Trust Oriented Peered Customized Mechanism for Malicious Nodes Isolation for Flying Ad Hoc Networks

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

[1]School of Computer Science and Engineering, Central South University, Changsha, 410083, China

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

[3] Centre of Excellence of 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, Spain

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

Email: waqasbuksh156@gmail.com, yingguo@csu.edu.cn, saleem.iqbal@aiou.edu.pk, kashifnq@gmail.com, jlloret@dcom.upv.es

Abstract

Flying Ad-Hoc Networks (FANETs) gains the popularity due to its extra ordinary features in avionics and electronics domain. Flying Ad-Hoc Networks (FANETs) also consider most power full weapon in military assets as well as in civil security applications. Due to its infrastructure-less design and wireless nature network, some security challenges are overhead that should be overcome before the whole network performance degradation. Malicious nodes are capable to degrade the network throughput and credibility by inclusion false and malicious data. Secure the dynamic network from malicious nodes is a critical issue in infrastructure-less 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 trust value among flying ad-hoc nodes. In this research, we have 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. Obtaining simulated results showed that proposed Trust Oriented Peered Customized Mechanism (TOPCM) works more effectively and meets our desired expectation. The main contribution of this research is to establishment of trust among nodes that will be helpful to isolate the malicious nodes and make enhancement in packet delivery rate.

Keywords: - *Ad-Hoc Networks: FANETs: Malicious Node: Trust: Security: Network Simulator NS2*

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. Flying Ad-Hoc Networks (FANETs) are self-organized, self-configured and infrastructure-less network, inherited form of

Wireless Ad-Hoc Network (WANET) however one of the most valuable research direction towards Ad-hoc Networks [1, 2]. In FANETs, due to its wireless nature, infrastructure less design and frequently topology changes, many security issues and challenges are surrounding that play an important role to degrade 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 to perform data forwarding but they unable to do so [5, 6]**.** The concept of Flying Ad-Hoc Networks (FANETs) is demonstrated in Figure 1.

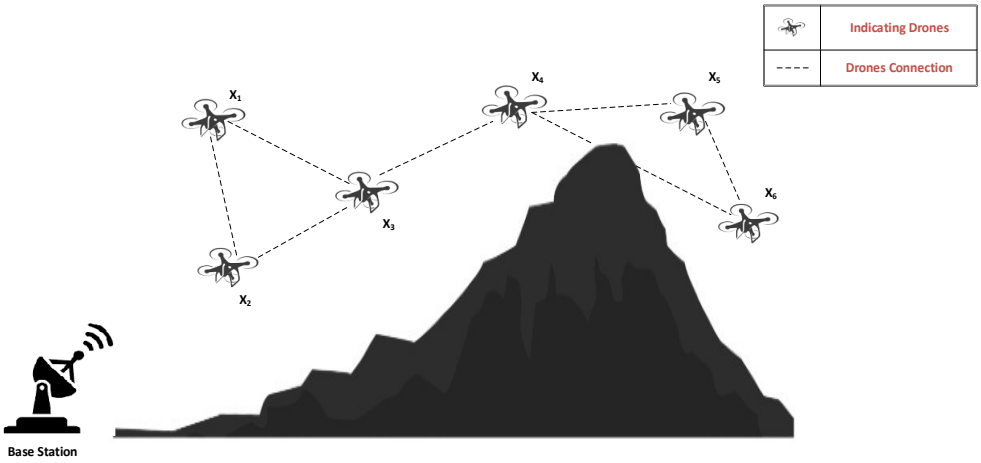

Figure: 1: Flying Ad-Hoc Networks with Drones and Base Station

Node independency to join or leave network without informing other nodes build a chance to apply malicious mechanism by eavesdropper. 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 highly movement of node involved 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 have introduced itself path [8, 9]. In Wireless Ad-Hoc dynamic networks, malicious node may be a part of network by eavesdropper to disturb the communication. Packets dropping rate and frequently modification performed give indication towards malicious node presence in a network. If a network compromised by limited resource constraint (battery drain, power and bandwidth consumption) then there is a possibility that participated nodes acting as a malicious node and performing misbehaving activities. When a packet not reached to desired destination then there is a chance of malicious node [10, 11].

The prime contributions of this paper are follows as:

- Introduction of state-of-the-art trust-oriented mechanism and stimulate the research flow towards ad-hoc networks (FANETs).
- Perform identification and isolation of malicious nodes from dynamic network by the establishment of 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 UAVs in the domain of military is witnessed in different forms for the last two decades for surveillance of border areas and monitoring the sensitive surfaces [12]. The FANETs have also some commercial applications like in search and rescue operations, the where the response time is very critical. In order to search and recognize the target, FANETs perform in efficient manners and facilitate the rescue team towards reaching the target [13]. Table 1 shows the commercial applications of FANETs.

Table 1: Commercial Applications of FANETs

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 UAVs
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 vise coverage like mapping and border monitoring or surveillance. The size of area can be increase or decrease according to mission requirements. The next one commercial use of FANET is construction missions where UAVs are used to perform construction by lifting the building elements. The swarm of UAVs is organizing the elements of building elements and place at their specific position. In order to accomplish this mission properly, the timing and synchronization between the UAVs collaboration should be ensure by communication architecture. In this category, delivery and transportation mission, the UAVs are employing to provide transportation services and delivery of good 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 content explained 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 content demonstrated the detailed working and implementation of proposed Trust Oriented Peered Customized Mechanism (TOPCM). Finally, Section 4 presented simulation details and results comparison of proposed mechanism. Section 5 followed by 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 cause network throughput degradation as well as downsize the network reliability by inclusion 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 isolate 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 term 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 are mentioned that have been used to evaluate the trust value of neighbor node or forwarder node in direct and hybrid way as well as perform 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 made based observational evidence to identify and prevent malicious node [17]. In this research paper author established a trust evaluation mechanism by calculating 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 considering traffic profile information's 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 detect and isolate the malicious node [19]. Author

defined a mechanism based on trace file (TCL) to calculate the trust value of node present in the network. Trace file (TCL) contain all the detailed information related to traffic flow. Trace file (TCL) traffic flow information 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 achieve 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 employ 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, detect black hole attacks and design a defensive mechanism [25]. Table 2 shows the comparison with technical details.

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)	Trace File 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

The Table 2 represents a comparison of state of art FANET based approaches that are applicable in identification of malicious nodes. Different characteristics and 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 cause significant processing overhead while performing direct and indirect trust calculation. In addition, due to dependency of another node or recommender node, while getting the recommendation about other nodes, the trust value of nodes may compromise. Because when the recommender node is not trustworthy then its recommendation can also be unrealistic and non-trustworthy. In some of the approaches, only static nodes are considered and employed. These approaches are not completely functional with independent nodes and promote third party recommendation that may cause significant processing and degrade 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 trace files 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 is needed to establish, that properly identify the malicious nodes and isolate them to make network more reliable.

3. Proposed Work

To increase the FANETs trustworthiness, this research proposes Trust Oriented Peered Customized Mechanism (TOPCM). The TOPCM express 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, elaborated in this section. Simulation results authenticated that our proposed mechanism is qualitative better and meets towards our expected requirements. Here some assumptions that have been followed throughout the simulation environment. These assumptions considered as 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 are assigned by default trust value to make trust establishment. After that, perform peer to peer node trust evaluation by employing some worth-full parameters ($FN_{(D\_Add)}$, $FN_{(B\_ID)}$, $FN_{(ID)}$, $FN_{(NH\_ID)}$) to perform trustworthy decision. Decision maker module is responsible to distribute the nodes in malicious or trustworthy list.

3.1. Design of Proposed Mechanism (TOPCM)

In this section, made discussions are made on design of proposed Trust Oriented Peered Customized Mechanism (TOPCM). The proposed mechanism TOPCM consists of two modules. The first module is Peer to Peer trust evaluation module and second module labeled as 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 sub components 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 base of their behavior, the trust value of nodes is calculated by increment and decrement in their trust value and store in trust table.

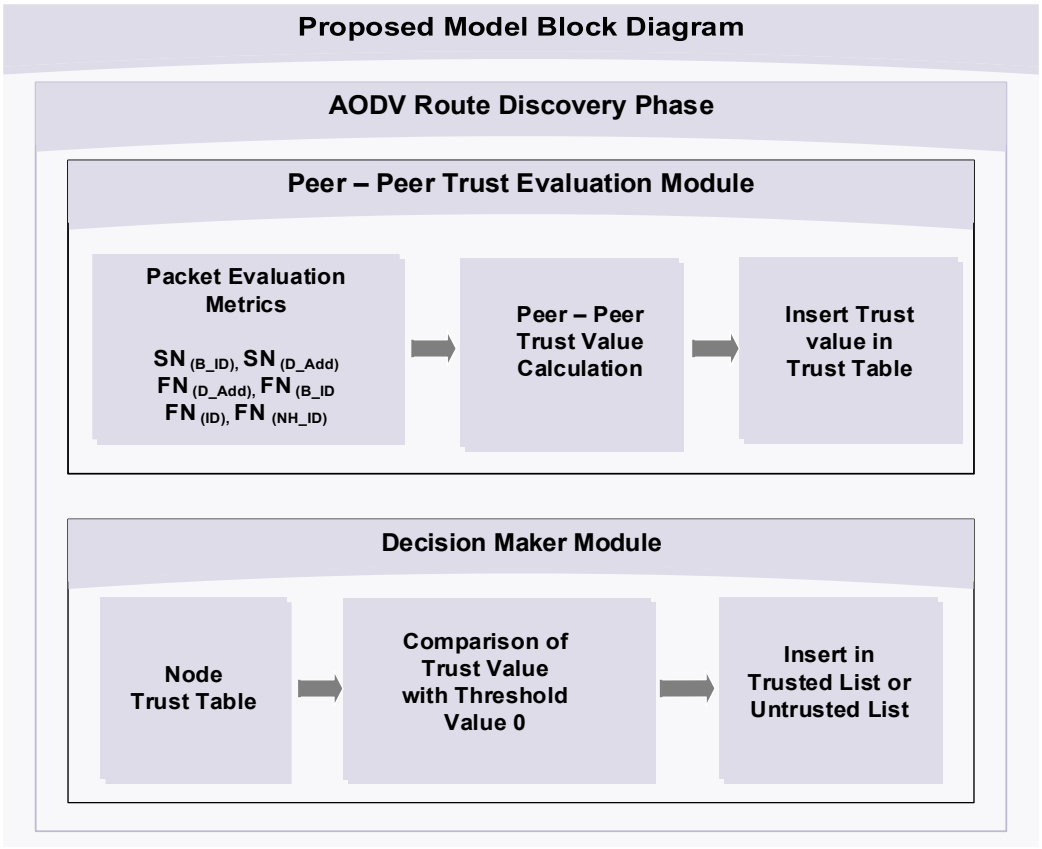

Figure 2: Block Diagram of Proposed Mechanism TOPCM

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 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 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 declared as malicious and insert in malicious list else node labeled as trustworthy and only trustworthy nodes should be a part of dynamic network for reliable data transmission.

3.2. Running Procedure of Proposed Mechanism (TOPCM)

Before actual data transmission, Source node initiate route discovery process and establish a route towards destination then it broadcast RREQ to its neighbor or entire the network. Nodes update their information in its table after receiving the RREQ packet from source node. If node is either destination or may have route towards destination with high sequence number, then it unicast RREP towards particular requested RREQ node otherwise RREQ will be broadcasted. When RREQ request already processed by each node then it discarded by that node and do 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 select the route with most recent sequence number and minimum number of hop count and update the route information for that destination to start transmission. Before Data transmission node verify route towards desired destination is available or not in its routing table. If route exist then, it perform data transmission otherwise it broadcast RREQ entire the network to initiate route discovery [3]. The conventional format of RREQ packet has shown in Figure 3.

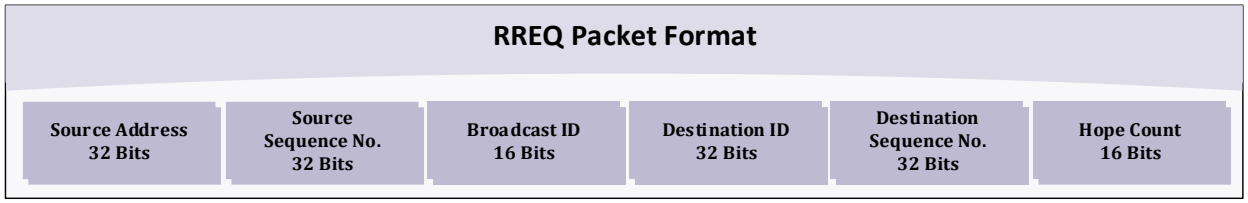

Figure 3: RREQ Packet Format

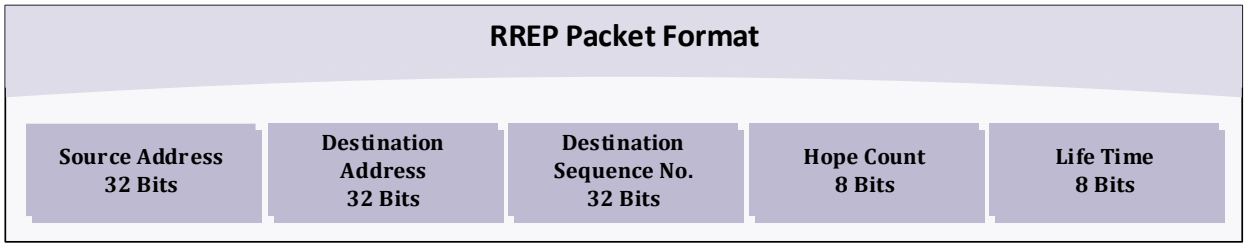

Figure 4: RREP Packet Format

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 has shown in Figure 4.

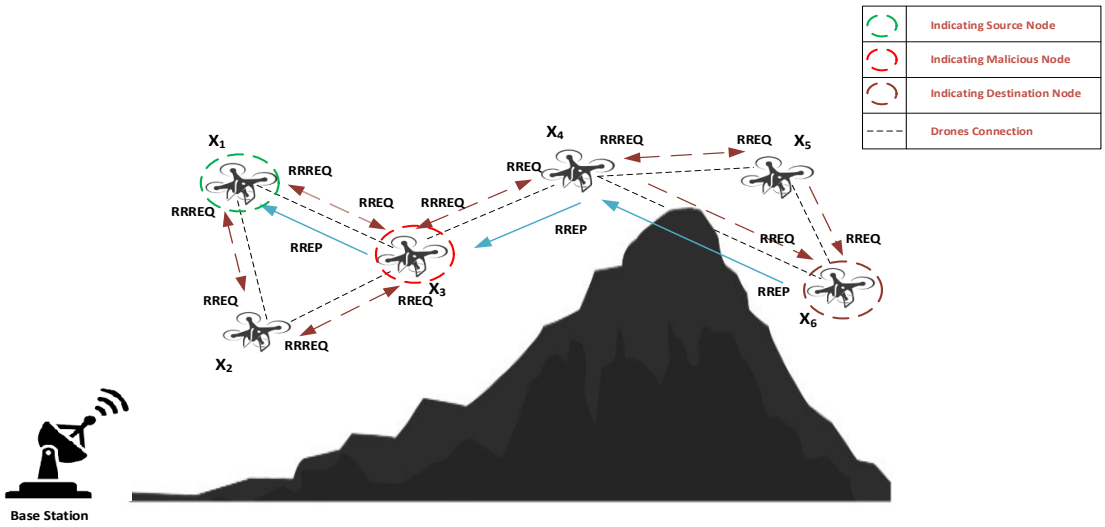

Figure 5: Proposed Trust Evaluation Mechanism by using Route Discovery Phase

TOPCM introduced innovative technique to identify the malicious nodes and isolation them during the route discovery process. In Trust-Oriented Peered Customized Mechanism (TOPCM), each node is responsible to evaluate the trust level of its neighbor nodes by monitoring R(RREQ) control packet information's 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 broadcast RREQ packet to its neighbor node. Node that broadcast RREQ packet known as Sender node and another node that reply back R(RREQ) to specific RREQ Requested node 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 initiate route discovery process, firstly node X_1 broadcast RREQ packets to its neighbor X_2 and X_3. Node X_2 and X_3 check their routing table either is it 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 reply R(RREQ) only to X_1 with additional information as mentioned in Figure 6 (Next Hop ID and Current Node ID). Node X_1 extract 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) consider these following parameter values to evaluate X_3 (Intermediate node) trust value.

- **Broadcast ID:** Node X_1 check Broadcast ID, if X_1 RREQ broadcast id and R(RREQ) broadcast id sent by X_3 are similar then X_1 perform further processing on X_3 R(RREQ)

parameters to calculate trust value otherwise X_1 make decrement and process another node trust evaluation. Trust values are saved in evaluated node trust table.

- **Destination Address:** To check further credibility, R(RREQ) Destination Address looked as next parameter. If X_3 Destination Address meets with X_1 Destination Address without any modification, then further parameters considered to evaluate X_3 trust level otherwise X_1 make decrement and process another node trust evaluation.
- **Additional Information:** The additional information of R(RREQ) as shown in Figure 6 used to examine X_3 next hope position whether is it in range or not and adopted route is optimal or not by employing Dα, Dß calculation methods given in equation (I & II).

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

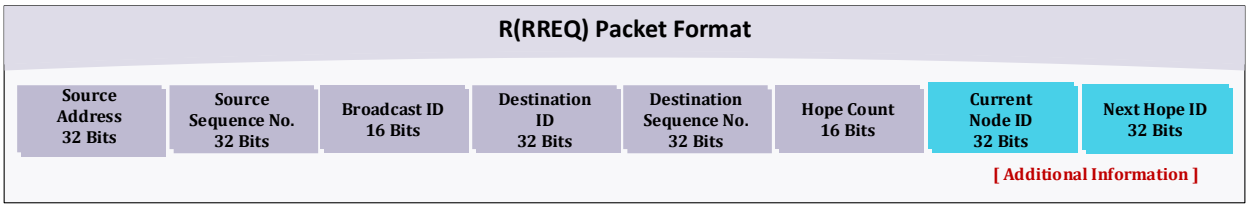

Figure 6: R(RREQ) Packet Format

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 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 less than or equal to threshold trust value, then that node declared as malicious and insert in malicious zone else node 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 is discussed in descriptive manners. 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 broadcast RREQ and get 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.

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 b/w Forward Node and its Nsext Hop
$D_{ß}$	Distance b/w Forward Node and Destination Node
VD	Velocity Towards Direction

Table 3: Simulation Parameters in Network Simulator NS2

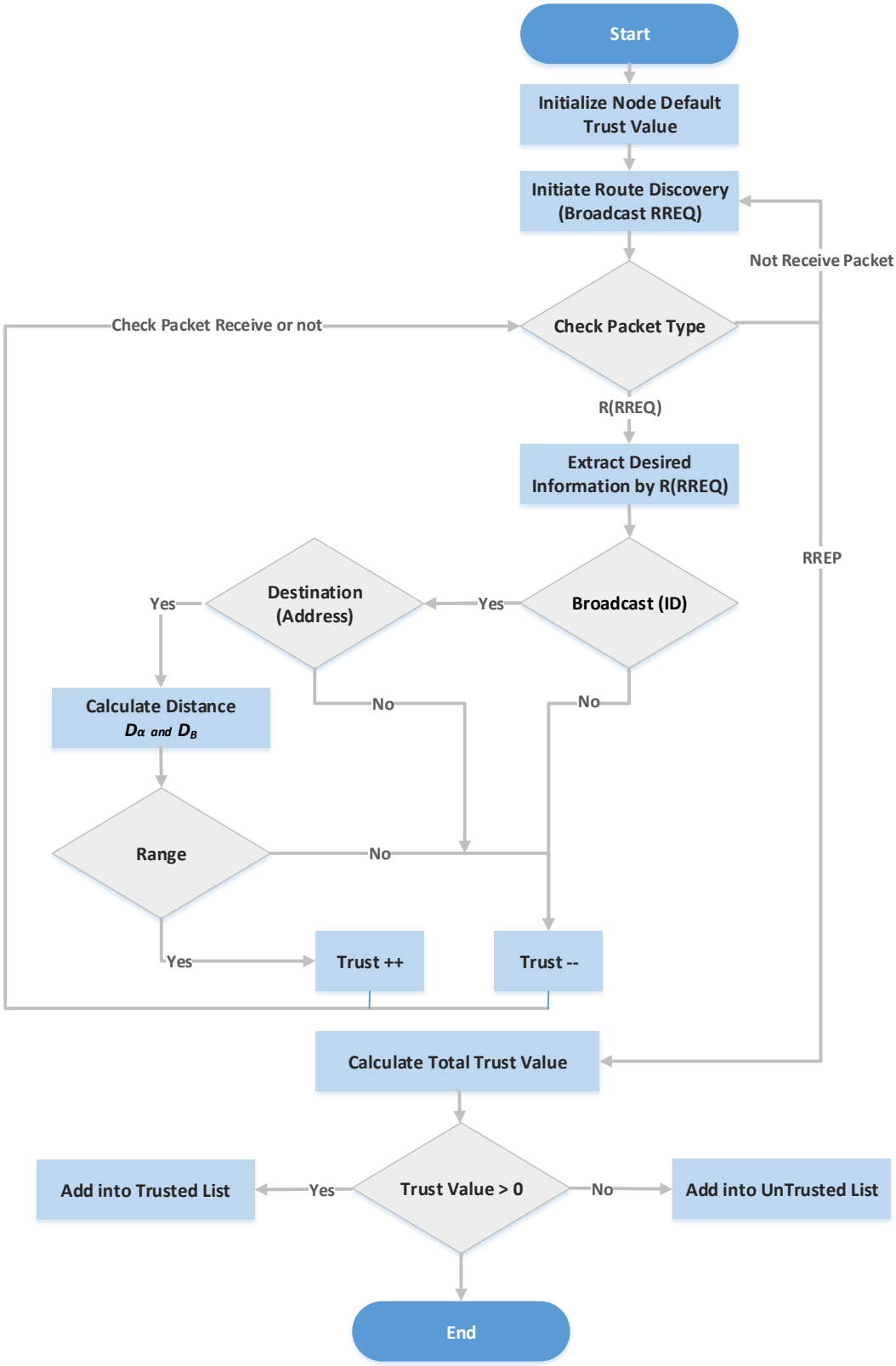

Figure 7: Proposed Mechanism TOPCM Flow Chart

ALGORITHM 1: NODE TRUST EVALUATION

```
    Input: SN(B_ID), SN(D_Add), FN(D_Add), FN(B_ID), FN(ID), Dα, Dβ
    Output: Trust Values
1   While until node receive RREP Packets
2     If (FN(B_ID) == SN(B_ID)) then
3         If (FN(D_Add) ! = NULL & FN(D_Add) == SN(D_Add)) then
4             If (Dα<= Range and Dα < Dβ and FN(VD)) then
5                 FN(ID).Trust++
6             Else
7                 FN(ID).Trust--;
8             End if
9         Else
10            FN(ID).Trust--;
11        End if
12    Else
13        FN(ID).Trust--;
14    End if
15  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 $(FN_{(D\_Add)} ! = null \text{ and } FN_{(D\_Add)} == SN_{(D\_Add)})$ to ensure that the destination of Forwarder node is similar to destination of sender node. If condition is true, then calculate the distance from forwarder node to its next hop and from forwarder node to destination node by using equation I and II.

I. $\mathbf{D_\alpha = Location\ (FN_{(ID)}) - Location\ (FN_{(NH\_ID)})}$

II. $\mathbf{D_\beta = Location\ (FN_{(ID)}) - Location\ (DN_{(ID)})}$

After that, apply another condition $(D_\alpha <= Range \text{ and } D_\alpha < D_\beta \text{ and } FN_{(VD)})$ to check the Next Hop of Forwarder node is in range or not as well as ensure the direction of forwarder node towards destination. The distance from Forwarder Node to Next Hop D_α is always less than from Forwarder Node to destination node D_β. If this condition is true, then the Forwarder node adopted accurate path and make increment in trust value of nodes else perform decrement.

ALGORITHM 2: MALICIOUS NODE DETECTION AND PREVENTION

```
    Input: Trust Value
    Output: Trusted List and Untrusted List
1   Let X = List of all nodes
2   For all x|x € X do
3       If (x.TV > 0)  then
4           Trusted_List.add (X)
5       Else
6           Untrusted_List.add (X)
7   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 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 insert in malicious list else node considered as trusted and insert 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, perform 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 analyzes and monitor the control packet whenever each forwarder node broadcast 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 Trust Oriented Peered Customized Mechanism (TOPCM) towards malicious nodes detection, we have employed Network Simulator NS-2 with some pre-defined parameters as summarized in below Table 4 [26]. Initially 10 numbers of nodes are considered then gradually increase to 70 nodes.

Parameters	Values
Simulator	Network Simulator 2.35
Simulation Duration	100 s
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	800m X 800m
Packet Format	CBR

Table 4: Simulation Parameters in Network Simulator NS2

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.

Detection of Malicious Node: This evaluation metric demonstrates that how much proposed mechanism is effective as compared to other conventional mechanisms in malicious node detection. The proposed mechanism **TOPCM** is compared with conventional mechanisms Malicious Node Removal in Route Identification Process (**MNRiRIP)** and Malicious Node Detection Algorithm **MNDA** Method. Results analysis illustrate that proposed mechanism is

much better for malicious nodes detection in qualitative and quantitative way. In Figure 8, it showed how many numbers of malicious nodes present in network and how much proposed mechanism (TOPCM) detected malicious nodes successfully as compared to conventional mechanisms. Malicious node detection rates are expressed in term of percentage on left side of graph as shown in Figure 8.

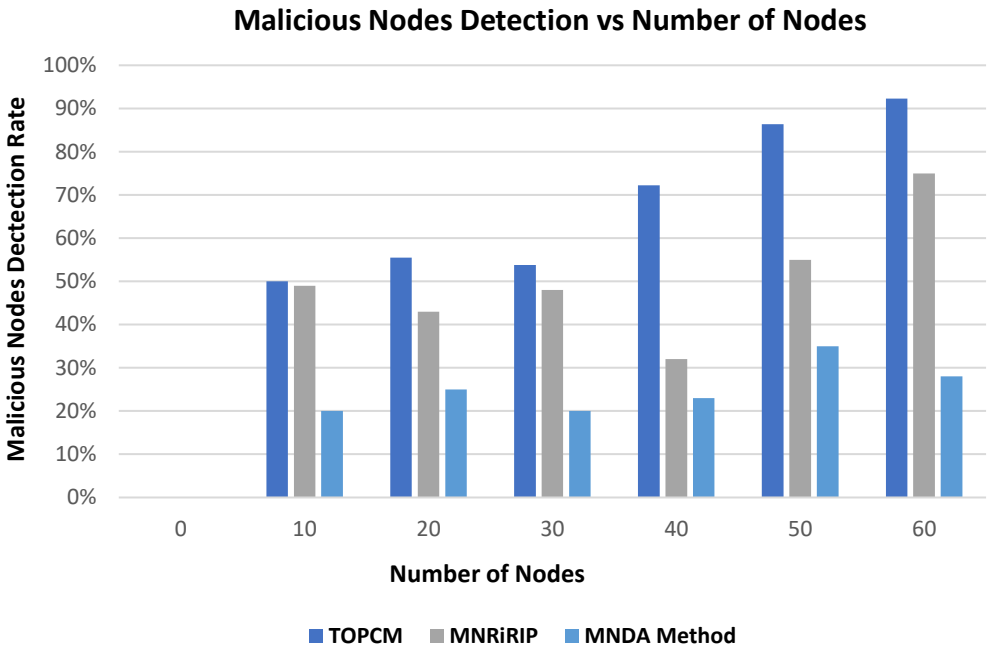

Figure 8: Malicious Node Detection vs Nodes

Packet Delivery Rate: Packet delivery rate by the proposed mechanism TOPCP comparatively better than conventional mechanism due to accurately identification and isolation of malicious nodes. Packet delivery rates are analyzed in term of number of nodes as shown in Figure 9**.** Packet delivery rate reflect reliability of network. Packet delivery rate shows numbers of packets are received at destination node and numbers of packets are dropped due to malicious node behavior. In short, Packet Drop Rate shows that numbers of packets that couldn't reach towards destination successfully.

In Figure 9, Packet Delivery Rate of proposed mechanism (TOPCM) is compared with traditional mechanisms like Malicious Node Removal in Route Identification Process (MNRiRIP) and Malicious Node Detection Algorithm (MNDA) methods. In the X-axis we have number of nodes that are gradually increase by 10 and in Y axis presenting Packet Delivery Rate expressed in term of percentage. Results showed that, Packet Delivery Rate evaluated by the proposed mechanism is gradually improved due to accurate and effective isolation of malicious nodes. However, the functionality of proposed mechanism is much better than other traditional mechanisms.

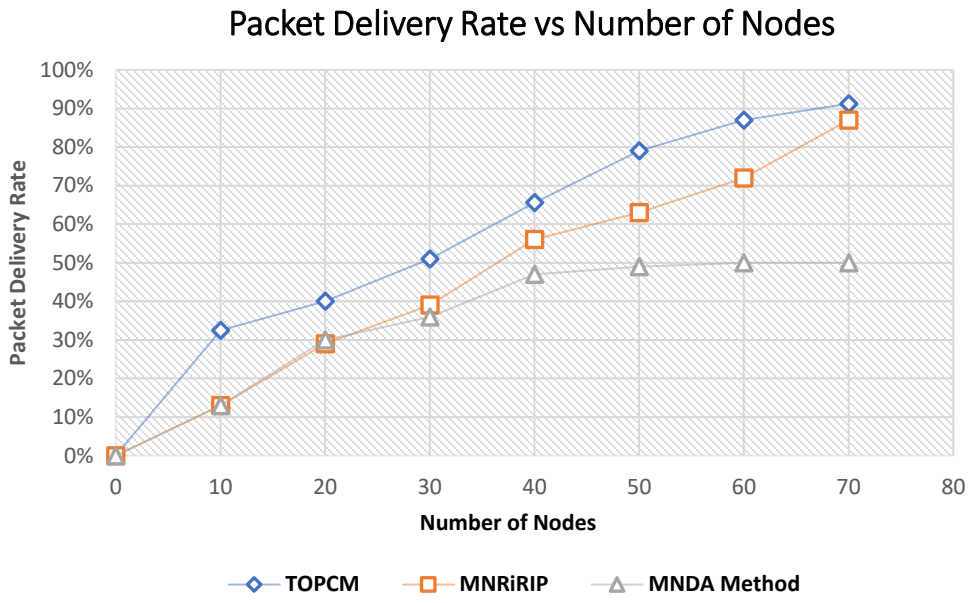

Figure 9: Packet Delivery Rate vs Nodes

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's 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 term of percentage and x-axis showed the number of nodes.

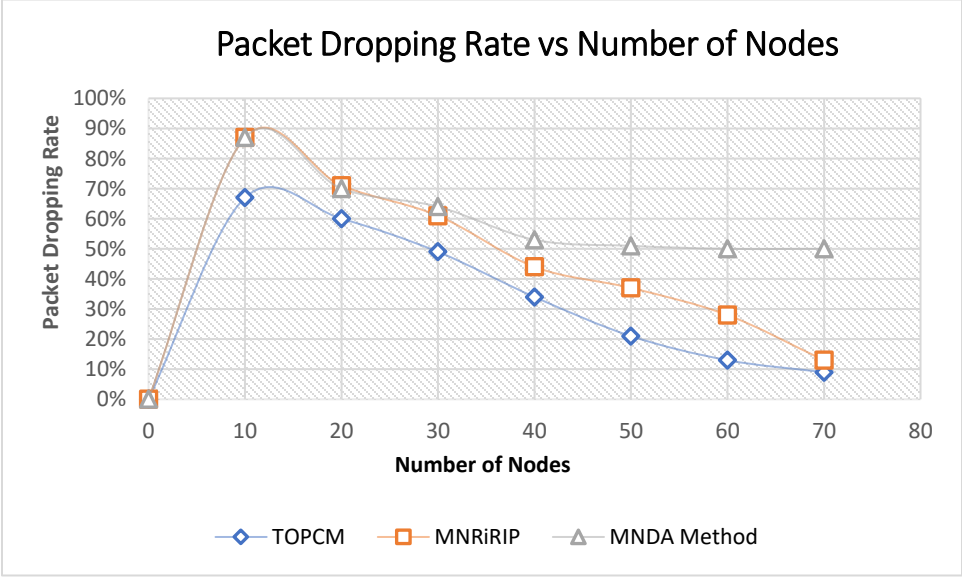

Figure 10: Packet Dropping Rate vs Nodes

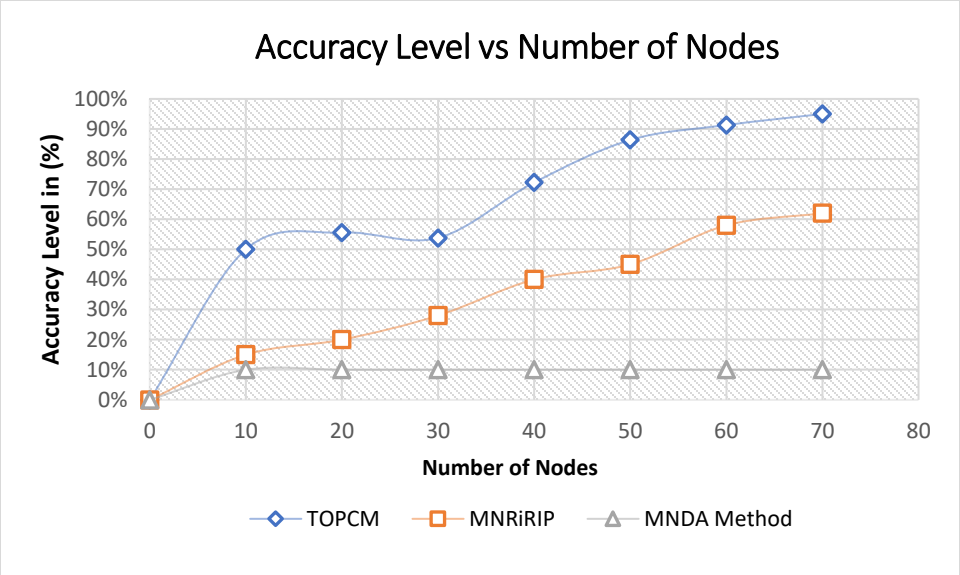

Figure 11: Accuracy Level of Malicious Nodes Detection

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 effects on packet delivery date and packet dropping rate as well as trust level between participated nodes. In Figure 11, accuracy level of proposed mechanism (TOPCM) meeting towards desired expectation that is much better than other traditional mechanisms (Malicious Node Removal in Route Identification Process MNRiRIP, Malicious Node Detection Algorithm MNDA Method). The constantly increment in accuracy level of proposed mechanism (TOPCM) is an indication that packet delivery rate increase and packet dropping rate reduce by accurate detection of malicious nodes.

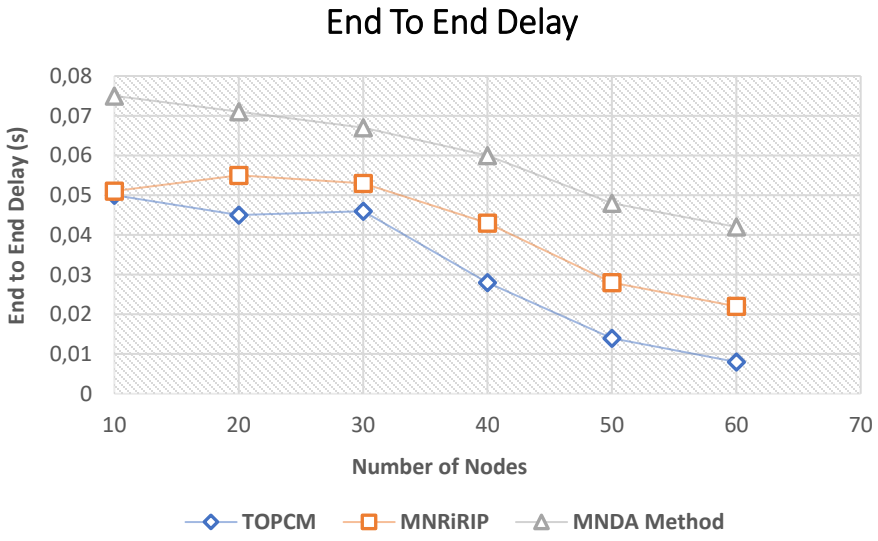

Figure 12: End-to-End Delay

End-to-End Delay: The presence of malicious nodes and false routing mechanism of used protocol promote end-to-end delay in the network. Malicious nodes choose false routing and perform redirection or adopting non optimal route towards destination that cause network end to end delay. In this research paper, proposed mechanism (TOPCM) minimized the end-to-end delay causes by accurately detecting the malicious nodes and isolating them from network. In Figure 12, results showed that by adopting (TOPCM) end-to-end delay minimized much better as compared to other traditional mechanisms (Malicious Node Removal in Route Identification Process MNRiRIP, Malicious Node Detection Algorithm MNDA).

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 Trust Oriented Peered Customized Mechanism (TOPCM), to make identification and isolation of malicious nodes from network. The trustworthiness level of participated nodes is calculated by employing the desired information's 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 towards 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 to degrade the network throughput and credibility by inclusion false and malicious data. Secure the dynamic network from malicious nodes is a critical issue in infrastructure-less 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 "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)" in the framework "Programa Nacional de Desarrollo Rural 2014-2020", for the grant GO TECNOGAR, in cofuding EU 80% by the "Fondo Europeo Agrícola de de Desarrollo Rural-FEADER" and 20% by the "Ministerio de Agricultura, Pesca y Alimentación" with a total fund of 432.329,05 €. Being the "Dirección general de desarrollo Rural, innovación y Formación Agroalimentaria" (DGDRIFA) the national managing authority entrusted with the application of the FEADER grant.

References

[1] A. Chriki, H. Touati, H. Snoussi, and F. Kamoun, "FANET: Communication, mobility models and security issues," *Computer Networks,* vol. 163, p. 106877, 2019.

[2] K. N. Qureshi, F. Bashir, and N. U. Islam, "Link aware high data transmission approach for internet of vehicles," in *2019 2nd international conference on computer applications & information security (ICCAIS)*, 2019, pp. 1-5.

[3] J. Agarkhed, "Study of security enhancement in AODV routing protocol in ad hoc networks," *International Journal of Computer Engineering & Technology,* vol. 8, pp. 99-106, 2017.

[4] K. N. Qureshi, S. Din, G. Jeon, and F. Piccialli, "Link quality and energy utilization based preferable next hop selection routing for wireless body area networks," *Computer Communications,* vol. 149, pp. 382-392, 2020.

[5] B. U. I. Khan, R. F. Olanrewaju, and M. H. Habaebi, "Malicious Behaviour of Node and its Significant Security Techniques in MANET-A," *Australian Journal of Basic and Applied Sciences,* vol. 7, pp. 286-293, 2013.

[6] C. Cambra Baseca, S. Sendra, J. Lloret, and J. Tomas, "A smart decision system for digital farming," *Agronomy,* vol. 9, p. 216, 2019.

[7] K. N. Qureshi, G. Jeon, and F. Piccialli, "Anomaly Detection and Trust Authority in Artificial Intelligence and Cloud Computing," *Computer Networks,* p. 107647, 2020.

[8] C. Cambra, J. R. Díaz, and J. Lloret, "Deployment and performance study of an ad hoc network protocol for intelligent video sensing in precision agriculture," in *International Conference on Ad-Hoc Networks and Wireless*, 2014, pp. 165-175.

[9] C. C. Baseca, J. R. Díaz, and J. Lloret, "Communication Ad Hoc protocol for intelligent video sensing using AR drones," in *2013 IEEE 9th International Conference on Mobile Ad-hoc and Sensor Networks*, 2013, pp. 449-453.

[10] R. Saini and M. Khari, "Defining malicious behavior of a node and its defensive techniques in ad hoc networks," *International Journal of Smart Sensors and Ad Hoc Networks,* vol. 1, pp. 17-20, 2011.

[11] K. N. Qureshi, A. Iftikhar, S. N. Bhatti, F. Piccialli, F. Giampaolo, and G. Jeon, "Trust management and evaluation for edge intelligence in the Internet of Things," *Engineering Applications of Artificial Intelligence,* vol. 94, p. 103756, 2020.

[12] Y. Zeng, R. Zhang, and T. J. Lim, "Wireless communications with unmanned aerial vehicles: Opportunities and challenges," *IEEE Communications Magazine,* vol. 54, pp. 36-42, 2016.

[13] S. Hayat, E. Yanmaz, and R. Muzaffar, "Survey on unmanned aerial vehicle networks for civil applications: A communications viewpoint," *IEEE Communications Surveys & Tutorials,* vol. 18, pp. 2624-2661, 2016.

[14] N. A. N. Hala Mustafa, "Detection of Route Discovery Misbehaving Nodes in AODV MANETs: A Survey," *International Journal of Networks and Communications,* vol. 4, pp. 155-122, 2018.

[15] S. K. Bhoi, K. K. Jena, A. Jena, B. C. Panda, S. Singh, and P. Behera, "A Reputation Deterministic Framework for True Event Detection in Unmanned Aerial Vehicle Network (UAVN)," in *2019 International Conference on Information Technology (ICIT)*, 2019, pp. 257-262.

[16] V. Valentin-Alexandru, B. Ion, and P. Victor-Valeriu, "Energy efficient trust-based security mechanism for wireless sensors and unmanned aerial vehicles," in *2019 11th International Conference on Electronics, Computers and Artificial Intelligence (ECAI)*, 2019, pp. 1-6.

[17] C. Ge, L. Zhou, G. P. Hancke, and C. Su, "A Provenance-Aware Distributed Trust Model for Resilient Unmanned Aerial Vehicle Networks," *IEEE Internet of Things Journal,* 2020.

[18] K. Singh and A. K. Verma, "A trust model for effective cooperation in flying ad hoc networks using genetic algorithm," in *2018 International Conference on Communication and Signal Processing (ICCSP)*, 2018, pp. 0491-0495.

[19] R. W. Anwara, A. Zainala, F. Outayb, A. Yasarc, and S. Iqbald, " BTEM: Belief based trust evaluation mechanism for Wireless Sensor Networks," Future Generation Computer Systems Volume 96, July 2019, Pages 605-616.

[20] A. J. Deepak Sharma, "Enhancement of Security in Flying AD-HOC Network Using a Trust Based Routing Mechanism," *International Journal of Innovative Technology and Exploring Engineering (IJITEE),* vol. 9, pp. 1-5, 2019.

[21] K. Singh and A. K. Verma, "FCTM: A Novel Fuzzy Classification Trust Model for Enhancing Reliability in Flying Ad Hoc Networks (FANETs)," *Ad Hoc Sens. Wirel. Networks,* vol. 40, pp. 23-47, 2018.

[22] K. Singh and A. K. Verma, "A fuzzy-based trust model for flying ad hoc networks (FANETs)," *International Journal of Communication Systems,* vol. 31, p. e3517, 2018.

[23] A. Rajeswari, K. Kulothungan, S. Ganapathy, and A. Kannan, "A trusted fuzzy based stable and secure routing algorithm for effective communication in mobile adhoc networks," *Peer-to-Peer Networking and Applications,* vol. 12, pp. 1076-1096, 2019.

[24] S. Balaji, E. G. Julie, Y. H. Robinson, R. Kumar, and P. H. Thong, "Design of a security-aware routing scheme in mobile ad-hoc network using repeated game model," *Computer Standards & Interfaces,* vol. 66, p. 103358, 2019.

[25] M. Faraji and R. Fotohi, "Secure Communication between UAVs Using a Method Based on Smart Agents in Unmanned Aerial Vehicles," 2020.

[26] S. Nikam and B. Jadhav, "Delay Analysis of DSDV Protocol using NS 2.34," *International Journal of Computer Applications,* vol. 2, pp. 13-16, 2016.