
4. Train the ANN model on each cluster for e epochs;
5. ***end for***
6. Combine the trained model of each cluster;
7. Obtain the global decision on a final prediction, i.e. whether the node has a CB or not;
8. Seclude the CB malicious node from the routing path;
9. Apply the C-SSA to choose the most stable path for effective data transfer;
10. Transmit the data from origin to the target node;
11. **End**

3.3 Shared learning-based ANN for CB attacker node prediction

Once all the network parameters and trust update parameters of each node in each cluster (group) are determined, those are created as a database. The database includes the network parameters, $\alpha_{rec}(t)$, $\alpha_{rperiod}$, $\beta_{rec}(t)$, $\beta_{rperiod}$, $\tau_{\alpha}(t)$, $\tau_{\beta}(t)$, γ, μ,

Table 2. Simulation parameters

Parameters	Values
Topology area	1400×1400m^2
Number of nodes	200
Number of attackers	15
Channel type	Wireless
Antenna type	Omni-directional
Link layer type	Link layer
Radio propagation scheme	2-ray ground
Queue class	Drop tail
MAC type	MAC802.11
Mobility model	Random waypoint
Protocol type	AODV
Node mobility	10-60m/sec
Transmission range	250m
Initial energy	16.5J
Packet size	512bytes/packet
Traffic type	Constant bit rate
Simulation time	300sec

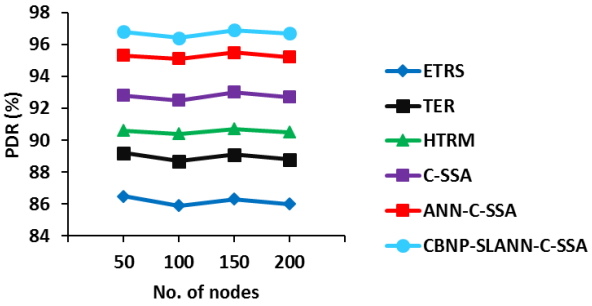

Figure. 3 PDR vs. No. of nodes

$\alpha^x_{rec}(t)$, $\alpha^x_{rperiod}$, $\beta^x_{rec}(t)$, β^x_{newr}, $\tau^x_\alpha(t)$, $\tau^x_\beta(t)$, $\beta^x_{rperiod}$, $\tau_p(t)$, $\tau_q(t)$, $\alpha^y_{fwd}(t)$, $\alpha^y_{rperiod}$, $\tau^y_\alpha(t)$, $\tau^y_\beta(t)$, β^y_{newf}, $\beta^y_{rperiod}$. Using this database, the ANN model [17], as illustrated in Fig. 2, is trained in the shared learning environment to predict CB nodes from different clusters in the MANET. Thus, based on the shared learning concept, the ANN model can be trained in each group for one or a few epochs. Then, the trained model for each cluster is combined to get a global decision on predicting the CB nodes without using the threshold values for successive periods.

4. Result and discussion

The effectiveness of the CBAP-SLANN-C-SSA algorithm with the C-SSA routing protocol is assessed by simulating it in network simulator version 2.34 (NS2.34) and evaluated with the existing algorithms: C-SSA [16], ANN-C-SSA [17], ETRS [19], TER [22] and HTRM [23]. The assessment is carried out regarding PDR, PLR, throughput, energy consumption, end-to-end delay, false positives and

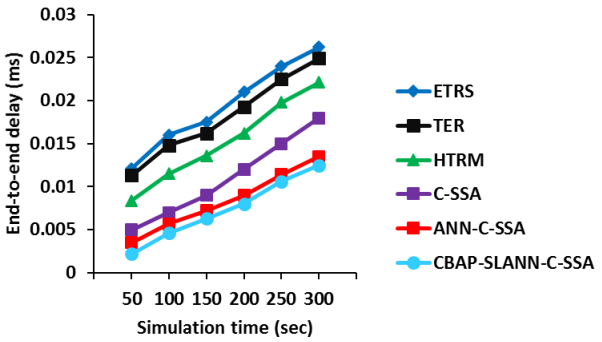

Figure. 4 End-to-end delay vs. simulation time

detection rate. To measure the performance of the proposed CBAP-SLANN-C-SSA algorithm, the considered existing models are also simulated and tested for CB attack prediction. The simulation parameter settings for the existing and proposed algorithms are given in Table 2.

4.1 PDR

It refers to the percentage of the number of data accepted correctly by the target node to the overall amount of data transferred from the origin node.

Fig. 3 portrays the PDR (in %) achieved by the ETRS, TER, HTRM, C-SSA, ANN-C-SSA and CBAP-SLANN-C-SSA algorithms under a varying number of nodes. It indicates that the PDR achieved by the CBAP-SLANN-C-SSA algorithm is larger than the other algorithms to detect the suspected/CB attackers in the network during data transfer. For 150 nodes, the PDR of ANN-C-SSA is increased by 12.28%, 8.75%, 6.84%, 4.19% and 1.4%, compared to the ETRS, TER, HTRM, C-SSA and ANN-C-SSA algorithms, respectively.

4.2 End-to-end delay

It is the mean interval needed by data transported between the origin node and the target nodes.

Fig. 4 exhibits the end-to-end delay (in ms) achieved by the ETRS, TER, HTRM, C-SSA, ANN-C-SSA and CBAP-SLANN-C-SSA algorithms under a varying simulation time (in sec). It observes that the end-to-end delay obtained by the CBAP-SLANN-C-SSA algorithm is less than the other algorithms to identify the suspected/CB attacks in the network. If the simulation time is 200sec, the end-to-end delay of ANN-C-SSA is 61.9% less than the ETRS, 58.55% less than the TER, 50.62% less than the HTRM, 33.33% less than the C-SSA and 11.11% less than the ANN-C-SSA.

4.3 PLR

It defines the percentage of data dropped through

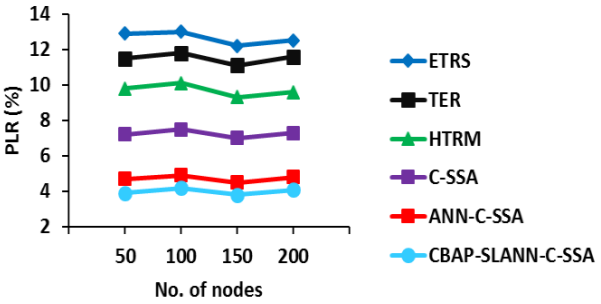

Figure. 5 PLR vs. No. of nodes

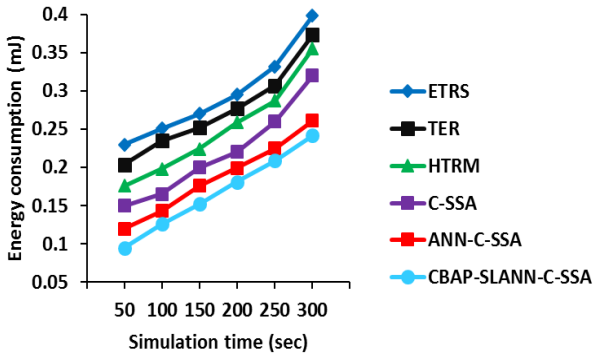

Figure. 6 Energy consumption vs. simulation time

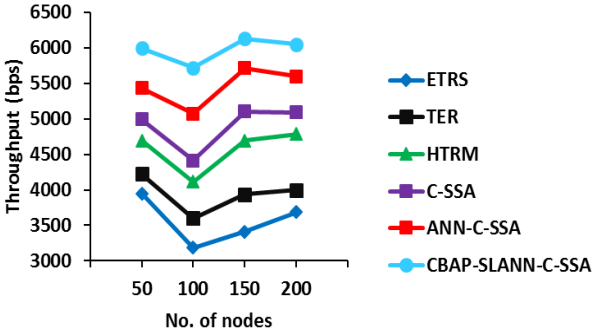

Figure. 7 Throughput vs. No. of nodes

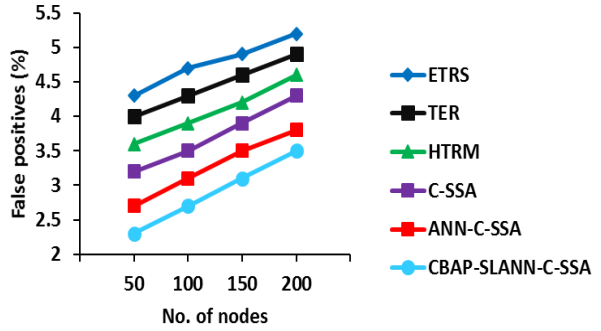

Figure. 8 False positives vs. No. of nodes

malicious nodes to the total amount of data delivered.

Fig. 5 displays the PLR (in %) achieved by the ETRS, TER, HTRM, C-SSA, ANN-C-SSA and CBAP-SLANN-C-SSA algorithms under a varying number of nodes. It analyses that the PLR obtained by the CBAP-SLANN-C-SSA algorithm is less than the other algorithms to detect the malicious/CB nodes in the network. For example, if there are 150 nodes in the network, the PLR of CBAP-SLANN-C-SSA is 68.85% less than the ETRS, 65.77% less than the TER, 59.14% less than the HTRM, 45.71% less than the C-SSA and 15.56% less than the ANN-C-SSA.

4.4 Energy consumption

It is the ratio of average used energy at every node to the primary energy.

Fig. 6 portrays the energy consumption (in mJ) achieved by the ETRS, TER, HTRM, C-SSA, ANN-C-SSA and CBAP-SLANN-C-SSA algorithms under a varying simulation time (in sec). It observes that the energy consumption obtained by the CBAP-SLANN-C-SSA algorithm is less than the other algorithms to identify the malicious/CB nodes in the network. If the simulation time is 200sec, the energy consumption of CBAP-SLANN-C-SSA is 38.64% less than the ETRS, 34.66% less than the TER, 30.12% less than the HTRM, 17.73% less than the C-SSA and 9.05% less than the ANN-C-SSA.

4.5 Throughput

It is the destination node's average number of bits received per second.

Fig. 7 depicts the throughput (in bits/sec) achieved by the ETRS, TER, HTRM, C-SSA, ANN-C-SSA and CBAP-SLANN-C-SSA algorithms under a different amount of nodes. It observes that the throughput obtained by the CBAP-SLANN-C-SSA algorithm is greater than the other algorithms to detect the malicious/CB nodes in the network. For example, if there are 150 nodes in the network, the throughput of CBAP-SLANN-C-SSA is 79.73% greater than the ETRS, 55.72% greater than the TER, 30.65% greater than the HTRM, 20.07% greater than the C-SSA and 7.29% greater than the ANN-C-SSA.

4.6 False positives

It is the percentage of malicious trustworthy nodes to the overall amount of trusted nodes.

Fig. 8 shows the false positives (in %) achieved by the ETRS, TER, HTRM, C-SSA, ANN-C-SSA and CBAP-SLANN-C-SSA algorithms under a varying number of nodes. It analyses that the false positives obtained by the CBAP-SLANN-C-SSA algorithm is less than all other algorithms to detect the malicious/CB nodes in the network. For example, if there are 150 nodes in the network, the false positives of CBAP-SLANN-C-SSA is 36.73% less than the ETRS, 32.61% less than the TER, 26.19% less than the HTRM, 20.51% less than the C-SSA and

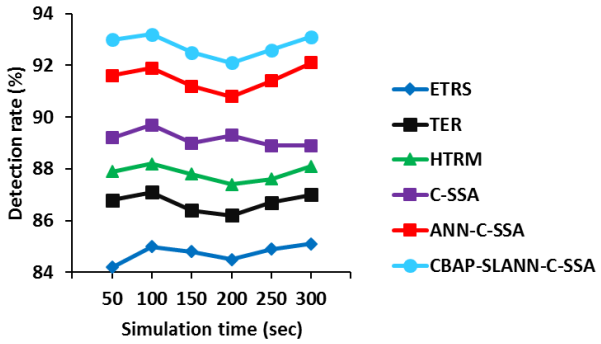

Figure. 9 Detection rate vs. simulation time

11.43% less than the ANN-C-SSA.

4.7 Detection rate

It is the proportion of detected malicious nodes to the overall amount of malicious nodes.

Fig. 9 portrays the detection rate (in %) achieved by the ETRS, TER, HTRM, C-SSA, ANN-C-SSA and CBAP-SLANN-C-SSA algorithms under varying simulation times (in sec). It observes that the detection rate obtained by the CBAP-SLANN-C-SSA algorithm is higher than all other protocols to recognize the malicious/CB nodes. If the simulation time is 200sec, the detection rate of CBAP-SLANN-C-SSA is 8.99% higher than the ETRS, 6.84% higher than the TER, 5.38% higher than the HTRM, 3.14% higher than the C-SSA and 1.43% higher than the ANN-C-SSA.

5. Conclusion

In this study, the CBAP-SLANN algorithm was presented for CB attack prediction in various nodes and timeslots with the same node. Primarily, nodes were grouped into overlapping clusters and the trust of each node was assessed independently for each group. Also, the network parameters of each node in each group were determined in different periods. The ANN algorithm was then trained in shared environment for each group using various network parameters and trust values in the different periods. Further, the trained model in each group was combined to get the outcome to predict the CB attacks in the network. Finally, after deploying 300 nodes, the simulation results realized that the CBAP-SLANN algorithm achieves 93.1% accuracy when compared to the traditional algorithms in MANET.

Conflict of interest

The authors declare no conflict of interest.

Author contributions

Conceptualization, methodology, software, validation, Vijay Anand; formal analysis, investigation, Abel Thangaraja; resources, data curation, writing—original draft preparation, Vijay Anand; writing—review and editing, Vijay Anand; visualization; supervision, Abel Thangaraja;

References

[1] F. A. Fattah, K. A. Farhan, F. H. A. Tarawneh, and F. A. Tamimi, "Security Challenges and Attacks in Dynamic Mobile Ad Hoc Networks MANETs", In: *Proc. of IEEE Jordan International Joint Conf. on Electrical Engineering and Information Technology*, pp. 28-33, 2019.

[2] G. Liu, Z. Yan, and W. Pedrycz, "Data Collection for Attack Detection and Security Measurement in Mobile Ad Hoc Networks: A Survey", *Journal of Network and Computer Applications*, Vol. 105, pp. 105-122, 2018.

[3] M. A. Elsadig and Y. A. Fadlalla, "Mobile Ad Hoc Network Routing Protocols: Performance Evaluation and Assessment", *International Journal of Computing and Digital Systems*, Vol. 7, No. 01, pp. 59-66, 2018.

[4] B. O. Abdulazeez and O. N. Akpofure, "Mobile Adhoc Network Routing Protocols: Performance Evaluation & Assessment", *An International Multidisciplinary Research Journal*, Vol. 11, No. 5, pp. 1266-1273, 2021.

[5] M. G. K. Alabdullah, B. M. Atiyah, K. S. Khalaf, and S. H. Yadgar, "Analysis and Simulation of Three MANET Routing Protocols: A Research on AODV, DSR & DSDV Characteristics and their Performance Evaluation", *Periodicals of Engineering and Natural Sciences*, Vol. 7, No. 3, pp. 1228-1238, 2019.

[6] T. S. Vamsi, E. P. Kumar, and T. Sruthi, "Performance Analysis of AODV Routing Protocol in Manet under Blackhole Attack", *International Journal of Engineering Research and Applications*, Vol. 9, No. 5, pp. 58-63, 2019.

[7] A. M. Bamhdi, "Efficient Dynamic-Power AODV Routing Protocol Based on Node Density", *Computer Standards & Interfaces*, Vol. 70, pp. 1-16, 2020.

[8] N. Prasath and J. Sreemathy, "Optimized Dynamic Source Routing Protocol for MANETs", *Cluster Computing*, Vol. 22, No. 5, pp. 12397-12409, 2019.

[9] G. Najafi and S. J. Gudakahriz, "A Stable Routing Protocol Based on DSR Protocol for Mobile Ad Hoc Networks", *International*

Journal of Wireless and Microwave Technologies, Vol. 3, pp. 14-22, 2018.

[10] A. A. Mahamune and M. M. Chandane, "An Efficient Trust-Based Routing Scheme against Malicious Communication in MANET", *International Journal of Wireless Information Networks*, Vol. 28, No. 3, pp. 344-361, 2021.

[11] A. B. Usman and J. Gutierrez, "Toward Trust Based Protocols in a Pervasive and Mobile Computing Environment: A Survey", *Ad Hoc Networks*, Vol. 81, pp. 143-159, 2018.

[12] P. Sathyaraj and D. R. Devi, "Designing the Routing Protocol with Secured IoT Devices and QoS over Manet Using Trust-Based Performance Evaluation Method", *Journal of Ambient Intelligence and Humanized Computing*, Vol. 12, No. 7, pp. 6987-6995, 2021.

[13] M. S. Usha and K. C. Ravishankar, "Implementation of Trust-Based Novel Approach for Security Enhancements in MANETs", *SN Computer Science*, Vol. 2, No. 4, pp. 1-7, 2021.

[14] H. Xu, H. Si, H. Zhang, L. Zhang, Y. Leng, J. Wang, and D. Li, "Trust-Based Probabilistic Broadcast Scheme for Mobile Ad Hoc Networks", *IEEE Access*, Vol. 8, pp. 21380-21392, 2020.

[15] D. Zhang, C. Gong, K. Jiang, X. Zhang, and T. Zhang, "A Kind of New Method of Intelligent Trust Engineering Metrics (ITEM) for Application of Mobile Ad Hoc Network", *Engineering Computations*, pp. 1617-1643, 2019.

[16] N. Veeraiah, O. I. Khalaf, C. V. P. R. Prasad, Y. Alotaibi, A. Alsufyani, S. Alghamdi, and N. Alsufyani, "Trust Aware Secure Energy Efficient Hybrid Protocol for MANET", *IEEE Access*, pp. 120996-121005, 2021.

[17] K. V. Anand and G. A. Thangaraja, "A Competent Intelligence Modeling for Trust-Based Security Scheme in Mobile Ad Hoc Network", *International Journal of Computer Networks and Applications*, Vol. 9, No. 6, pp. 736-745, 2022.

[18] M. Sirajuddin, C. Rupa, C. Iwendi, and C. Biamba, "TBSMR: A Trust-Based Secure Multipath Routing Protocol for Enhancing the QoS of the Mobile Ad Hoc Network", *Security and Communication Networks*, pp. 1-9, 2021.

[19] A. A. Mahamune and M. M. Chandane, "An Efficient Trust-Based Routing Scheme against Malicious Communication in MANET", *International Journal of Wireless Information Networks*, pp. 1-18, 2021.

[20] N. Chugh, G. S. Tomar, R. S. Bhadoria, and N. Saxena, "A Novel Anomaly Behavior Detection Scheme for Mobile Ad Hoc Networks", *Electronics*, Vol. 10, No. 14, pp. 1-18, 2021.

[21] R. I. Sajan and J. Jasper, "A Secure Routing Scheme to Mitigate Attack in Wireless Adhoc Sensor Network", *Computers & Security*, Vol. 103, pp. 1-14, 2021.

[22] R. Suganthi, I. Poonguzhali, J. Navarajan, R. Krishnaveni, and N. N. Saranya, "Trust based Efficient Routing (TER) Protocol for MANETS", *Materials Today: Proceedings*, Vol. 80, pp. 2014-2021, 2023.

[23] S. N. Pari and K. Sudharson, "Hybrid Trust Based Reputation Mechanism for Discovering Malevolent Node in MANET", *Computer Systems Science and Engineering*, Vol. 44, No. 3, pp. 2775-2789, 2023.

[24] S. Shafi, S. Mounika, and S. Velliangiri, "Machine Learning and Trust Based AODV Routing Protocol to Mitigate Flooding and Blackhole Attacks in MANET", *Procedia Computer Science*, Vol. 218, pp. 2309-2318.

[25] K. Nirmaladevi and K. Prabha, "A Selfish Node Trust Aware with Optimized Clustering for Reliable Routing Protocol in Manet", *Measurement: Sensors*, Vol. 26, p. 100680, 2023.