Chapter 4

Distributed PDA Detection

4.1 Introduction

Various results and analysis of centralized PDA detection methodology in chapter 3 shows that centralized PDA detection methodology is not suitable for a highly dynamic network with malicious node deployment.

Intrusion detection is normally based on collection and analysis of system and network audit data [11]. Apart from this, it also depends on cooperation of neighbor nodes [145][146][147][148]. Distribution is restricted to data collection. A distributed PDA detection methodology is proposed which is named as “New Ad hoc on Demand Distance Vector (NAODV)”. PDA is detected and confirmed not only by the node which has been suffering but also confirmed by other nodes participating in the network. It is not limited to data collection and detection, but also generates alarm to avoid malicious nodes from the network. One of the primary goals of detection methodology is to identify the misbehavior and implement detection methodology in such a way that it should raise less alarm [149]. It is assumed that intelligent agents are supposed to adapt decision making by cooperation with other nodes participating in the network.

4.2 The Architecture

4.2.1 Assumption

In the system model, low rates of packet loss or any other packets drop other than
malicious packet drop are assumed as threshold packet drop. When packet drop is more than the threshold packet drop then PDA is suspected. PDA is suspected in certain node based on the different network performance parameters such as packet delivery ratio as well as throughput of the network. It is assumed that packets are forwarded in a hop-by-hop fashion in on demand ad hoc way. The communication links are assumed to be bi-directional and there is no wireless channel error. All nodes use unidirectional antennas for bidirectional communications. Neighbor discovery protocol is assumed to work in such a way that every node can understand its corresponding neighbor.

It is assumed that all the nodes in MANETs have the capability to understand packet drop in them. Thus it has the ability to understand the threshold packet drop as well as malicious packet drop. Promiscuous mode of node is enabled with source routing. A malicious node can drop packets continuously or selectively. Here collusion of more than one node is not considered, so that malicious node can monitor each other and collude and mask the misbehavior of each other.

It is assumed that intelligent agent are supposed to adapt decision making by the cooperation with other nodes. Activity of the agent is dependent on the network performance matrices such as:

a. Delay in Delivery of the Packet
b. Response Time
c. Quality of Service Provider
d. Packet Forwarding Misbehavior

Accordingly in every node, local agent calculates the following to suspect packet drop misbehavior i.e.:

\[
\text{Packet Drop Ratio} = \frac{\sum \text{No. of packets sent}}{\sum \text{No. of packets received}}
\]

\[
\text{Throughput} = \frac{y}{t} \quad \text{i.e. } y \text{ numbers of packets are delivered within } t \text{ times at a node.}
\]

If for a particular node Packet Drop Ratio (PDR) is very high and throughput is very low then that node is suspected of malicious activity. It is assumed that nodes are communicating to one another in wireless channel and there is some amount of packet
drop due to congestion, overload or for media interference. Flow of traffic will be observed by each node that participated in communication. Agents will perform local analysis of packet drop in every node.

4.2.2 System Model

Proposed distributed PDA detection methodology New Ad hoc on Demand Distance Vector (NAODV) is based on cooperation of different nodes available within the network. Data, collected from different nodes are analyzed to detect PDA. Upon detection, message will be distributed amongst the nodes in terms of alarm to avoid the malicious nodes for packet forwarding. The system is unique in comparison to existing system in several points. Unlike the other TRUST evaluation procedure, While sending PROB REQ, it takes care to avoid feed back or to receive duplicate packets. Use of CONFIDENCE level to determine the TRUST level of a node is also a unique process. It generates more accurate result. Calculation of adaptive time for collecting PROB RESP based on four different conditions, randomly generating the
option is also unique. Use of incremental order decision tree algorithm ID5R, increases the accuracy of the system to evaluate TRUST level of the suspected malicious node. The entire system is an automatic, self manageable process. Data, collected from various node’s host level audit system like “system log”, are analyzed by the system.

**Local Operation**

Local operation runs on each node to detect PDA locally. Then these will collaborate with other modules to confirm PDA in the network.

*Packet analyzer:* It analyzes the packet stream with various fields in the packets and stores the content according to the specified logic. Packet analyzer will legitimately be used to analyze each packet that comes to every node to identify any suspected malicious packet drop in the network.

*Threshold packet drop evaluator:* It determines the threshold value of packet drop due to any reason except malicious packet dropping.

*Initial trust evaluator:* When a node first time joins the network, its trust value is evaluated by this module in cooperation with neighbor nodes according to algorithm 4.3.

*Packet drop detector:* It compares the dropped packets that are evaluated by packet analyzer with threshold packet drop. Once the number of dropped packets is more than the threshold packet drop then packet dropping attack is suspected. It communicates to “cooperative operation” module for confirmation of packet dropping attack.

**Cooperative Operation**

*Communicator:* This module is activated after getting signal from “packet drop detector” module that some packets are dropped beyond the threshold packet drop due to some suspected malicious node. Then it sends the PROB REQ message to all its neighbors to know TRUST and CONFIDENCE level of the suspected malicious node within the adaptive time.
Data collector: PROB RESP, which are sent in response to PROB REQ are collected by this module within the adaptive time. Adaptive time is based on either of the following conditions, randomly generating the options:

a. Number of node scanned ( % of total nodes)
b. Number of Responses expected( % of total nodes)
c. Fixed amount of time to forward PROB REQ and to get PROB RESP
d. Number of level crossed

Decision Maker: This module dynamically evaluates the TRUST level of a node. PROB RESP that is collected from various neighbors containing TRUST and CONFIDENCE level of suspected malicious node, are analyzed to confirm whether the suspected malicious node is really a malicious node or not. To analyze dynamically, incremental decision tree algorithm ID5R [18][19][20][21] is used.

Trust updater: It dynamically updates the TRUST level of the nodes according to Algorithm 4.2

Response Operation

Alarm generator: If the “Decision Maker” confirms that suspected malicious node is a confirmed malicious node then alarm will be broadcasted in the network to avoid the malicious node for packet forwarding.

4.2.3 Algorithm of the Proposed System (NAODV)

Algorithm 4.1 Algorithm for distributed PDA detection methodology

Input: PDR, Tth, Dth, Receive packets, Sent Packets, Drop packrts, Node IP, adaptive_time

Output: malicious Node IP, alarm

1. Initialize the value of Tth { * Tth is the minimum throughput for a network *}
2. Initialize the value of Dth { * Dth is the threshold packet drop in a network *}
3. if (node IP = new node IP) then { * If a node joins as new node. Node IP means IP address of a node *}
4. evaluate initial TL { * As in Algorithm 4.3 *}
5. create LOG file and save TL in LOG file
6. end if
7. \[ PDR := \frac{\sum \text{No.of sent}}{\sum \text{No.of receive}} \] { * PDR is the packet drop ratio *}

105
8. \[ T := \frac{y}{t} \] \{ * T is the Throughput and \( y \) is the numbers of packets delivered within \( t \) times at a node. * \}

9. \textbf{if} (PDR > Dth) AND (T < Tth) \textbf{then} 
10. \hspace{1em} print \textit{suspected_malicious_node} 
11. \hspace{1em} broadcast \textit{PROB REQ} \{ * \textit{PROB} \textit{REQ} is the \textit{REQ} packet which is sent to all neighbors of the node that suspects PDA* \} 
12. \textbf{end if} 
13. \textbf{do} 
14. \hspace{1em} neighbor checks its "\textit{LOG file}" for relevant data 
15. \hspace{1em} if (TRUE) 
16. \hspace{2em} send \textit{PROB RESP} to original\_sender in step 11 
17. \hspace{2em} else 
18. \hspace{3em} forward \textit{PROB REQ} to their neighbors 
19. \hspace{2em} end if 
20. \hspace{1em} collect \textit{PROB RESP} from the neighbors 
21. \hspace{1em} forward \textit{PROB RESP} to original\_sender 
22. \hspace{1em} generate decision tree to identify \textit{confirm_malicious_node} \{ * Decision tree is generated as per logic of ID5R * \} 
23. \textbf{while} (adaptive\_time) \textbf{goto} step 12 \{ * Till adaptive\_time, sender accepts PROB RESP * \} 
24. \textbf{if} (suspected\_malicious\_node== confirm\_malicious\_node) \textbf{then} 
25. \hspace{1em} GD:="malicious" \{ * GD is the global decision of all neighbors to confirm PDA \} 
26. \hspace{1em} * \} 
27. \hspace{1em} print "Confirm\_malicious\_node IP" 
28. \hspace{1em} Generate and broadcast "alarm" to avoid the malicious node for packet forward 
29. \hspace{1em} else 
30. \hspace{2em} GD:="non malicious" 
31. \hspace{1em} end if 

Activity diagram for the Algorithm 4.1 is shown in Figure 4.2.
The "LOG file" contains the following fields in it.

Node IP: IP address of its neighbors
Confidence level (CL): Confidence level of node
Trust level (TL): Trust level of node

PROB REQ contains the following fields,

Req_from: IP address of the node that sends PROB REQ
Req_to: IP address of the node to whom it sends PROB REQ
**Mal_node**: IP address of the suspected malicious node

Neighbor list: List of neighbor nodes of the sender to avoid feedback which may occur due to duplicate `PROB REQ` that may be sent from the receiver.

**Adaptive_time**: It is time within which node should respond to sender, Adaptive time is based on either of the following conditions, randomly generating the options:

- Number of node scanned (% of total nodes)
- Number of `PROB RESP` expected (% of total nodes)
- Fixed amount of time to forward `PROB REQ` and to get `PROB RESP`
- No. of level crossed

In **Algorithm 4.1**, `PROB RESP` contains the following fields,

- `Req_from`: IP address of the sender
- `Suspected_mal`: IP address of suspected malicious node
- `Response_to`: IP address of the node where it will send the response
- `Confidence_level`: Confidence level of the suspected malicious node
- `Trust_level`: Trust level of the suspected malicious node

In **Algorithm 4.1**, Condition of **No Response** may occur due to following reasons, if

- There is no neighbor to forward the request.
- If adaptive time “t” is over
- If the node is in out of range from the network after getting request
- If any node is a co-operative malicious node with the suspected malicious node
- If a node is not communicating due to selfish behavior or to save its resources
- If link failure occurs

Following Algorithm 4.2 shows the dynamic TRUST evaluation process of nodes based on their cooperative participation in detection process.

---

**Algorithm 4.2** Algorithm to update TRUST level of node

**Input**: $T_{ln}$, GD
Output: $T_{Lc}$

1: get $T_{Lm}$ {* $T_{Lm}$ is the TRUST level of suspected_malicious_node send by $n$ *}
2: get $GD$ {* $GD$ is the Global decision generated by decision tree for suspected malicious node in algorithm 4.1*}
3: If ($GD=\text{"malicious"}$) then
4: \hspace{1em} If ($T_{Lm}=\text{"high"}$) then
5: \hspace{2em} $T_{Lc}:=\text{low}$ {* $T_{Lc}$ is the TRUST level of node $n$ that sends PROB RESP *}
6: \hspace{1em} else
7: \hspace{2em} $T_{Lc}:=\text{high}$
8: end if
9: end if
10: If ($GD=\text{"non malicious"}$) then
11: \hspace{1em} If ($T_{Lm}=\text{low}$) then
12: \hspace{2em} $T_{Lc}:=\text{low}$
13: \hspace{1em} else
14: \hspace{2em} $T_{Lc}:=\text{high}$
15: end if
16: end if

In Algorithm 4.3, Initial TRUST LEVEL ($TL$) evaluation algorithm is given. Trust Level ($TL$) for a node can be defined according to behavior of the node. It can be defined either as TRUST or DISTRUST. TRUST is assumed as “1” and DISTRUST as “0”. To assign initial $TL$ to a node, it follows a distributed cooperative process. It not only depends on the node which wants to assign $TL$ but also depends on the other neighbors of that node according to Algorithm 4.3.

Algorithm 4.3 Algorithm to find initial TRUST evaluation of a node

Input: $T_{Li}$, $n$, $i$

Output: $TL$

1: $i:=1$
2: for all ( $i$ in $n$) do {* $n$ is the number of neighbors of a new node for which initial TRUST to be evaluated *}
3: \hspace{1em} send TRREQ {* TRREQ is the trust request send to all neighbors of a node to send TRUST level for which TRUST to be evaluated *}
4: \hspace{1em} if ($TL(i)=1$) then {* $TL_i$ is the TRUST level sent by neighbor $i$ *}
5: \hspace{2em} $TOT_{TRUST}:=TOT_{TRUST}+1$ {* $TOT_{TRUST}$ is the Total number of nodes that assign TRUST value as “HIGH” *}
6: \hspace{1em} else
7: \hspace{2em} $TOT_{DISTRUST}:=TOT_{DISTRUST}+1$ {* $TOT_{DISTRUST}$ is the Total...
number of nodes that assign TRUST value as “LOW” *}

8:     end if
9:     end for
10:   $p := \frac{2}{3} \times n$
11:   if ($TOT\_TRUST \geq p$) then
12:     $TL := HIGH$ \{ * $TL$ is the TRUST level of the new node *\}
13:   else
14:     $TL := LOW$
15:   end if

4.2.4 Performance Parameters

Network performance parameters which are used to measure network performance before and after implementation of proposed detection methodology, NAODV are same as mentioned in section 3.2.4 of Chapter 3.

4.3 Multi Agent System for Proposed Methodology
4.3.1 Introduction

Multi agent system is a system that consists of several autonomous agent involved with different activity with common objective. These are computational systems work asynchronously with respect to other agents [155]. They can interact, cooperate or exchange data with other agents so that their common effort helps to attain the goal. Due to flexible problem solving approach of multi agent system, these are in high demand to address the challenges faced by MANETs. In MANETs, capability of nodes to forward packets and to participate in routing process, directly affects the network characteristics [150][153]. Moreover, intrusion detection in MANETs, that carried out in a mobile agent based system has the advantages of overcoming different challenges of MANETs such as network latency, reducing network load, autonomous execution, platform independency, dynamic adaptation and scalability [151][152][156]. Mobile agents are alternative to the client-server distribution model. Such autonomy system can generate decision, distribute decision automatically, but limited to the specification provided in the design.
4.3.2 Multi Agent Architecture for Proposed Algorithm

![Diagram of multi agent system]

Proposed distributed packet dropping attack detection methodology can relate with multi agent system in which several agents as mentioned below should work actively to set a common goal that is packet dropping attack detection.

According to Figure 4.3, the multi agent system consists of the following agents:

**Local Agent:** Local agent will run on each node to suspect packet dropping attack locally. Then these will collaborate with other agent to confirm packet dropping attack in the network. Based on the type of functions, it contains the following agents under it.

- Packet Analyzer
- Threshold Packet drop evaluator
- Initial trust evaluator

Figure 4.3: Schematic diagram of multi agent system of distributed PDA detection
- Packet Drop Detector

Co-operative Agent: Cooperative agents involve with collaboration of other categories of agents such as Local agent and Response agent. It also contains following agents under it.
- Communicator agent
- Data collector agent
- Decision Maker agent
- Trust updater agent

Response Agent: This agent generates and distributes alarm to the network when decision taken by cooperative agents with respect to malicious packet dropping attack is positive.

4.3.3 Collaboration-Multi Agent System

The proposed PDA detection methodology is based on collaborative functions of different independent agents. Agents are well understood about their functions. Automated agents work independently in the network and then correlate or exchange their data with other agents to generate a common decision.

As shown in Figure 4.3, the proposed multi agent system is a combination of three groups of agent namely Local agent, Cooperative agent and Response agent. They collaborate with one another to take mutual decision of packet dropping attack in MANETs.

Local agent is implemented in every system in the network, which gathers information about its own system. It analyzes the packet dynamically to compare the packet drop in the network with threshold packet drop. If it finds number of packet drop is more than the threshold packet drop than it communicates with cooperative agent for distributed cooperative decision for PDA.

Communicator agent communicates with neighboring nodes to send specified data to data collector agent of cooperative agent.
Data collector agent is implemented with detection methodology to provide specified data to decision maker agent to decide the PDA in MANETs. Trust updater agent of cooperative agent dynamically updates TRUST of nodes based on cooperative participation of nodes.

If the Cooperative agent confirms malicious packet dropping in the network, then it communicates with response agent to broadcast an alarm to the network to avoid the malicious node from further communication.

4.4 Performance Evaluation of the Detection Mechanism

4.4.1 NAODV using Random Way Point Model

Simulation Environment

Table 4.1: Simulation Environment (RWP Model)

<table>
<thead>
<tr>
<th>Animation area</th>
<th>1000m X 1000m</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mobility model</td>
<td>Random way point (RWP)</td>
</tr>
<tr>
<td>Channel type</td>
<td>Wireless</td>
</tr>
<tr>
<td>No. of nodes</td>
<td>100</td>
</tr>
<tr>
<td>Simulation time</td>
<td>600 sec</td>
</tr>
<tr>
<td>Pause time</td>
<td>10-70 sec</td>
</tr>
<tr>
<td>Node Speed</td>
<td>10-70 m/s</td>
</tr>
<tr>
<td>Data rate</td>
<td>100 kbs</td>
</tr>
<tr>
<td>Transmission range</td>
<td>100 m</td>
</tr>
<tr>
<td>Packet size</td>
<td>512 byte</td>
</tr>
<tr>
<td>Traffic type</td>
<td>CBR</td>
</tr>
<tr>
<td>Routing protocol</td>
<td>AODV, SAODV, TAODV, NAODV</td>
</tr>
</tbody>
</table>

Simulation Results

Simulations are performed for three different methodologies namely SAODV, TAODV and proposed NAODV with following criteria:
a. When percentage of malicious node is increasing, then constant node speed and pause time is maintaining
b. When node speed is increasing, then constant malicious node percentage and pause time is maintaining
c. When pause time is varying, then constant node speed and percentage of malicious node is maintaining

4.4.1.1 Detection Rate (NAODV, SAODV, TAODV)

Figure 4.4 shows the detection rate of all the three different methodologies with increased number malicious nodes. Similarly, Figure 4.5 shows the detection rate with increased node mobility, while Figure 4.6 shows the detection rate with increased pause time. It is observed that NAODV shows the best performance in all the three cases.

![Detection Rate Graph](image)

Figure 4.4. Effect of increase of malicious node on detection rate (RWP Model)

It can be explained by the fact that in NAODV, malicious node detection and avoidance is completely based on cooperation of neighbors. Global decision is taken based on decision tree algorithm. Accordingly TRUST level of the node is dynamically updated. On the other hand, TAODV is a trusted routing protocol that cooperates with a self organized key management mechanism. Moreover it performs trusted routing in a self-organized way. In SAODV, signature is verified by both source node and intermediate node and then only routing table is updated. Malicious
node cannot generate signature of destination node, hence it will not be able to impersonate destination node.

![Figure 4.5. Effect of increase of node mobility on detection rate (RWP Model)](image)

![Figure 4.6. Effect of increase of pause time on detection rate (RWP Model)](image)

### 4.4.1.2 False Positive Rate (NAODV, SAODV, TAODV)

Figure 4.7, Figure 4.8 and Figure 4.9 compare the false positive rate of three different methodologies with respect to increased number of malicious node, increased node mobility and increased pause time. SAODV is not designed to resist the DoS attacks like packet dropping attack. It provides a cryptographic support to secure the routing protocol. It shows the vulnerabilities to packet dropping attack.
Figure 4.7 Effect of increase of malicious node on false positive rate (RWP Model)

Figure 4.8 Effect of increase of node mobility on false positive rate (RWP Model)

Figure 4.9 Effect of increase of pause time on false positive rate (RWP Model)
TAODV facilitates trusted routing, not directly involve with PDA detection. On the other hand, in NAODV, detection of malicious packet dropping is done in distributed cooperative way, after confirmation only it generates an alarm to avoid the malicious nodes for further packet forwarding, hence false positive rate will be comparatively less.

4.4.1.3 Throughput Analysis (NAODV, SAODV, TAODV)

Throughput of the network is compared for three methodologies as shown in Figure 4.10, Figure 4.11 and Figure 4.12.

![Figure 4.10 Effect of increase of malicious node on throughput (RWP Model)](image)

In SAODV, it takes some extra time for computation and verification of security fields during route discovery process. It always prefers safest path instead of shortest path. These all consume some extra time. Since throughput depends on total number of packets delivered in specified time, hence it comes down. TAODV also consumes extra time for updating TRUST by evidence & opinion, exchange and authentication. But NAODV doesn’t consume much time for route discovery and there are not so complex security measures during route discovery, so it delivers more packets in specified time. This implies more throughputs.
Figure 4.11 Effect of increase of node mobility on throughput (RWP Model)

Figure 4.12 Effect of increase of pause time on throughput (RWP Model)

4.4.1.4 Packet Delivery Ratio Analysis (NAODV, SAODV, TAODV)

Figure 4.13, Figure 4.14 and Figure 4.15, compare the packet delivery ratio of NAODV, SAODV and TAODV.

In all the three cases, NAODV performs the best. NAODV is simply meant for packet dropping attack detection. So, for any network, it tries to detect malicious node in distributed cooperative way and avoid the same for further packet forwarding. By this it decreases packet drop ratio and oppositely it increases packet delivery ratio.
When the node mobility is higher, it signifies the high failure of connectivity and frequent change of topology. As a result, packets drop ratio will be more. Nodes may
be falsely accused of malicious. It is more in case of SAODV than TAODV, while less in case of NAODV. SAODV chooses the safest path instead of shortest path and tries to eliminate the malicious nodes in the way, so the average path length is longer. As the node mobility is higher, the network topology will break frequently and it will not be able to deliver the packets on time. Moreover high security application of SAODV will resist the path more.

### 4.4.1.5 Normalized routing load Analysis (NAODV, SAODV, TAODV)

NRL is the ratio between total numbers of routing packets to total number of delivered packets. A network contains more malicious nodes means it will drop more packets. NRL is inversely proportional to PDR. In presence of malicious node, NAODV shows better performance in comparison to other two methodologies such as SAODV and TAODV as shown in Figure 4.16.

![Figure 4.16](image)

**Figure 4.16** Effect of increase of malicious node on normalized routing load (RWP Model)

In presence of malicious nodes in the network, it forces SAODV to use hash chain and digital signature to provide secure routing process. That leads to slow PDR, thus it creates more NRL in the network. Similarly, in TAODV, system performance is improved in comparison to SAODV by avoiding generating and verifying digital signatures at every routing hop.
According to Figure 4.17, in case of SAODV, NRL is found to be more than that of TAODV and NAODV due to its intensity to find the safest path. In high mobility of node, network topology change and link failure occurs frequently. Network becomes unstable for all the time. As a result, SAODV is unable to find the safe path for routing. PDR is decreasing, thus NRL is increasing. In TAODV, a node does not request and verify certificates continuously. So, computation overhead is reduced greatly. At the same time, in TAODV, the whole system provides security to the system up to certain level, not directly involved in PDA detection. NAODV is directly involved with PDA detection and avoidance in distributed way, hence controlling of PDA in NAODV, leads to high packet delivery ratio. So, NRL is less in comparison to other two systems.

![Figure 4.17 Effect of increase of node mobility on normalized routing load (RWP Model)](image)

![Figure 4.18 Effect of increase of pause time on normalized routing load (RWP Model)](image)
According to Figure 4.18, with increase number of pause time in the network, NRL is gradually decreasing in all the methodologies such as SAODV, TAODV and NAODV. When pause time is increasing network is getting more stable which indicate regular and stable behavior of nodes. So, additional packet drop due to highly dynamic node will be reduced.

4.4.1.6 End-to-end Delay Analysis (NAODV, SAODV, TAODV)

In Figure 4.19, it is observed that end-to-end delay is increasing with increased number of malicious in all the three different methodologies. In MANETs, end-to-end delay is the delay encountered by a packet right from the generation of the packet from the source and till it gets back the ACK from destination. The packet delay consists of the queuing delay experienced at the source node, the queuing delays incurred at the intermediate nodes as well as MAC delay observed at the source and intermediate nodes. Presence of increased malicious node in MANET will invariably drop packets. In SAODV and TAODV, due to high security measures during route discovery from source to destination, end-to-end delay is more. As number of malicious nodes is increasing it consumes more time, thus end-to-end delay is also more.

In Figure 4.20, in case of high node mobility, with deployment of malicious node, both SAODV and TAODV show the instability in end-to-end delay. Due to dynamic nature of nodes in MANET, state and characteristics of nodes may change, even in high node mobility; nodes can change their characteristic frequently. Thus packets from source to destination may not reach on time or end-to-end delay may increase. In case of SAODV and TAODV, high security measures during path delivery as well as packet delivery, causes the high end-to-end delay. On the other hand NAODV shows almost a stable and low end-to-end delay in spite of increased number of node speed. In Fig 4.21, when the pause time is more, due to network stability, in all the three cases end-to-end delay is gradually decreasing. Still it is more in case of SAODV and
TAODV because of their computational overhead during security measure during packet delivery.

Figure 4.19 Effect of increase of malicious node on end-to-end delay (RWP Model)

Figure 4.20 Effect of increase of node mobility on end-to-end delay (RWP Model)

Figure 4.21 Effect of increase of pause time on end-to-end delay (RWP Model)
4.4.1.7 **Round trip time (NAODV, SAODV, TAODV)**

From the Figure 4.22, it is clear that as the number of malicious node is increasing in the network, NAODV consumes less RTT in comparison to other two methodologies. In SAODV, it measures the generation and validation of nodes that switch between signing, verifying and hash chain operations rapidly in case of both send and receive message. Each message is validated before any further processing takes place. So, each RREQ and RREP gets delayed by some amount of time at each hop through which message should be forwarded. When the number of malicious nodes is increasing, due to complex security measures, SAODV shows more RTT in comparison to other two methodologies. TAODV shows comparatively less amount of time. But in TAODV, due to its simplicity in comparison to SAODV, there is much less pre-packet overhead. The main overhead that incurred in TAODV is the overhead related to R ACK packets which is a new kind of packet rather than packet extension.

![Figure 4.22 Effect of increase of malicious node on round trip time (RWP Model)](image)

As in Figure 4.23, when the node speed is increasing with malicious node deployment, RTT is increasing in all the three cases, though it is lowest in case of NAODV. High mobility is the significance of more unstable network, frequent breakage of links etc, as a result packet delivery time will also be increased, and thus it takes much time to get ACK packet from destination to source after sending packet.
from source. On the other hand, in case of SAODV and TAODV, it is affected more because of their complexity in computation.

In Figure 4.24, as the pause time is increasing, for all the three cases, RTT is gradually decreasing. When the pause time in the network is more, it indicates more stable network, thus node characteristics are also remained constant. Probability of frequent link breakage will be low. Packets may deliver to destination on time, source also gets ACK packet on time. Hence, RTT is getting low. In SAODV and TAODV, it is more than that of NAODV, because of additional time consumption for security measures during packet delivery.
4.4.2 NAODV using Levy Walk Model

Simulation Environment

<table>
<thead>
<tr>
<th>Table 4.2: Simulation Environment (LWM)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Animation area</td>
</tr>
<tr>
<td>Mobility model</td>
</tr>
<tr>
<td>Channel type</td>
</tr>
<tr>
<td>No. of nodes</td>
</tr>
<tr>
<td>Simulation time</td>
</tr>
<tr>
<td>Pause time</td>
</tr>
<tr>
<td>Node Speed</td>
</tr>
<tr>
<td>Data rate</td>
</tr>
<tr>
<td>Transmission range</td>
</tr>
<tr>
<td>Packet size</td>
</tr>
<tr>
<td>Traffic type</td>
</tr>
<tr>
<td>Routing protocol</td>
</tr>
</tbody>
</table>

Simulation Results

Simulations are performed for three different methodologies namely SAODV, TAODV and proposed NAODV with following criteria:

d. When percentage of malicious node is increasing, then constant node speed and pause time is maintaining

e. When node speed is increasing, then malicious node percentage and pause time is maintained as constant.

f. When pause time is varying, then constant node speed and constant percentage of malicious node is maintaining

4.4.2.1 Detection Rate (NAODV, SAODV, TAODV)

Figure 4.25 shows the detection rate of all the three different methodologies with increased number of malicious nodes. Similarly, Figure 4.26 shows the detection rate
with increased node mobility, while Figure 4.27 shows the detection rate with increased pause time. It is observed that NAODV shows the best performance in all cases except detection rate with increased pause time. In this case, initially SAODV shows the best performance. Mixed response is shown by the SAODV and TAODV in malicious node deployment. In this scenario, detection rate of NAODV is almost stable irrespective of increase of malicious node.

![Figure 4.25. Effect of increase of malicious node on detection rate (LWM)](image)

![Figure 4.26. Effect of increase of node mobility on detection rate (LWM)](image)

It can be explained by the fact that in NAODV, malicious node detection and avoidance is completely based on cooperation of neighbors. Global decision is taken based on incremental order decision tree algorithm. Accordingly TRUST level of the node is dynamically updated. On the other hand, TAODV is a trusted routing protocol
that cooperates with a self organized key management mechanism. Moreover, it performs trusted routing in a self-organized way. In SAODV, signature is verified by both source node and intermediate node and then only routing table is updated. Malicious node cannot generate signature of destination node, hence it will not be able to impersonate destination node.

Figure 4.27. Effect of increase of pause time on detection rate (LWM)

4.4.2.2 False Positive Rate (NAODV, SAODV, TAODV)

Figure 4.28 Effect of increase of malicious node on false positive rate (LWM)
Figure 4.28, Figure 4.29 and Figure 4.30 compare the false positive rate of three different methodologies with respect to increased number of malicious node, increased node mobility and increased pause time. Initially, the false positive rate of TAODV is slightly differed from NAODV, but as the number of malicious node is increasing, false positive rate of TAODV and SAODV is also increasing, it is less in case of TAODV compared to SAODV. Observation from Figure 4.29, it is clear that NAODV shows mixed response with increase node mobility. Still its performance is better. At certain point with high node mobility, false positive rate of TAODV is more than SAODV. But in Figure 4.30, as the pause time is increasing, there is very less difference in performance amongst SAODV, TAODV and NAODV, though at high pause time NAODV shows better performance. SAODV partially resists the DoS
attacks like packet dropping attack. It provides a cryptographic support to secure the routing protocol. Hence it shows vulnerabilities to packet dropping attack. TAODV facilitates trusted routing rather than PDA detection. On the other hand, in NAODV, detection of PDA is based on distributed cooperative way and it generates alarm to avoid the malicious nodes for further packet forwarding after getting confirmation from all neighbors. As a result, false positive rate is comparatively less.

**4.4.2.3 Throughput Analysis (NAODV, SAODV, TAODV)**

![Figure 4.31 Effect of increase of malicious node on throughput (LWM)](image)

Throughput of the network is compared for three methodologies as shown in Figure 4.31, Figure 4.32 and Figure 4.33.

In SAODV, it takes extra time for computation and verification of security fields during route discovery process. It always prefers safest path instead of shortest path. These all consume some extra time. Due to this throughput comes down as it depends on total number of packets delivered in specified time. TAODV also consumes extra time for updating TRUST by evidence & opinion, exchange and authentication. But NAODV doesn’t consume much time for route discovery and there is not much complex security measures during route discovery, so it delivers more packets in specified time. This implies more throughputs. When node mobility is high, at some point, throughput of SAODV and TAODV are almost equal but later on during high
node mobility, performance of TAODV becomes better though its performance is quite low in comparison to NAODV.

![Figure 4.32](image1.png)

**Figure 4.32** Effect of increase of node mobility on throughput (LWM)

![Figure 4.33](image2.png)

**Figure 4.33** Effect of increase of pause time on throughput (LWM)

### 4.4.2.4 Packet Delivery Ratio Analysis (NAODV, SAODV, TAODV)

Figure 4.34, Figure 4.35 and Figure 4.36, compare the packet delivery ratio of NAODV, SAODV and TAODV.

In all the three cases, NAODV performs the best. NAODV is simply meant for packet dropping attack detection while other two methodologies partially detect PDA. NAODV detects malicious node from the network in cooperative distributed way and
avoid such nodes for packet forwarding. By this it reduces packet drop ratio and oppositely increases packet delivery ratio.

![Graph showing packet delivery ratio vs node mobility](image1)

**Figure 4.34 Effect of increase of malicious node on packet delivery ratio (LWM)**

![Graph showing packet delivery ratio vs node mobility](image2)

**Figure 4.35 Effect of increase of node mobility on packet delivery ratio (LWM)**

When the node mobility is higher, it signifies the high failure of connectivity and frequent change of topology. As a result, it drops more packets. Nodes may be falsely accused of malicious. It is more in case of SAODV than TAODV, while less in case of NAODV. SAODV chooses the safest path instead of shortest path and tries to eliminate the malicious nodes in the way, so the average path length is longer. When the node mobility is higher, the network topology breaks down frequently and it is not
be able to deliver the packets on time. Moreover high security application of SAODV resists the path more.

![Figure 4.36 Effect of increase of pause time on packet delivery ratio (LWM)](image)

### 4.4.2.5 Normalized routing load Analysis (NAODV, SAODV, TAODV)

Normalized Routing Load (NRL) is the ratio between total numbers of routing packets to total number of delivered packets. A network contains more malicious nodes means it drops more packets. NRL is inversely proportional to PDR. In presence of malicious node, NAODV shows better performance in comparison to other two methodologies such as SAODV and TAODV as shown in Figure 4.37. Of course at certain point NRL of NAODV and TAODV becomes almost same. But after that NRL of NAODV is getting down irrespective of more malicious node deployment.

In presence of malicious nodes in the network, it forces SAODV to use hash chain and digital signature to provide secure routing process. That leads to less packet delivery ratio, thus it generates more NRL in the network. But in TAODV, system performance is improved in comparison to SAODV by avoiding generating and verifying digital signatures at every routing hop.
According to Figure 4.38, in case of SAODV, NRL is found to be more than that of TAODV and NAODV due to its intensity to find the safest path. During high node mobility, network topology changes frequently. That results in frequent link failure. Network becomes unstable for all the time. As a result, SAODV is unable to find the safe path for routing. PDR is decreasing, thus NRL is increasing. In TAODV, a node does not request and verify certificates continuously. So, computation overhead is reduced greatly in comparison to SAODV. At the same time, TAODV provides security to the system up to certain level, thus it decreases packet delivery ratio to some extent. Due to direct involvement of NAODV for PDA detection and avoidance of malicious node, its packet delivery ratio is higher in comparison to SAODV and TAODV. Thus, it results in low NRL.
According to Figure 4.39, NRL is gradually decreasing in all the three different methodologies as the pause time in gradually increasing. High pause time implies more stable network, which indicate regular and stable behavior of nodes. So, additional packet drop due to highly dynamic node is controlled.

![Normalized Routing Load (LWM) vs Pause Time](image)

Figure 4.39 Effect of increase of pause time on normalized routing load (LWM)

### 4.4.2.6 End-to-end Delay Analysis (NAODV, SAODV, TAODV)

In Figure 4.40, it is observed that end-to-end delay is increasing with increased number of malicious nodes in all the three different methodologies. In MANETs, end-to-end delay is the delay encountered by a packet right from the generation of the packet from the source and till it gets back the ACK from destination. The packet delay consists of the queuing delay experienced at the source node, the queuing delays incurred at the intermediate nodes as well as MAC delay observed at the source and intermediate nodes. Presence of increased malicious node in MANETs invariably drops packets. In SAODV, end-to-end delay is gradually increasing with increasing order of malicious node. But, TAODV shows mixed response. At some point, end-to-end delay of NAODV is same as that of TAODV but due to simplicity of operation of NAODV, end-to-end delay is getting down in comparison to TAODV and SAODV.
Figure 4.40 Effect of increase of malicious node on end-to-end delay (LWM)

Figure 4.41 Effect of increase of node mobility on end-to-end delay (LWM)

Figure 4.42 Effect of increase of pause time on end-to-end delay (LWM)
In Figure 4.41, in case of high node mobility, with deployment of malicious node, both SAODV and TAODV show the instability in end-to-end delay. Due to dynamic nature of nodes in MANETs, state and characteristics of nodes may change. Nodes can change their characteristic frequently. Thus packets from source to destination may not reach on time or end-to-end delay may increase. Techniques that provide security used by SAODV and TAODV are more complex in comparison to NAODV; it results in high end-to-end delay. On the other hand, NAODV shows almost a stable and low end-to-end delay in spite of high node mobility.

In Figure 4.42, when the pause time is more, due to network stability, in all the three cases end-to-end delay is gradually decreasing. Still it is more in case of SAODV and TAODV because of their computational overhead during security measure in packet delivery.

### 4.4.2.7 Round trip time (NAODV, SAODV, TAODV)

From the Figure 4.43, it is clear that as the number of malicious node is increasing in the network, NAODV consumes less RTT in comparison to other two methodologies. In SAODV, it measures the generation and validation of nodes that switch between signing, verifying and hash chain operations. Each message is validated before any further processing takes place. So, each RREQ and RREP packet is delayed by some amount of time at each hop through which message should be forwarded. When the number of malicious nodes is increasing, due to complex security measures, SAODV takes more RTT in comparison to other two methodologies. TAODV takes comparatively less time. But in TAODV, due to its simplicity in comparison to SAODV, there is much less pre-packet overhead. The main overhead that incurred in TAODV is the overhead related to R ACK packets which is a new kind of packet rather than packet extension.

As in Figure 4.44, when the node speed is increasing with malicious node deployment, RTT is increasing in all the three cases, though it is lowest in case of NAODV. High node mobility is the significance of more unstable network. Due to
frequent breakage of links, packet delivery time also be increases, and thus it takes much time to get ACK packet from destination to source after sending packet from source. On the other hand, in case of SAODV and TAODV, it is affected more because of their complexity in computation.

![Figure 4.43 Effect of increase of malicious node on round trip time (LWM)](image)

![Figure 4.44 Effect of increase of node mobility on Round trip time (LWM)](image)

In Figure 4.45, as the pause time is increasing, for all the three cases, RTT is gradually decreasing. When the pause time in the network is more, it indicates more stable network, thus node characteristics are also remained constant. Probability of frequent link breakage will be low. Packets may deliver to destination on time, source also gets ACK packet on time. Hence, RTT is getting low. In SAODV and TAODV,
it is more than that of NAODV, because of additional time consumption for security measures during packet delivery.

![Figure 4.45 Effect of increase of pause time Round trip time (LWM)](image)

### 4.5 Discussion

From various simulation results for two different mobility models such as *Random way point mobility* model and *Levy walk* mobility model, it is found that distributed PDA detection methodology is more appropriate than centralized PDA detection methodology. Static, offline, centralized PDA detection methodology is not suitable to handle dynamic unstable nodes of MANETs. Distributed cooperative decision making process, dynamic TRUST evaluation of nodes; detection and avoidance of malicious nodes, makes the distributed PDA detection methodology efficient. Different simulation results that is generated for SAODV, TAODV and NAODV, for different network performance parameters, it is found that NAODV shows the best results.

TAODV is a trusted routing protocol with a self organized key management mechanism that follows the self organized way. SAODV indirectly handles PDA by providing cryptographic support to secure the routing protocol. NAODV detects PDA in distributed cooperative way. After confirmation of PDA, it generates alarm to the system to avoid malicious nodes from further communication. For computation and verification of security fields, SAODV takes some extra time to discover route and
deliver packets to destination. TAODV also needs some extra time for TRUST updates by evidence and opinion, exchange and authentication. NAODV computes and updates TRUST dynamically for PDA detection purpose and it doesn’t consume much time for route discovery and there is a not much complex security measure during route discovery so it delivers more packets in specified time.

High node mobility signifies the high failure of connectivity and frequent change of topology. Nodes may be falsely accused of malicious. From results, it is confirmed that it is more in SAODV and TAODV in comparison to NAODV. SAODV uses the hash chain and digital signature to provide secure routing process. But the other two methodologies avoid generating and verifying digital signature at every routing hop.

Performance of all the three different methodologies degrade in case of increased node mobility, while it upgrades during increased number of pause time. It is because of the unsteadiness of the network during high node mobility and stability of the network during high pause time. Performance of NAODV is still better in comparison to the other two methodologies, because of simplicity of computation and dedication of service for PDA detection.