Received: 17 August 2021 | Revised: 19 December 2021 | Accepted: 17 February 2022

DOI: 10.1002/ett.4489

RESEARCH ARTICLE

WILEY

Trust-oriented peered customized mechanism for malicious nodes isolation for flying ad hoc networks

Waqas Buksh[1] | Ying Guo[1] | Saleem Iqbal[2] | Kashif Naseer Qureshi[3] | Jaime Lloret[4,5]

[1]School of Computer Science and Engineering, Central South University, Changsha, China

[2]Department of Computer Science, Allama Iqbal Open University, Islamabad, Pakistan

[3]Centre of Excellence in Artificial Intelligence, Department of Computer Science, Bahria University, Islamabad, Pakistan

[4]Instituto de Investigacion para la Gestion Integrada de Zonas Costeras, Universitat Politecnica de Valencia, Valencia, Spain

[5]School of Computing and Digital Technologies, Staffordshire University, Stoke, UK

Correspondence
Jaime Lloret, Instituto de Investigacion para la Gestion Integrada de Zonas Costeras, Universitat Politecnica de Valencia, Valencia, Spain.
Email: jlloret@dcom.upv.es

Funding information
European Commission; Ministerio de Economía y Competitividad; Ministerio de Agricultura, Pesca y Alimentación" through the "proyectos de innovación de interés general por grupos operativos de la Asociación Europea para la Innovación en materia de productividad y sostenibilidad agrícolas (AEI-Agri)" " project GO TECNOGAR; Ministerio de Ciencia e Innovación, Grant/Award Number: PID2020-114467RR-C33

Abstract

Flying Ad Hoc Networks (FANETs) are gaining popularity due to its extra-ordinary features in avionics and electronics domain. FANETs are also considered as most powerful weapon in military assets as well as in civil security applications. Due to its infrastructureless design and wireless nature network, some security challenges are overhead that should be overcome before the whole network performance degradation. Malicious nodes are capable of degrading the network throughput and credibility by including false and malicious data. Securing the dynamic network from malicious nodes is a critical issue in infrastructureless environment. In this paper we have purely focused on identification and isolation of malicious node in order to make enhancement in packet delivery rate and maintain the network reliability. To accomplish all these tasks, we have introduced Trust-Oriented Peered Customized Mechanism (TOPCM) to estimate the trust value among flying ad hoc nodes. In this research, we have also eliminated the malicious nodes presence that causes misbehavior and interruption in the network. To demonstrate the effectiveness of our proposed approach we have used Network Simulator NS2 to demonstrate the entire process into simulated environment. Simulated results showed that proposed TOPCM works more effectively and meets our desired expectation. The main contribution of this research is to establish trust among nodes that will be helpful to isolate the malicious nodes and make enhancement in packet delivery rate.

1 | INTRODUCTION

Flying Ad Hoc Networks (FANETs) are most promising and efficient source to accomplish the crucial tasks by coordination and collaboration with each other. FANETs are self-organized, self-configured, and infrastructureless network, inherited form of Wireless Ad Hoc Network; however, one of the most valuable research direction toward ad hoc networks.[1,2] In FANETs, because of its wireless nature, infrastructureless design, and frequently changing topology, many security issues and challenges exist and play an important role in degradation of the network lifetime, reliability, and credibility. Flying ad hoc nodes perform coordination and collaboration with other nodes to forward desired information beyond their transmission range. To accomplish this task, flying ad hoc node must have excellent cooperation between them. But malicious nodes perform malicious activities and as a result, they badly effect the network life time by dropping packets.[3,4] Malicious is a mechanism that can be applied by eavesdropper on each participated node to perform misbehaving activities and those nodes that perform malicious activities called malicious nodes. Nodes are said to be malicious if they capable of performing data forwarding but they unable to do so.[5,6] The concept of FANETs is demonstrated in Figure 1.

Node independency to join or leave network without informing other nodes build a chance to eavesdropper for applying malicious mechanism. Malicious nodes aim to degrade the limited network resource like nodes' battery, power consumption, and their bandwidth that cause network lifetime degradation. Frequent changes in network topology, where the movement of node involved is high, may cause malicious node behavior.[5,7] Malicious nodes compromise network resources by choosing false routing and dropping the packets. Packet transmission process may take different path selection, so eavesdropper can introduced their own path.[8,9] In wireless ad hoc dynamic networks, malicious node may be a part of eavesdropper's network to disturb the communication. Packets dropping rate and frequent modifications indicates the malicious node presence in a network. If a network is compromised by limited resource constraint (battery drain, power, and bandwidth consumption), then there is a possibility of presence of a malicious node with misbehaving activities among the participated nodes. Also when a packet has not reached the desired destination then there is a chance of presence of malicious node.[10,11]

The prime contributions of this paper are as follows:

- introduction of state-of-the-art trust-oriented mechanism and stimulate the research flow towards ad hoc networks (FANETs) and
- to perform identification and isolation of malicious nodes from dynamic network by establishing an autonomous trust-oriented mechanism.

The FANETs are most appropriate type of networks deployed in hard to reach area for performing crucial task. The applications of FANETs are found in military as well as in civil security applications. The use of unmanned aerial vehicles (UAVs) such as surveillance of border areas and monitoring the sensitive surfaces in the military domain is witnessed in different forms for the last two decades .[12] The FANETs also have some commercial applications like search and rescue operations, where the response time is very critical. In order to search and recognize the target, FANETs perform efficiently and facilitate the rescue team towards reaching the target.[13] Table 1 shows the commercial applications of FANETs.

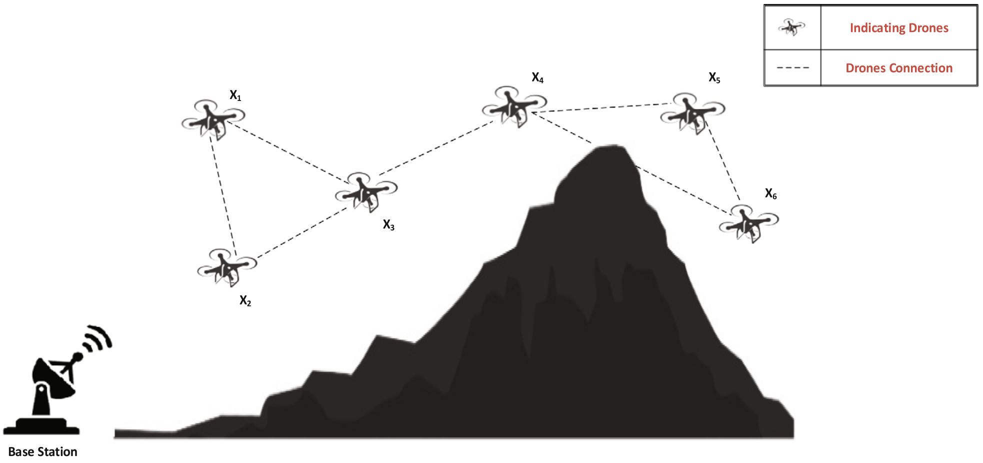


FIGURE 1 Flying ad hoc networks with drones and base station

TABLE 1 Commercial applications of flying ad hoc networks

Commercial application	Application category description
Search and Rescue (SAR)	• Perform Random search and recognize target area. • Extract victims on disaster location. • Perform scanning in circular area via repeated checks.
Coverage	• Perform surveillance services by monitoring and mapping the target area or city streets. • Provide network coverage by unmanned aerial vehicles
Construction	• Lifting the building components and place them at specific positions
Transportation and Good Delivery	• Provide transportation services and delivery of good in fast and efficient way.

Most of the civil applications are covered under the umbrella of coverage mission category. In this mission category, it performs area-wise coverage like mapping and border monitoring or surveillance. The size of area can be increased or decreased based on mission requirements. The next commercial use of FANET is in construction missions where UAVs are used to perform construction by lifting the building elements. The swarm of UAVs organizes the elements of building elements and place them at their specific position. In order to accomplish this mission properly, the timing and synchronization between the UAVs collaboration should be ensured by communication architecture. In this category, delivery and transportation mission, the UAVs are employed to provide transportation services and delivery of goods in fast and efficient way. For example, Amazon use mini UAVs to provide transportation service and deliver goods to customers. In this type of scenario, the estimated distance value between pickup point and delivery point should be considered.

The paper is structured as follows: Section 2 explains some past approaches as literature review that has been adopted by previous researchers, and limitations of these approaches are part of this section. Section 3 demonstrates the detailed working and implementation of proposed Trust-Oriented Peered Customized Mechanism (TOPCM). Finally, Section 4 presents simulation details and results comparison of proposed mechanism. Section 5 presents conclusion and future work remarks.

2 | LITERATURE REVIEW

In dynamic type of networks, during the data transmission by localization and globalization, each node may act as a malicious node and perform malicious activities resulting in network throughput degradation as well as the network reliability downsizing by inclusion of false routing and other selfish behaviors. In short, the desired network life is under attack. Predicting and monitoring the behavior of malicious nodes as well as isolating them from dynamic network is a crucial task.[14] Many authors demonstrate their defensive approaches to satisfy the security requirements of dynamic network but those solutions are not much faithful in terms of reliability and credibility. Majority of the solutions are tagged with security loop-holes. Many researchers demonstrate their proposed solutions to perform detection and prevention of malicious node to overcome these types of security challenges. Here some trust evaluation mechanisms that have been used to evaluate the trust value of neighbor node or forwarder node in direct and hybrid ways are mentioned along with prevention of malicious nodes.

Reputation system enables source nodes to select secure and reliable paths by using trust mechanism. This mechanism has shown node's reliability by detecting the malicious nodes in the reputation trust evaluation system.[15] In order to tackle the UAV-Sensor communication, author established a Trust-Based Security mechanism by aggregation of direct and indirect trust values for determining the final trust value. Direct and Indirect Trust evaluation mechanism employed sensor-received information (Direct Trust Update frame - Indirect Trust Update ITU frame).[16] Data-driven method has adopted to ensure secure communications and employed message creator behavior to generate observational evidence. Distributed trust evaluation has been made, based on the observational evidence, to identify and prevent malicious node.[17] In this research paper author established a trust evaluation mechanism by calculating the direct and indirect trust values. Author used network behavior defining parameters (signal strength, PDR, nodes energy, and delay) with their optimal weight defined by genetic algorithm in order to calculate direct trust value while indirect trust value has been calculated by the recommendation manager.[18] Bayesian estimation approach considered traffic profile information and different parameters (PRE, PSE, and TPE) to calculate the final trust value of targeted node, by adding direct trust value and indirect trust value as well as detecting and isolating the malicious node.[19] Author defined a mechanism based on trace file (TCL) to calculate the trust value of node present in the network. TCL contains all the detailed information related to traffic flow. TCL traffic flow information is employed to evaluate the trustworthy level of node.[20]

The trust-oriented approaches are more effective to make improvement in security and cooperation of network. Trust level of nodes can be achieved by using fuzzy logic trust management model to identify and isolate the malicious nodes. The node trust level is calculated by immediate node as well as recommendation node. Fuzzy classification model obtained trust value of nodes by employing social parameters and quality parameters. Fuzzy classification method is used to classify the nodes based on their behavior and performance. The main goal of this research is to classify the node into different clusters like good, bad, and neutral.[21,22] Another approach for securing the routing mechanism based on trustworthy nodes selection procedure for offering routing performance. In order to make enhancement in security, the node selection procedure technique employs trust values of nodes to identify and isolate the malicious nodes from the routing process. This technique adopted secure and reliable route by selecting trustworthy nodes. A cooperative approach aims to detect malicious nodes from network and provide malicious node-free environment to enhance packet delivery rate.[23,24] This approach has two phases in order to defend the malicious attacks. In first phase, author performed rules and principles to identify the malicious nodes and isolate them from the network on the base of their behavior to prevent spreading the false information to other nodes. Moreover, Reference 25 detected black hole attacks and designed a defensive mechanism. Table 2 shows the comparison with technical details.

Table 2 represents a comparison of state-of-art FANET-based approaches that are applicable in identification of malicious nodes. Different characteristics have been considered in terms of pros and cons. Some approaches are limited to only identification of malicious nodes instead of both identification and isolation. The involvement of central entity causes significant processing overhead while performing direct and indirect trust calculations. In addition, due to dependency of another node or recommender node, while getting the recommendation about other nodes, the trust value of nodes may be compromised. Because when the recommender node is not trustworthy then its recommendation can also be unrealistic and nontrustworthy. In some of the approaches, only static nodes are considered and employed. These approaches are not completely functional with independent nodes and they promote third party recommendation that may cause significant processing and degrade the trust level of nodes. Previously, trust values of nodes are calculated by only employing the trace files that contained the detailed information of traffic flow in the network. However, if the TCL values are modified by other nodes then trust value of nodes are easily compromised and malicious nodes can destroy the performance of whole network. Here a trust-oriented mechanism that properly identifies the malicious nodes and isolate them to make network more reliable is need to established.

TABLE 2 Comparison with technical details

Evaluation metrics	Reputation system	UAV – sensor communication	Genetic algorithm	BTEM	TCL
Trust evaluation mechanism	Central hub recommendation	DTU and IDTU Packets	Network attributes	Traffic profile (TP)	TCL values
Insignificant processing overhead	Yes	No	Yes	Yes	Yes
Dynamic or static nodes	Dynamic	Static	Dynamic	Static	Dynamic
Security compromises	Yes	Yes	Yes	Yes	Yes
Detection and isolation	Only Detection	Only Detection	Both	Both	Both
Communication type	UAV-UAV	UAV-Static WSN	UAV-UAV	B/w Static Sensor	UAV-UAV
Direct trust	Yes	Yes	Yes	Yes	Yes
Indirect/recommendation trust	Yes	Yes	Yes	Yes	No
Distributed or centralized	Centralized	Distributed	Distributed	Distributed	Centralized

Abbreviations: TCL, trace file; UAV, unmanned aerial vehicles.

3 | PROPOSED WORK

To increase the FANETs trustworthiness, this research proposes TOPCM. The TOPCM is expressed in descriptive and qualitative manners that may act as an additional brick to overcome the subjected security loop-holes. Moreover, this research contains how the proposed approach will be functional in all possible aspects to upgrade the network credibility. The proposed methodology is demonstrated in abstract form by using block diagram as shown in Figure 2. Possible assumptions that have been adopted are elaborated in this section. Simulation results authenticated that our proposed mechanism is qualitatively better and meets our expected requirements. Here some assumptions are followed throughout the simulation environment. These assumptions are considered realistic and act as the next stair to proceed toward the proposed approach.

The assumptions are as follows:

- Source node and destination nodes are trustworthy and all other nodes or intermediate present in a dynamic network initially marked as trustworthy.
- GPS locations of all participated nodes are well-known by Base Station.
- Intermediate node must send R (RREQ) only to (RREQ) Requested node

Initially all nodes by default are assigned with trust value to make trust establishment. After that, peer-to-peer node trust evaluation is performed by employing some worthy parameters ($FN_{(D\_Add)}$, $FN_{(B\_ID)}$, $FN_{(ID)}$, $FN_{(NH\_ID)}$) to perform trustworthy decision. Decision-maker module is responsible for distributing the nodes in malicious or trustworthy list.

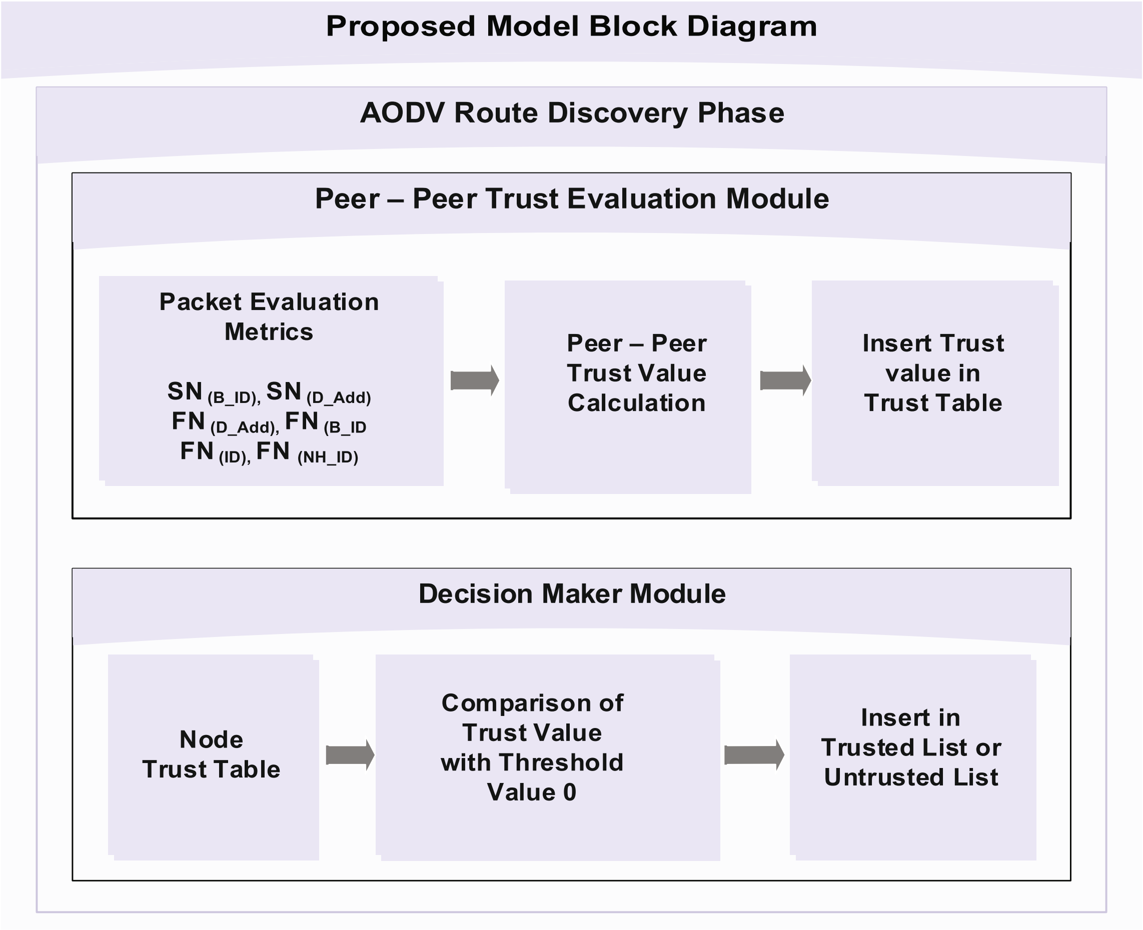

Proposed Model Block Diagram
AODV Route Discovery Phase
Peer – Peer Trust Evaluation Module
Packet Evaluation Metrics
SN (B_ID), SN (D_Add)
FN (D_Add), FN (B_ID
FN (ID), FN (NH_ID)
Peer – Peer Trust Value Calculation
Insert Trust value in Trust Table
Decision Maker Module
Node Trust Table
Comparison of Trust Value with Threshold Value 0
Insert in Trusted List or Untrusted List

FIGURE 2 Block diagram of proposed mechanism (trust-oriented peered customized mechanism)

3.1 | Design of proposed mechanism (TOPCM)

In this section, discussions are made on design of proposed TOPCM. The TOPCM consists of two modules. The first module is Peer-to-Peer trust evaluation module and second module is Decision-maker module. TOPCM perform malicious nodes identification and isolation by evaluating their trustworthiness level to enhance packet delivery rate. The design of proposed methodology is demonstrated in abstract form by using block diagram as shown in Figure 2.

In Peer-to-Peer Trust Evaluation module, during the route discovery phase trust value of the participated node has been calculated. This module contained subcomponents that perform trust evaluation. Packet evaluation metrics ($FN_{(D\_Add)}$, $FN_{(B\_ID)}$, $FN_{(ID)}$, $FN_{(NH\_ID)}$) are extracted by R(RREQ) packet and these evaluation metrics are employed to evaluate the behavior of nodes. On the basis of their behavior, the trust value of nodes is calculated by increment and decrement in their trust value and store in trust table.

Decision-maker module is responsible to label node as Trusted or Untrusted node. When the trust evaluation process has been completed, then decision-maker module performs identification and isolation of malicious node. In this module, calculated node trust values are used as input and compared with threshold trust value to make classification of participated node as trusted node or malicious node. If node trust value is less than or equal to threshold trust value, then that node is declared as malicious and inserted in malicious list else node is labeled as trustworthy as only trustworthy nodes should be a part of dynamic network for reliable data transmission.

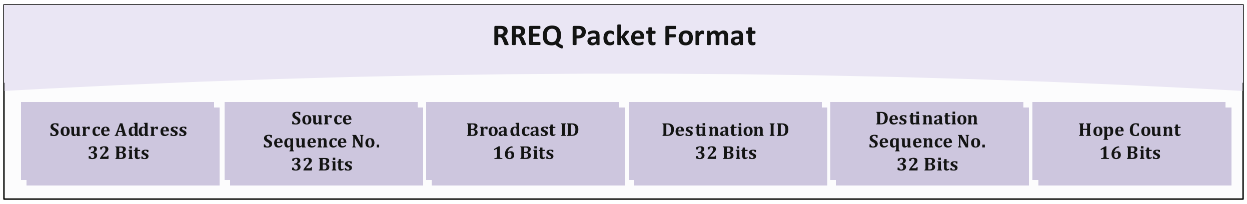
3.2 | Running procedure of proposed mechanism

Before actual data transmission, source node initiates route discovery process, establishes a route toward destination, and broadcasts RREQ to its neighbor or entire the network. Nodes update their information in its table after receiving the RREQ packet from the source node. If node is either destination or may have route towards destination with high sequence number, then it unicasts RREP toward particular requested RREQ node, otherwise RREQ will be broadcasted. When RREQ request has been already processed by each node then it is discarded by that node and does not broadcast. As soon as RREP propagates back to the source, nodes set up forward pointers to the destination. Whenever source node receives RREP packet it can perform data transmission.

Source node selects the route with most recent sequence number and minimum number of hop count and updates the route information for that destination to start transmission. First data transmission node verifies route toward desired destination whether is available or not in its routing table. If route exists then it performs data transmission otherwise it broadcasts RREQ entire the network to initiate route discovery.[3] The conventional format of RREQ packet has shown in Figure 3.

Source Address, Broadcast ID and Destination Sequence number should be same throughout route discovery process. Source Sequence number, Destination Sequence number, Hope Count, Next Hop ID, and Current node ID may have some changes mention as additional information in Figure 6. Each node knows about its next and previous hop information.[3] RREQ and RREP packets can be modified to meet logical requirements. The conventional format of RREP packet is shown in Figure 4.

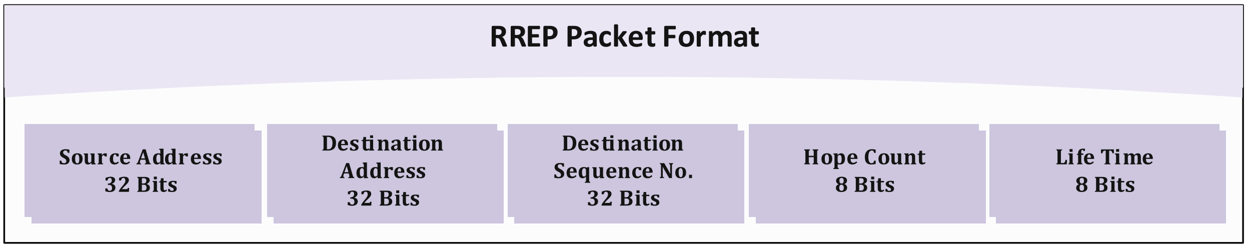
TOPCM introduced innovative technique to identify the malicious nodes and isolation them during the route discovery process. In TOPCM, each node is responsible to evaluate the trust level of its neighbor nodes by monitoring R(RREQ) control packet information during route discovery phase. Whenever each node wants to establish a route to make data transmission securely, then during the route discovery phase trust evaluation of participated node is processed. Each node broadcasts RREQ packet to its neighbor node. Node that broadcasts RREQ packet is known as Sender node and



RREQ Packet Format

Source Address 32 Bits	Source Sequence No. 32 Bits	Broadcast ID 16 Bits	Destination ID 32 Bits	Destination Sequence No. 32 Bits	Hope Count 16 Bits

FIGURE 3 RREQ packet format



RREP Packet Format

Source Address 32 Bits	Destination Address 32 Bits	Destination Sequence No. 32 Bits	Hope Count 8 Bits	Life Time 8 Bits

FIGURE 4 RREP packet format

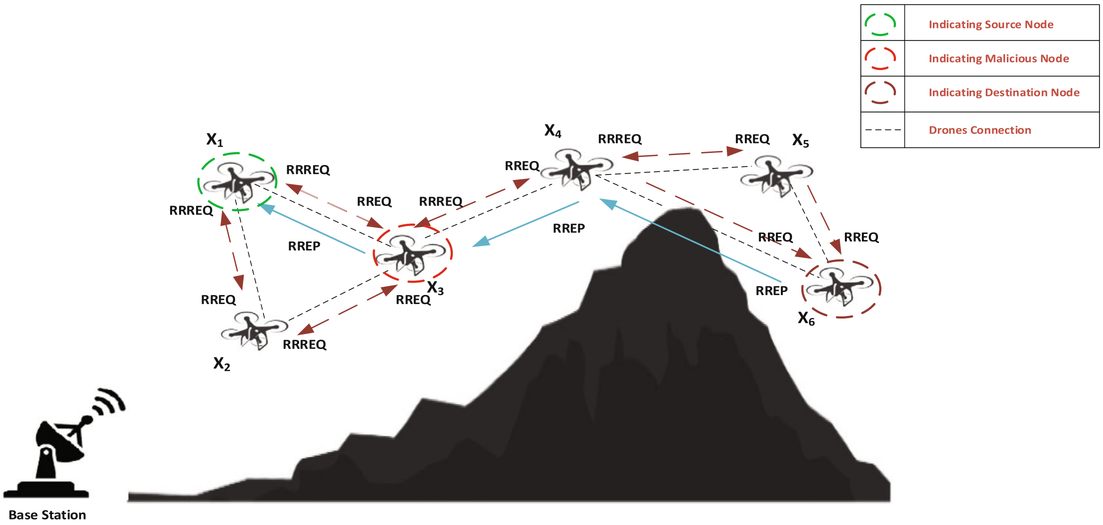
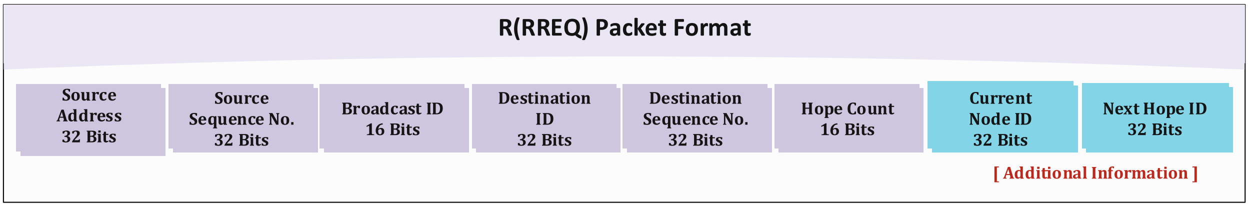


FIGURE 5 Proposed trust evaluation mechanism by using route discovery phase



R(RREQ) Packet Format

Source Address 32 Bits	Source Sequence No. 32 Bits	Broadcast ID 16 Bits	Destination ID 32 Bits	Destination Sequence No. 32 Bits	Hope Count 16 Bits	Current Node ID 32 Bits	Next Hope ID 32 Bits

[Additional Information]

FIGURE 6 R(RREQ) packet format

another node that reply back R(RREQ) to specific RREQ Requested node is called Forwarder node. As shown in Figure 5, a dynamic network where Node X_1 has two neighbors X_2 and X_3. When Node X_1 want to evaluate the trust value of its neighbor node during AODV route discovery phase, then node X_1 initiates route discovery process, firstly node X_1 broadcasts RREQ packets to its neighbor X_2 and X_3. Nodes X_2 and X_3 check their routing table whether it is destination or not. If yes, then it will unicast RREP to source otherwise they will broadcast RREQ packet to their neighbor nodes. According to our assumption, node replies R(RREQ) only to requested RREQ node. X_3 replies R(RREQ) only to X_1 with additional information as shown in Figure 6 (Next Hop ID and Current Node ID). Node X_1 extracts the desired information from R(RREQ) packets like Broadcast ID, Destination Address, Next Hop ID and Current Node ID. After extraction process, X_1 (Source node) considers these following parameter values to evaluate X_3 (Intermediate node) trust value.

- **Broadcast ID:** Node X_1 checks Broadcast ID, if X_1 RREQ broadcasts ID and R(RREQ) broadcasts ID sent by X_3 are similar then X_1 performs further processing on X_3 R(RREQ) parameters to calculate trust value, otherwise X_1 will make decrement and will process another node trust evaluation. Trust values are saved in evaluated node trust table.

- **Destination address:** To check further credibility, R(RREQ) Destination Address is looked as next parameter. If X_3 Destination Address meets with X_1 Destination Address without any modification, then further parameters are considered to evaluate X_3 trust level, otherwise X_1 will make decrement and will process another node trust evaluation.
- **Additional information:** The additional information of R(RREQ) as shown in Figure 6 is used to examine whether X_3's next hop position is in range or not and its adopted route is optimal or not by employing D_α, $D_ß$ calculation methods given in Equations (1) and (2).

All condition must be true to make increment or maintain the node trust level. If all these conditions are true and give indication toward evaluated node authenticity, then X_1 will make increment otherwise will make decrement in X_3 trust value. This process will be functional until node receives R(RREQ) packet by their neighbor nodes.

Decision-maker module is responsible in labeling node as Trusted or Untrusted node. When the trust evaluation process has been completed, then decision-maker module performed identification and isolation of malicious node. In this module, calculated node trust values are used as input and compared with threshold trust value to make identification and isolation of participated node. If node trust value is less than or equal to threshold trust value, then that node is declared as malicious and inserted in malicious zone or else node is labeled as trustworthy and only trustworthy nodes should be a part of dynamic network.

3.3 | Implementation of proposed mechanism (TOPCM)

In this section, the flow chart and algorithms of proposed solution are discussed in descriptive manner. The flowchart diagram of proposed mechanism is illustrated in Figure 7. As we mentioned in above Section 3.3, when each node performs route discovery process, it broadcasts RREQ and gets R(RREQ) packet in response from its neighbor nodes. In flow chart diagram and proposed algorithms, the trust value of nodes is calculated by using some evaluation metrics as input shown in Table 3 $SN_{(B\_ID)}$, $SN_{(D\_Add)}$, $FN_{(D\_Add)}$, $FN_{(B\_ID)}$, $FN_{(ID)}$, $FN_{(NH\_ID).}$ These evaluation metrics are extracted by R(RREQ) control packet.

Algorithm 1. Node trust evaluation

```
Input: $SN_{(B\_ID)}, SN_{(D\_Add)}, FN_{(D\_Add)}, FN_{(B\_ID)}, FN_{(ID)}, D_\alpha, D_ß$
Output: Trust Values
While until node receive RREP Packets
  If ($FN_{(B\_ID)} == SN_{(B\_ID)}$) then
    If ($FN_{(D\_Add)} != NULL$ & $FN_{(D\_Add)} == SN_{(D\_Add)}$) then
      If ($D_\alpha <= Range$ and $D_\alpha < D_ß$ and $FN_{[VD]}$) then
            $FN_{(ID)}.Trust_{++}$
      Else
            $FN_{(ID)}.Trust$--;
      End if
    Else
      $FN_{(ID)}.Trust$--;
    End if
  Else
    $FN_{(ID)}.Trust$--;
  End if
End while
```

In Algorithm 1, the trust value of nodes is calculated by performing the operations until RREP packet is received. Forwarder Node is compared with Broadcast ID with Sender Node Broadcast ID by employing this condition ($FN_{(B\_ID)==} SN_{(B\_ID)}$) to ensure that whether Forwarder node forward the same packet that is received from sender node. If true, then we move toward another condition ($FN_{(D\_Add)!=}$ *null and* $FN_{(D\_Add)==} SN_{(D\_Add)}$) to ensure that the destination of Forwarder node is similar to destination of sender node. If condition is true, then the distance from forwarder node to its

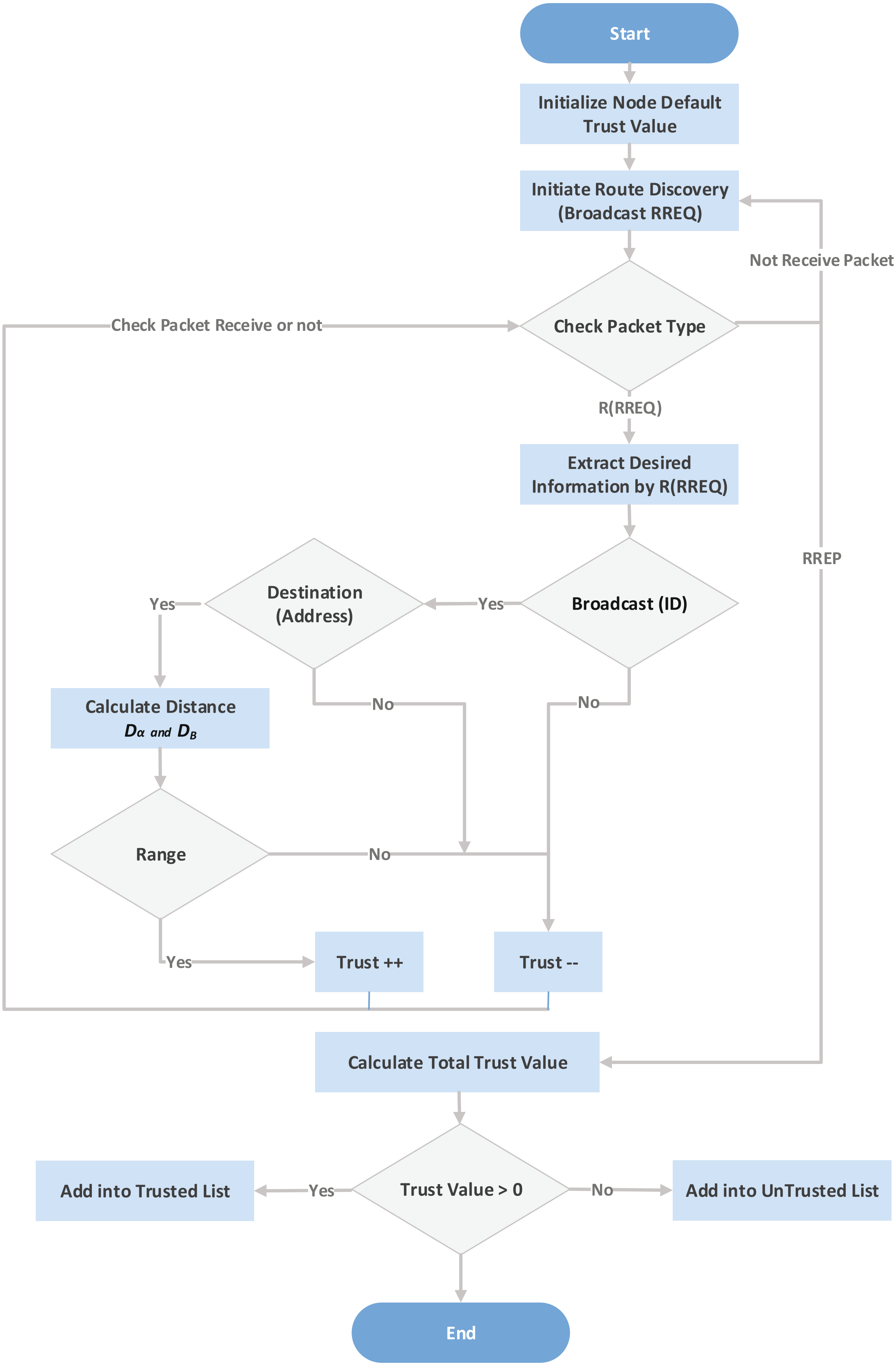

Start
Initialize Node Default Trust Value
Initiate Route Discovery (Broadcast RREQ)
Not Receive Packet
Check Packet Receive or not
Check Packet Type
R(RREQ)
Extract Desired Information by R(RREQ)
RREP
Destination (Address)
Yes
Broadcast (ID)
Yes
Calculate Distance D_α and D_B
No
No
Range
No
Yes
Trust ++
Trust --
Calculate Total Trust Value
Add into Trusted List
Yes
Trust Value > 0
No
Add into UnTrusted List
End

FIGURE 7 Proposed mechanism trust-oriented peered customized mechanism flow chart

TABLE 3 Simulation parameters in network simulator NS2

Input	Description
$SN_{(B\_ID)}$	Source node Broadcast ID
$SN_{(D\_Add)}$	Source node Destination Address
$FN_{(D\_Add)}$	Forward node Destination Address
$FN_{(B\_ID)}$	Forward node Broadcast ID
$FN_{(ID)}$	Forward node ID
$FN_{(NH\_ID)}$	Forward next hop ID
D_{α}	Distance between forward node and its next hop
$\mathrm{D}_{\text{ß}}$	Distance between forward node and destination node
VD	Velocity towards direction

next hop and from forwarder node to destination node is calculated by using Equations (1) and (2).

$$\mathrm{D}_{\alpha} = \text{Location } \left(FN_{(ID)}\right) - \text{Location } \left(FN_{(NH\_ID)}\right) \tag{1}$$

$$\mathrm{D}_{\text{ß}} = \text{Location } \left(FN_{(ID)}\right) - \text{Location } \left(DN_{(ID)}\right) \tag{2}$$

After that, another condition ($D_{\alpha} \leq Range\ and\ D_{\alpha} < D_{\text{ß}}\ and\ FN_{\ (VD)}$) is applied to check whether the next hop of forwarder node is in range or not as well as to ensure the direction of forwarder node is toward destination. The distance from forwarder node to next hop D_{α} is always less than from forwarder node to destination node $D_{\text{ß}}$. If this condition is true, then the forwarder node adopted accurate path and will make increment in trust value of nodes, else will perform decrement.

Algorithm 2. Malicious node detection and prevention

```
Input: Trust Value
Output: Trusted List and Untrusted List
Let $X = List\ of\ all\ nodes$
For all $x|x$ € $X$ do
    If ($x._{TV} > 0$) then
        Trusted_List.add (X)
    Else
        Untrusted_List.add (X)
End for
```

In Algorithm 2, when trust value of nodes has being calculated, then the calculated trust values are injected into decision-maker module to perform further processing. The calculated node trust values are compared in decision-maker module with threshold trust value and labeled node as malicious or trustworthy based on their trust values. If calculated trust value of node is less than or equal to threshold trust value, then that node declared as malicious and inserted in malicious list, else node is considered as trusted and inserted into trusted node list and only trusted nodes should be a part of future dynamic network for data transmission.

In terms of the computational complexity both algorithms have the complexity of n. The Algorithm 1 is evaluated against receiving of route reply (RREP) packet. The Algorithm 2 performs operations that are proportional to the size of node list. Both loops are executed n times and take linear time complexity that is $O(n)$. In order to make analysis and continuously check the behavior of control packets such as RREQ/RREP packets, the promiscuous mode need to be functional. In the proposed mechanism, the primary function of promiscuous mode is to analyze and monitor the control packet whenever each forwarder node broadcasts the packet to its neighbor nodes. During the computation of trust value of nodes, the promiscuous mode has a minute processing and energy overhead.

4 | SIMULATIONS AND RESULTS

In order to demonstrate the effectiveness of proposed TOPCM toward malicious nodes detection, we have employed Network Simulator NS2 with some predefined parameters as summarized in Table 4.[26] Initially 10 numbers of nodes are considered then gradually increase to 70 nodes.

Simulation work compared and analyzed the performance of proposed mechanism by employing variation in number of nodes and number of packets. Following performance evaluation parameters are considered in order to assess performance of proposed mechanism.

4.1 | Detection of malicious node

This evaluation metric demonstrates that how much the proposed mechanism is effective when compared to other conventional mechanisms in malicious node detection. The proposed mechanism (TOPCM) is compared with conventional mechanisms such as Malicious Node Removal in Route Identification Process (MNRiRIP**)** and Malicious Node Detection Algorithm (MNDA) method. Result analysis illustrates that proposed mechanism is much better for malicious nodes detection in qualitative and quantitative ways. Figure 8 shows how many number of malicious nodes present in a network

TABLE 4 Simulation parameters in network simulator NS2

Parameters	Values
Simulator	Network Simulator 2.35
Simulation duration	100 seconds
Data rate	1Mbps
Number of nodes	10-70
Number of packets	40,80 120 160 200 240 280 300
Data traffic type	TCP
Simulation area	800 m × 800 m
Packet format	CBR

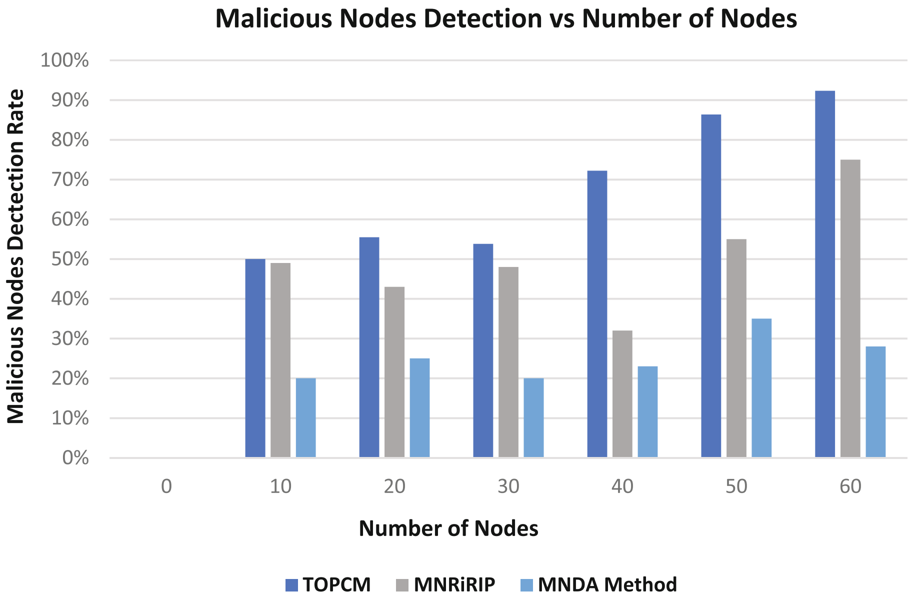


FIGURE 8 Malicious node detection vs nodes

and how much proposed mechanism (TOPCM) has successfully detected malicious nodes as compared to those of conventional mechanisms. Malicious node detection rates are expressed in term of percentage on left side of graph as shown in Figure 8.

4.2 | Packet delivery rate

Packet delivery rate by the proposed mechanism TOPCP is comparatively better than the conventional mechanism because of its accurate identification and isolation of malicious nodes. Packet delivery rates are analyzed in terms of number of nodes as shown in Figure 9. Packet delivery rate reflects reliability of network and shows numbers of packets that are received at destination node and numbers of packets that are dropped due to malicious node behavior. In short, Packet Drop Rate shows the number of packets that could not reach toward destination successfully.

In Figure 9, Packet Delivery Rate of proposed mechanism (TOPCM) is compared with traditional mechanisms like MNRiRIP and MNDA method. In the *x*-axis we have number of nodes that are gradually increasing by 10 and in *y*-axis Packet Delivery Rate expressed in terms of percentage. Results showed that, Packet Delivery Rate evaluated by the proposed mechanism is gradually improving due to accurate and effective isolation of malicious nodes. However, the functionality of proposed mechanism is much better than the other traditional mechanisms.

In Figure 10, Packet Dropping Rate is evaluated by proposed mechanism (TOPCM) and compared with MNRiRIP and MNDA traditional methods. Initially, the packet dropping rate is high due to presence of malicious node in the network but with the passage of time when malicious nodes are detected and isolated from network then, the packet dropping rate going to minimalize. It is very clear from Figure 10, the performance of proposed mechanism (TOPCM) is much better than other traditional mechanisms. In *y*-axis, packet dropping rate is expressed in terms of percentage and *x*-axis showed the number of nodes.

4.3 | Accuracy level

Accuracy level shows that how many malicious nodes are identified by proposed mechanism in accurate and authentic way among total number of malicious nodes present in the network. Accurate identification of malicious nodes has effects on packet delivery date and packet dropping rate as well as the trust level between participated nodes. In Figure 11, accuracy level of the proposed mechanism (TOPCM) meets toward desired expectation that is much better than the other

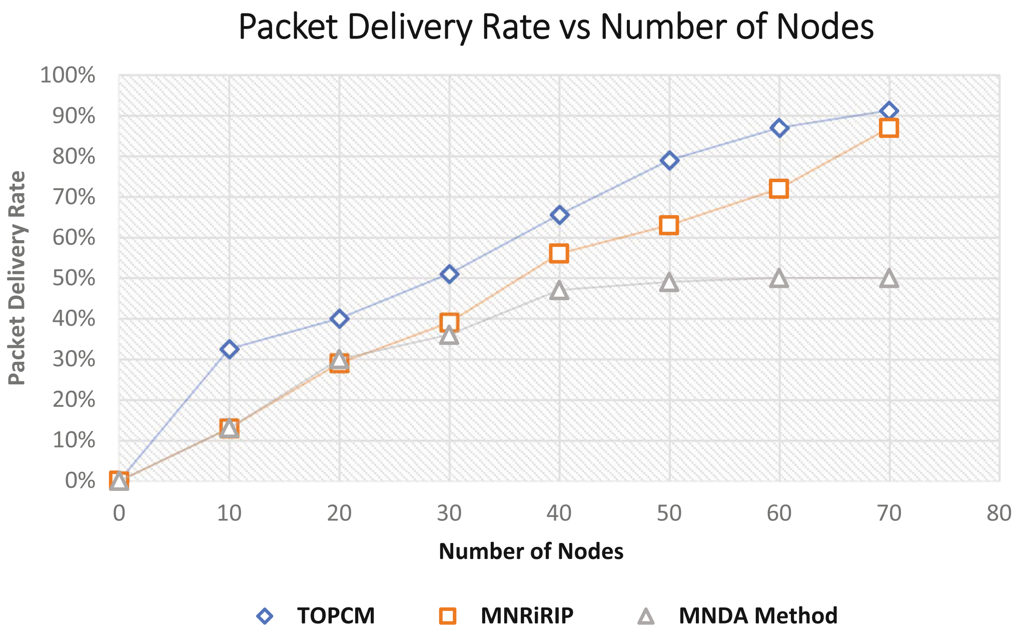


FIGURE 9 Packet delivery rate vs nodes

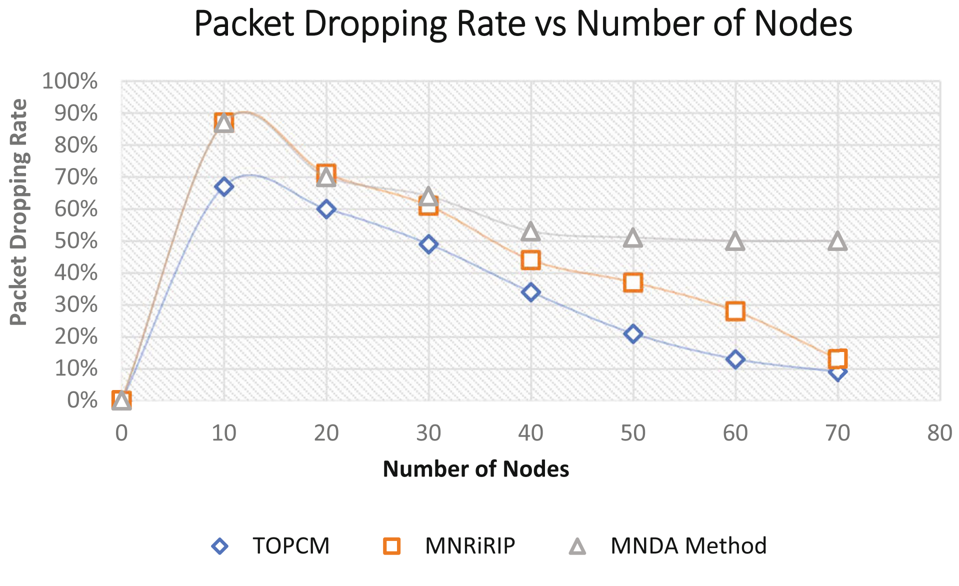


FIGURE 10 Packet dropping rate vs nodes

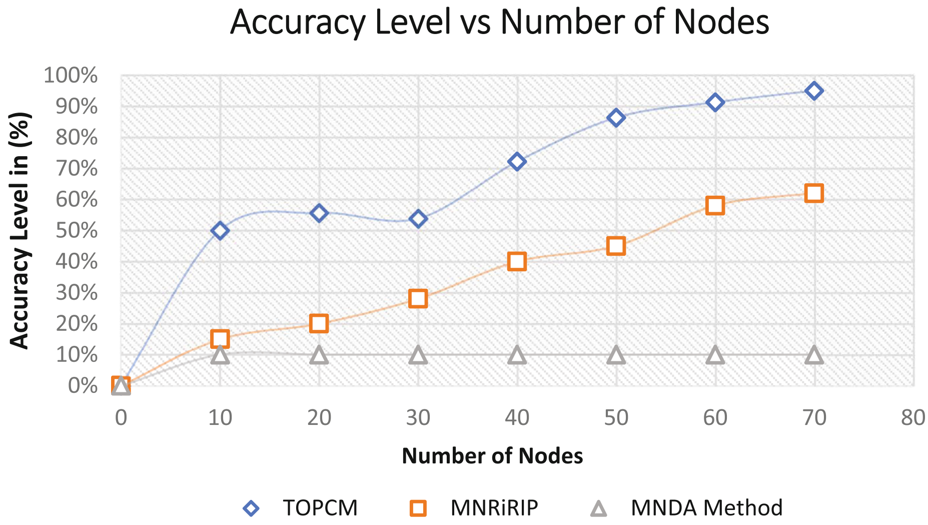


FIGURE 11 Accuracy level of malicious nodes detection

traditional mechanisms (MNRiRIP, MNDA method). The constant increment in accuracy level of proposed mechanism (TOPCM) is an indication that packet delivery rate increases and packet dropping rate reduces by accurate detection of malicious nodes.

4.4 | End-to-end delay

The presence of malicious nodes and false routing mechanism of used protocol promotes end-to-end delay in the network. Malicious nodes choose false routing and perform redirection or adopting nonoptimal route toward destination that cause network end-to-end delay. In this research paper, the proposed mechanism (TOPCM) minimized the end-to-end delay caused by accurately detecting the malicious nodes and isolating them from network. From Figure 12, results show that by adopting TOPCM, end-to-end delay will be minimized much better as compared to that of other traditional mechanisms (MNRiRIP and MNDA).

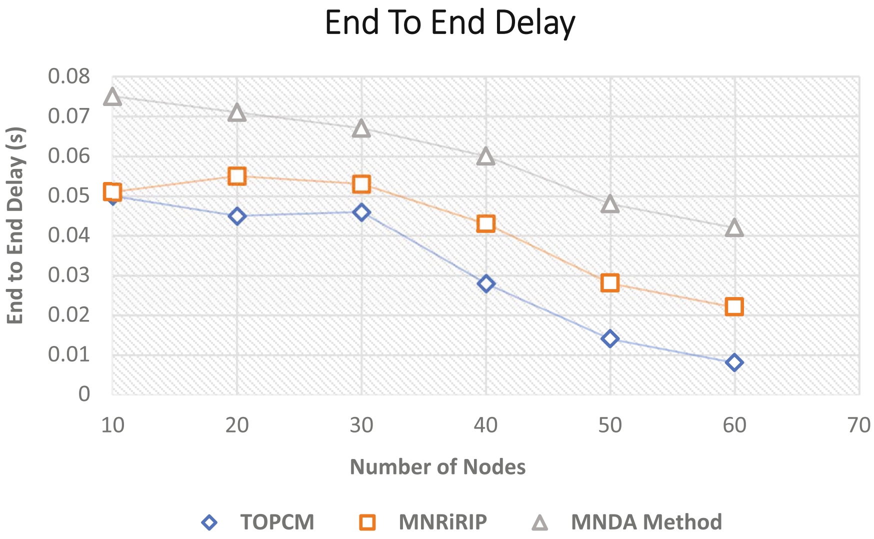


FIGURE 12 End-to-end delay

5 | CONCLUSION AND FUTURE WORK

In this research, it is concluded that presence of malicious nodes in dynamic network cause whole network performance degradation as well as harmful effect on reliability and credibility. We have demonstrated TOPCM to make identification and isolation of malicious nodes from network. The trustworthiness level of participated nodes is calculated by employing the desired information that exists in R(RREQ) packet. We have distributed evaluated nodes into malicious nodes or trustworthy nodes based on their calculated trust value. These malicious nodes are not considered in future route discovery phase or initial data transmission. Some effective simulations are performed in Network Simulator NS2 in order to validate the working of proposed mechanism and compare with other trust evaluation mechanisms as shown in Section 4. Experimental results showed that, our proposed mechanism (TOPCM) considered as a solid step toward dynamic network security enhancement by malicious node isolation and packet delivery enhancement. In addition, proposed mechanism (TOPCM) promotes packet delivery rate, credibility, and reliability by identification and isolation of malicious nodes. The malicious nodes are capable of degrading the network throughput and credibility by including false and malicious data. Securing the dynamic network from malicious nodes is a critical issue in infrastructureless environment and especially when the network is dynamic and mobile. In future, we will consider more attacks like byzantine attacks and information disclosure attacks by their difference behaviors to malicious nodes in the network. The proposed TOPCM mechanism will test with these types of attacks and improve security in the network.

ACKNOWLEDGEMENTS

This work has been funded by the “Ministerio de Ciencia e Innovación” through the Project PID2020-114467RR-C33 and by “Ministerio de Agricultura, Pesca y Alimentación” through the “proyectos de innovación de interés general por grupos operativos de la Asociación Europea para la Innovación en materia de productividad y sostenibilidad agrícolas (AEI-Agri)” ” project GO TECNOGAR.

CONFLICT OF INTEREST

Authors declare that they have no conflict of interest.

DATA AVAILABILITY STATEMENT

Data sharing not applicable to this article as no datasets were generated or analysed during the current study.

ORCID

Kashif Naseer Qureshi https://orcid.org/0000-0003-3045-8402
Jaime Lloret https://orcid.org/0000-0002-0862-0533

REFERENCES

1. Chriki A, Touati H, Snoussi H, Kamoun F. FANET: communication, mobility models and security issues. *Comput Netw*. 2019;163:106877.
2. Qureshi KN, Bashir F & Islam NU Link aware high data transmission approach for internet of vehicles. Paper presented at: Proceedings of the 2019 2nd International Conference on Computer Applications & Information Security (ICCAIS); Riyadh, Saudi Arabia 2019:1-5.
3. Agarkhed J. Study of security enhancement in AODV routing protocol in ad hoc networks. *Int J Comput Eng Technol*. 2017;8:99-106.
4. Qureshi KN, Din S, Jeon G, Piccialli F. Link quality and energy utilization based preferable next hop selection routing for wireless body area networks. *Comput Commun*. 2020;149:382-392.
5. Khan BUI, Olanrewaju RF, Habaebi MH. Malicious behaviour of node and its significant security techniques in MANET-A. *Austr J Basic Appl Sci*. 2013;7:286-293.
6. Cambra Baseca C, Sendra S, Lloret J, Tomas J. A smart decision system for digital farming. *Agronomy*. 2019;9:216.
7. Qureshi KN, Jeon G, Piccialli F. Anomaly detection and trust authority in artificial intelligence and cloud computing. *Comput Netw*. 2020;184:107647.
8. Cambra C, Díaz JR & Lloret J Deployment and performance study of an ad hoc network protocol for intelligent video sensing in precision agriculture. Paper presented at: Proceedings of the International Conference on Ad-Hoc Networks and Wireless; Benidorm, Spain, 2014:165-175.
9. Baseca CC, Díaz JR & Lloret J Communication ad hoc protocol for intelligent video sensing using AR drones. Paper presented at: Proceedings of the 2013 IEEE 9th International Conference on Mobile Ad-Hoc and Sensor Networks; Dalian, China; 2013:449-453.
10. Saini R, Khari M. Defining malicious behavior of a node and its defensive techniques in ad hoc networks. *Int J Smart Sens Ad Hoc Netw*. 2011;1:17-20.
11. Qureshi KN, Iftikhar A, Bhatti SN, Piccialli F, Giampaolo F, Jeon G. Trust management and evaluation for edge intelligence in the Internet of Things. *Eng Appl Artif Intel*. 2020;94:103756.
12. Zeng Y, Zhang R, Lim TJ. Wireless communications with unmanned aerial vehicles: opportunities and challenges. *IEEE Commun Mag*. 2016;54:36-42.
13. Hayat S, Yanmaz E, Muzaffar R. Survey on unmanned aerial vehicle networks for civil applications: a communications viewpoint. *IEEE Commun Surv Tutor*. 2016;18:2624-2661.
14. N. A. N. Hala Mustafa, εDetection of route discovery misbehaving nodes in AODV MANETs: a survey,ε *Int J Netw Commun*l. 4, pp. 155–122, 2018.
15. Bhoi SK, Jena KK, Jena A, Panda BC, Singh S & Behera P A reputation deterministic framework for true event detection in unmanned aerial vehicle network (UAVN). Paper presented at: Proceedings of the 2019 International Conference on Information Technology (ICIT); Bhubaneswar, India; 2019:257-262.
16. Valentin-Alexandru V, Ion B & Victor-Valeriu P Energy efficient trust-based security mechanism for wireless sensors and unmanned aerial vehicles. Paper presented at: Proceedings of the 2019 11th International Conference on Electronics, Computers and Artificial Intelligence (ECAI); Pitesti, Romania; 2019:1-6.
17. Ge C, Zhou L, Hancke GP, Su C. A provenance-aware distributed trust model for resilient unmanned aerial vehicle networks. *IEEE Internet Things J*. 2020;8(16):12481–12489.
18. Singh K & Verma AK A trust model for effective cooperation in flying ad hoc networks using genetic algorithm. Paper presented at: Proceedings of the 2018 International Conference on Communication and Signal Processing (ICCSP);Chennai, India; 2018:0491-0495.
19. Anwara RW, Zainala A, Outayb F, Yasarc A, Iqbald S. BTEM: belief based trust evaluation mechanism for wireless sensor networks. *Future Gener Comput Syst*. 2019;96:605-616.
20. Deepak Sharma AJ. Enhancement of security in flying AD-HOC network using a trust based routing mechanism. *Int J Innovat Technol Explor Eng*. 2019;9:1-5.
21. Singh K, Verma AK. FCTM: a novel fuzzy classification trust model for enhancing reliability in flying ad hoc networks (FANETs). *Ad Hoc Sens Wirel Netw*. 2018;40:23-47.
22. Singh K, Verma AK. A fuzzy-based trust model for flying ad hoc networks (FANETs). *Int J Commun Syst*. 2018;31:e3517.
23. Rajeswari A, Kulothungan K, Ganapathy S, Kannan A. A trusted fuzzy based stable and secure routing algorithm for effective communication in mobile adhoc networks. *Peer-to-Peer Netw Appl*. 2019;12:1076-1096.
24. Balaji S, Julie EG, Robinson YH, Kumar R, Thong PH. Design of a security-aware routing scheme in mobile ad-hoc network using repeated game model. *Comput Stand Interf*. 2019;66:103358.
25. Faraji M, Fotohi R. Secure communication between UAVs using a method based on smart agents in unmanned aerial vehicles; 2020.
26. Nikam S, Jadhav B. Delay analysis of DSDV protocol using NS 2.34. *Int J Comput Appl*. 2016;2:13-16.

How to cite this article: Buksh W, Guo Y, Iqbal S, Qureshi KN, Lloret J. Trust-oriented peered customized mechanism for malicious nodes isolation for flying ad hoc networks. *Trans Emerging Tel Tech*. 2022;e4489. doi: 10.1002/ett.4489