A Comprehensive Formal Testing of Few Attacks on Mobile Ad-hoc Networks By Using VDM-SL Tool Box

[1]Umar Draz[†], [*2]Tariq Ali[†], [3]Khurshid Asghar[††], [4]Asis Jamal[†††], [5]Aiman Anum[†], [6]Sarah Javed[†] ,[7]Sana Yasin[†]

[†]CS Department; COMSATS University Islamabad; Sahiwal Campus, Pakistan, 5700, +92 308 6903234
[††]CS Department; University of Okara, Okara Pakistan
[†††]CS Department; Barani Institute of Sciences, PMAS ARID University Rawalpindi, Sahiwal campus, Pakistan

Abstract
Due to less infrastructure framework Mobile Ad-hoc Networks (MANETs) also called a wireless ad-hoc network. Rapid advancement in the ad-hoc network creates a need to secure this type of network against different attacks. It is because of, indeed; the secure network has a great impact on overall performance and quality of the services (QoS) parameters like communication delay, packet delivery/loss ratio and bandwidth. One of the biggest challenge is to secure this type of network from all vulnerable external and internal possible attacks. In this paper, we analyze the active and passive attacks that mostly act upon on the network and describe its mathematical based verification and validation. The cluster-based approach is designed to resolve the issue of the vulnerable attacks for ad-hoc networks. The complete analysis is designed in Formal Methods (FMs) because formal methods are the most emerging technique based on mathematics. Formal language notation tool bx called Vienna Development Method-Specification Language (VDM-SL) is used to analyze all the passive and active attacks of the MANETs.

Keywords
MANET; Passive attacks, Vulnerable; defense; Formal Methods; Security; Verification & Validation; VDM-SL, etc.

1. Introduction

In recent years; Mobile Ad-hoc Networks (MANETs) have become one of the most popular research areas due to its wide variety of applications. Due to the absence of any physical infrastructure, the MANETs has a lot of research scope that needs to investigate further. Due to this feature MANETs network sometime called "infrastructure less network". Now MANETs is a new emerging technology that enables the users to communicate without any central infrastructure. The proliferation of small and more powerful devices that make the network fast, flexible and easy to use is the property of any network. Every device moves independently without any direction, therefore the nodes in this type of network are called mobile and the network is called mobile network [1]. All the nodes are connected to each other with some type of wireless links. Due to the constant mobility of every node, the topology of the network is not static but dynamic. As quickly changing the topology, the behavior of the network is difficult to predict. There are several routing protocols that work under the MANETs [2]. Under the ad-hoc routing protocol three main types of routing techniques like flat routing, hierarchical routing, and geographical position assisted routing are most common. Under these three categories, the types of routing protocol are further subdivided into proactive, reactive and hybrid nature. Flat routing is sub-divided into two main types proactive and reactive. FSR and DSDV [3], TBRPF [4], OLSR [5], and FSFL routing protocols are an example of a proactive nature. The most common routing protocols are AODV and DSR [6] that have reactive nature. in addition, we already performed the comparative analysis against different parameters for these two protocols in [22, 23]. In the hierarchical category CGSR, ZRP, HSR, and LANMAR are the most common routing protocols. Geo Casting, LAR, GPSR, and DREAM are fallen under the Geographical based routing category. There is a different broadcasting approach used in MANETs like unicasting, multicasting, broadcasting, and geocasting. Due to the decentralization of the network and constant change in topology, the message routing between nodes is difficult to process. Another reason is that the topology of the network does not static therefore there are several challenges and security threads that remain these types of networks.

As compared to wired network, MANETs is more vulnerable due to mobile nodes, dynamic topology, message routing, and infrastructure less entity, limited physical security, and low-quality management. These are a basic weakness of MANETs that needs to address. Due to these vulnerabilities, MANETs are less secure and has a large chance of malicious attack. There is much vulnerability that directly or indirectly affects the security of the network like, lack of central management, unavailable resources, scacilibilty issue of the topology, limited power supply, bandwidth constraints, adversary inside the network, no predefined boundary and dynamic topology [6]. Due to these major problems, the performance of the network is really disturbed in the form

Manuscript received July 5, 2019
Manuscript revised July 20, 2019

of several parameters like massage and packet forwarding, the throughput of the protocol, end-to-end delay and energy consumption, etc. All the proactive and reactive protocol is difficult to maintain the performance in front of several parameters. The variation of performance of routing protocol is basically affected due to its weakness of MANETs as mentioned above.

There are different types of possible attacks in MANETs like external attacks and internal attacks [7]. The external attack is more vulnerable because those nodes that are not part of the network cause send the false routing information to the nearby nodes. This may cause the unavailability of services inside the network. In internal attacks, there are different compromised nodes are present that already part of the network to analyze the network congestion and traffic inside the network. To check the availability of the node inside the network the Denial of Service (DoS) attacks is also affected the whole performance of the network. Due to the DoS attacks, the constant mobility of the nodes does not understand these types of attacks. At the time of deployment of the network, the mechanism of authentication does not properly implement. The initial fake packets send towards the destination. Several passive and active attacks is also disturbed the quality of MANETs like eavesdropping. In this type of attack node simply observe the information about the network not confirm that the information is confidential or not. So in this way, the information further used for malicious attack purposes. Two types of routing attacks are also present in MANETs like routing protocol attack and attack on packet forwarding or delivery system. Congenitally, these attacks are called a black and grey hole attacks [8].

In black hole attack, the attacker advertises the zero metrics transferred to all destination and grey hole attack responsible the routing misbehavior which leads to dropping of messages. Jamming, replay attack, and man-in-the-middle attack and wormhole attack are the few examples. As the trend of wireless technology is increasing day-by-day the number of applications is also increased. A lot of applications of MANETs likes a military battlefield, commercial sector, Personal Area Network (PAN), Local Area Network (LAN), and MANET-VoVoN. A newly emerging field of MANETs is VoVoN, which has an extended version of peer-to-peer JXTA virtual overlay network. This application is used as a private signaling exchange protocol based on the portable exchangeable communication channel. Regardless of the application of MANETs, there are several challenges of MANETs like routing, security and reliability, quality of services, internetworking, power consumption and multicast behavior of the topology and location aided routing. These challenges become the dominant weakness of ad hoc networks like MANETs.

Most of the work of the MANETs network is simulation-based that does not provide the correctness and authentication of the solution. Formal Methods (FMs) provided the correctness and validation of the work, as we already done for our last articles like [9-12] and [22, 23-25]. For verification and validation, the formal methods help the assurance about the proposed work but also provide the way to extend the work in various direction. In this paper, FMs are used to explore the solution of MANETs challenges by using the Vienne Development Method-Specification Language (VDM-SL) toolbox [13-15]. So in this paper, we proposed the solution of various challenges by formal verification. The cluster-based approach is used to prevent all these types of attacks.

Up to our best knowledge, this work is a pioneer done to detect and formalize the few attacks on MANETs. Rest of this paper is organized as: section 2 deals the related work and section 3 and 4 presents the possible classifications of attacks and formal specification through VDM-SL Toolbox respectively. Section 5 describes the model analysis and the proof of the correctness. Finally, the conclusion is a deal in section 6.

2. Related work

With the increasing trend of MANETs networks, in this regard security has need much attention of researchers. In order to use the MANETs network in the future, there is a need to make safe and sound routing inside the MANETs. To adopt any security mechanism there is a need to get knowledge about all types of attacks and its working mechanism. There is a need of adopting some type of defense mechanism to prevent that all vulnerable attacks on MANETs [16]. There are many security mechanisms that are proactive and reactive in nature. A lot of different types of attacks such that passive and active in nature. In the passive category, there are two fundamental types eavesdropping and selfishness. The detail of the remaining attacks is discussed in Fig. 1.

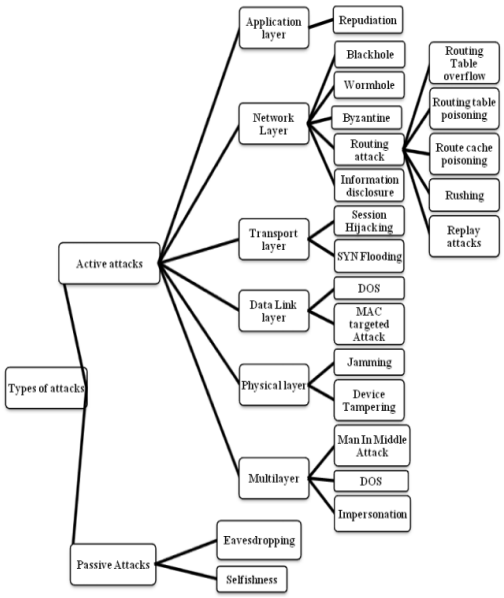

Fig. 1 Classification of attacks

In passive attacks: the attacker tries to snoop the network operation without disrupting the network operations to find out those nodes that are in promiscuous mode. Two techniques are used for this like eavesdropping and selfishness.

Eavesdropping: All the nodes share the wireless network; with its transmission range, nodes easily communicate with each other. By using encryption mechanism easily prevent this attack, because by encryption all the communication inside the nodes are safe and sound and does not be predicted by warm hands of the attacks. On the other hand, the selfishness nodes do not take part in the network communication. These nodes want to save battery and power resources so that any communication in the form of forwarding and receiving the packets will stop.

In active attacks: The word active means the properly disturbance of the communication of the network and its resources. In this way, the normal operations of the networks are easily disturbed by modified and tunneling the packets, replying and forwarding the data packets, fabricating the messages, etc. All these operations change the content of the messages that need to be forward from source to destination. Further classification of MANETs attacks is active attacks like external and internal attacks. The intention of internal attacks are disturbed the nodes within the network and the external attack has miss leading by the nodes that are not part of the networks. In different layers of MANETs different attacks are working it out. In the application layer, repudiation mechanism strongly workout with some kind of selfish nodes that disturb the network communication for a long time.

3. Classification of Attacks

***Hijacking techniques*:**

Also applied to hijack the network with the use of fake IP addresses. Firstly attackers find out the normal and correct sequence number that present inside the network [17]. After it spoofs the fake victim IP address. By hijacking the victim node it hangs the whole network communication easily. Fig. 2 easily elaborate on the concept of the hijacking mechanism. Usually, this type of attack is performed in the transport layer.

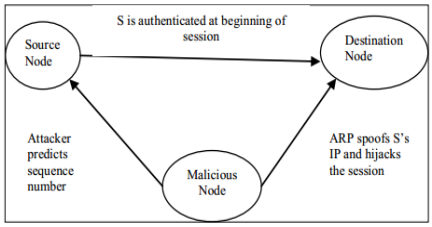

Fig. 2 Hijacking attack

***In synchronization flooding*:**

The nodes communicate with each other in the three-way handshaking mechanism. A particular node sends a large number of SYN packets to victim nodes. After receiving the SYN packets; the victim nodes send back to SYN+ACK packets. The attacker spoofs the returning ACK address and hijacks the network. In this way, the ACK does not send back to the particular node. All the information is hacked by this type of flooding attacks. Fig. 3 depicts this type of attack.

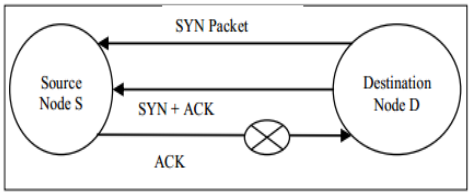

Fig. 3 SYN flooding Attack

The wormhole attack:

The most parlor attacks are wormhole attack, blackhole attack and grey whole attack. Usually found in the AODV routing protocol when node 'S' wants to communicate with 'D' then it further broadcast the RREQ to its nearby neighbors like A1 and X. A1 forward this request to A2, between A1 and A2 there is some kind of private channel. Note that the A1 and A2 are some kinds of colluding attackers. Further A2 forward the request to Z and then D. In this way the total route length from S to D is stored in the attacker's memory. So the entire traffic passes through the wrong path chosen instead of the right path chosen. Fig. 4 represents the best picture of this type of attack.

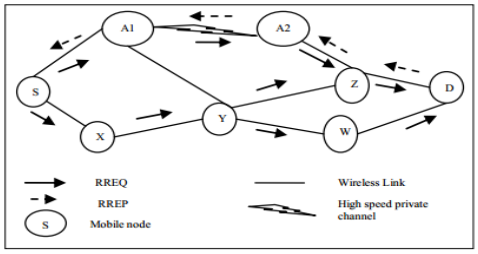

Fig. 4 Wormhole attack

***Black hole attack*:**

To advertise the short and optimal route for the victim is also an example of this type of attack. The main working of the blackhole attack is the presence of a malicious node inside the network. These malicious nodes are known as Blackhole. Fig. 5 shows the black hole attacks [18].

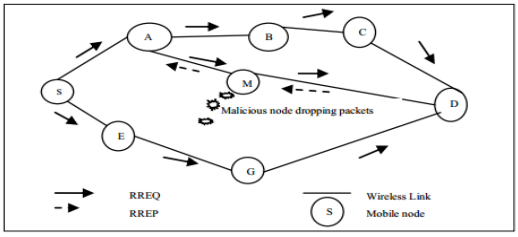

Fig. 5 Black hole attack

Byzantine attack:

To degrade the network performance the multiple attackers need to work in some collusion fashion like creating some kind of loops between source and destination. There are many factors that causing the loops such that choose a nonoptimal path, dropping packets, etc. It has been observed that in DSR the packet delivery ratio has been disrupting 90% of data packets [19]. Figure 6 illustrates the loop in a Byzantine attack.

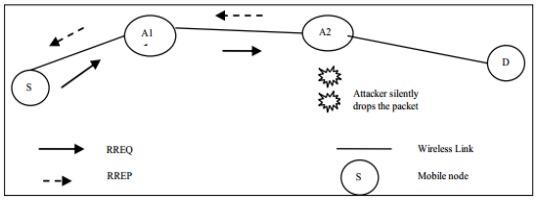

Fig. 6 Byzantine attack

The routing table is well maintained in AODV and DSR. To poising the route table with malicious and fabricated routing update to authorize node in the network. The attackers save the false route error messages and update the routing table with regular false route error. In a common example of sending the packets between source and destination, a malicious node' broke the link between the destination and itself by sending the RERR message then the brake line between the next node and destination node. So it can successfully stop the traffic between source and destination. For preventing the route table poisoning there is need some formal methods that check every pre and post condition before sending the packets towards the destination. Fig. 7 shows that the positioning of routing tale through M.

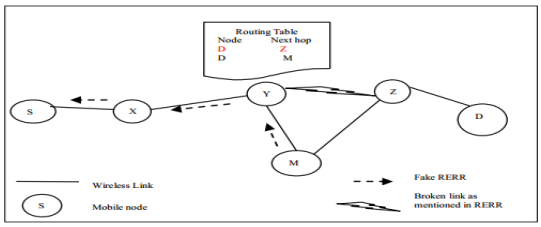

Fig. 7 Poising of the routing table

Different types of attacks have different strategies like in MANET nodes can be broken at some stage, due to broken nodes these are not functional forms that remaining the part of the network. With the status of broken nodes, these nodes are not forward the packets towards the destination. The malicious nodes try to disturb the network by packets drop and cause with denial of service attack.

Another most common attack in networking is a denial of service attack (DOS) [20]. DOS attack cannot need only one layer but this type of attack has enough capability to take multilayer for attacking the network. With a modified source route this is the common example in DSDV. The explicit effect of modified the selected source route has a long-lasting effect on the performance of the network. All the modified source route length is stored in a data packet header so it can be easily trapped all the routing information. In the following figure, M is a malicious node that wishes to launch a DoS attack in this route length from S to D. S want to communicate With D have an unexpired route in its cache. S transmits the data packet with the route length of S, X, M, Y, Z, and D. as data packet reaches at X position the M alter the source route by deleting any node like Z from the source route. So 'Y' receives the modified fake route, therefore, 'Y' move the packets 'Z' but d cannot hear 'Z' because 'Z' is not a part of route length so the whole transmission is failed. Fig. 8 shows the DoS attack.

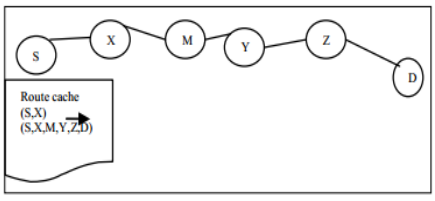

Fig. 8 DoS attack

Jellyfish attack:
The nature of the jellyfish attack is the same as the black hole attack in which malicious nodes need to attack the network while determining the order of packets, selection, and rejection of packets, jitter, and energy consumption to transmit the packets.

Rushing attack:
The most dangerous attack is a rushing attack when the source node does not know any secure route without the helping of the attacker. Due to attacker nodes already present in route length, therefore, it is difficult to pass the traffic toward the destination.

Replay attack:
The constant reply attack leads to the rapidly consuming energy and power resources of mobile nodes. So in this way, the congestion in the network can be increased.

Routing cache poisoning:
The concept of routing cache comes into existence with on-demand routing protocols like DSR etc. DSR usually stores all routes information in its routing cache, therefore cache overflow problem comes into existence. In this problem, a lot of lightweight routing algorithm has been proposed to resolve the issue of cache overflow with some threshold values inside the cache to some extent.

Device tampering:
In any type of ad hoc network, the size of nodes is small and hand-held unlike wired devices so it can easily damage. For this, there is a need to protect the formal mechanism to provide enough security to prevent the damaged and stolen of nodes.

Jamming:
To receive the packets from the sender and transmit it to the receiver is operated some suitable frequency. If this frequency traps by an attacker or the attacker it has enough frequency to travel the signal between the sender and receiver. So that the attacker has to perform signal jamming. Random pulses and noise are common problems in this regard. With the help of formal verification of frequency with suitable formal methods then this problem is easily solve-able. In this paper, we try to make formal verification of all possible problems and their sub-problems.

MAC targeted Attack:
In the ad-hoc network, all the nodes use wireless medium so medium access protocol (MAC) is used. To resolve the communication issue like contention and coordination, the attacker can disrupt the MAC procedure.

Routing table overflow:
Due to nonexistence nodes, the routing table has to be overflow with its required space. Malicious nodes play our role to overflow the routing table by sending the consecutive route request for non-existing nodes. With the help of apply formal methods its find out the occurrence of non-existing nodes. Hence the overflow of the routing table easily is solved.

Information disclosure:
Any compromised nodes that present in the network may violate the principle of security. To disclose all the information like passwords, a number of nodes in the network, private and public information about data packets, the location of nodes, optimal routes for authorized nodes, target nodes, and purpose of the network. by using formal verification all these credentials are to be secured in a well-disciplined manner.

Man-in-the-middle attack:
As the name comes the attacker sits between the sender and receiver and record all the information between them. In essence, the sender-receiver communicates each other but in actual they do not communicate with each other but they are talking to the man-in-the-middle who passes the message of the sender to the receiver. Here is described the defense mechanism of all possible attacks that are in proactive, reactive, passive, active and hybrid nature. Fig. 9 depicts the possible classification of defiance mechanism to secure the MANET.

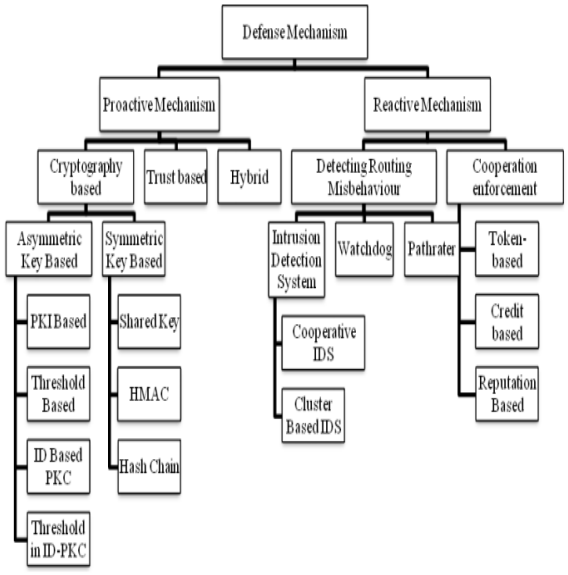

Fig. 9 Defence Mechanism for MANET [21]

4. Formal verification through VDM-SL

This section represents the formal specification of analysis of attacks on MANETs for wirelessly connected network to protect the network from the unauthorized user. This specification includes different types of composite objects, pre/post conditions, and some efficient and proactive operations that detect the attacks successfully. To provide protection to the network, secondary nodes are needed to be deployed at the cluster level. For this purpose, scattered topology is specified in each cluster in which nodes are

deployed that are far from each other. The scattered topology is represented in the form of composite objects that consists of three field's nodes, links, and range. The formal specification contains different types of nodes, modes, power, and links.

```
types
node = token;
Source node_id=token;
Destination node_ Id = token;
Sensor Modes = <SLEEP-MODE> | <ACTIVE-
MODE>;
N _Power = <high power> |<low power>;
Node:: Node_ id : Id : Node power : Power
Scattered Topology::node: nodes

Link: link
Range: range
connect: bool node position: int
attack_ information: Attack information;
link_Type = <Connected> | <Disconnected>
Link::Node1:Node
Node2:Node
inv mk_Link(node1, node2) == node1 <>
node2;

Communication::nodes:set of node
links: a set of links
inv mk_Communication(nodes, links) ==
forall links in set links &
li.node1 in set nodes and li.node2 in set
nodes and
forall node in set nodes & (exists li in
set links &
(node = li.node1 or node = li.node2));

values
LIMIT:nat=4;
```

MANETs consists of different types of nodes like a sensor, actor and mobile nodes which are wirelessly connected to each other to provide the basic functionalities in the network. These nodes have some common characteristics and are described through a composite object. The composite object against every node will be different according to the requirement. It contains different types of fields. There are some constraints that must be fulfilled before proceeding to the detection of attacks. **Invariants:** (1) The number of nodes should be less than the already defined fixed limit. Nodes length does not go above to the defined limit. (2) There should be a link between the nodes.

```
state MANET of
Mobility_nodes:set of nodes
node_edges:set of Edges
sensors: set of Sensor
ports:set of ports
cookies:set of cookies
session:set of sessions
loss_packets:set of packets
delay_packets:set of packets
Destination:set of nodes
cluster: set of Nodes
attack:set of malicious node
Backup_node:nodes

inv mk_MANET(nodes)== card nodes<=limit
invmk_MANET(mobile_nodes,node_adges,sensors
,loss_packet , delay_packet )
== forall edge in set node_edges &
edge.node1 in set sensor_node and
edge.node2 in set sensor_nodes and forall
kk in set sensors
init mk_MANET(nodes)==nodes={}
end
```

Active attacks are those attacks that directly harm the data or information of the network. The formal specification of an Active attack is specified as a composite object having a different number of fields. The *first field* shows the activities of the nodes when attacks occur. The *second field* shows the loss ratio that represents the number of packets that are loosed due to malevolent attacks. The *third field* accounts the deliverance time of the packets. The *fourth field* demonstrates the postponement between the nodes. To detect the attack proficiently, a unique secondary node is deployed in the network.

```
Active Attack = token; Node Behavior =
<ABNORMAL> |
<Data loss_ ratio> | <route failure> |
<unnecessary delay>;
Data :: b-data : int data : int;

DSensor :: as node : Node
m_sensor : set of malicious sensor  data :
Data
Abehavior: behavior
inv mk _ A Sensor(as_ node, sensor, data,
behavior) == for all an in set m_ sensor
an = node_ id and node_ mode = <ACTIVE>
<=> data. B_ data < BD_ data_ data or
data_ Bd_ data > data.  data => behavior =

<ABNORMAL> or behavior = <Data_ loss_
ratio> and
A_ behavior =<route_  failure> and
node. mode = <SLEEP> <=>
data. data=data. data=>A_
behavior=<ABNORMAL>;
```

Passive attacks are that attack that does not directly harm the network. These types of attacks are occurring due to open ports and network vulnerabilities. The purpose of the passive attack is not lost the information. Passive attacks only occur to gain some important information. The formal specification of a passive attack is specified as a composite object having a different number of fields. The *first field* shows the information about the nodes that are modified when attacks occur. The *second field* shows the nature of the attack that represents the number of packets that are corrupted due to malevolent attacks. The *third field* represents the deliverance time of the packets.

```
Passive Attack= token; Ground = token;
Location:: lug : Information-detail
_attacklg : Ground;

Passive_ Attack :: wp : int twp : int;
Passive_ attack_ Detected_ Sensor :: cd_ s_
node : Node
cdsdeployed : map set of Id to Location
attack :Passive_Attack
inv mk_ Passive_ Detected_ Sensor(wp_ s_
node, cd_ s_ deployed,
c_ attack) == for all n in set dom cds_
deployed
& n = {cdsnode.nid} and cdsnode.mode =
<ACTIVE> <=> cattack.cd >= cattack.twp
and cdsnode.mode = <SLEEP> <=>
cattack.wp < cattack.twp;
```

The network is divided into clusters to resolve the issue of the malicious attack in the network. The formal specification of a cluster head selection is represented below in which the head cluster node is selected by the neighboring nodes. The head node will be responsible to prevent the network at the cluster level. It will be able to detect the attack and run specific actions against the attack. These actions will be done according to the nature of the attack.

```
CH_ Head : : secondary : Secondary
s-neighbors : set of Node
inv mk_ CH_ Head (secondary , s-neighbors)


secondary. r nd not on set s-neighbors and
secondary. r Nd. conn «CONNECT» <=> s-
neighbors <> {}
and
secondary Nd. conn «DISCONNECT» <=> s-
neighbors
```

There are too many operations that are done to protect the network from unauthorized users. *The first operation* is the creation of the cluster. It contains a lot of mobile and sensor nodes. There are some pre and post-conditions for the creation of the clusters. The *second operation* is the creation of a sink node that will be able to receive the traffic of the whole network at a cluster level that makes the detection of the attacks too much easy. The *third operation* shows the creation of the secondary nodes. These nodes are the cluster head nodes that handle the attack at the cluster level and take actions according to the nature of the attacks. The *fourth operation* shows the creation of the sensor nodes these nodes are deployed to perform the basic functionalities of the network. These nodes sense information from the environment and transmit that information from source to the sink nodes at the cluster level. The *fifth operation* shows the creation of the backup nodes these nodes are deployed in the network to deal with the miserable situations in the network. These nodes come to action only when attacks occur on the network and some functional nodes are destroyed from it then these nodes take the charge of those destroyed node to make the network functional.

Pre-condition: (1) Cluster should not be present in the network before creation. (2) The secondary node should not exist in the cluster before creation. (3) Destination node should not exist in the network before the creation. (4) Sensor node should not exist in the network before the creation. (5) Backup nodes should not exist in the network before the creation.

Post-condition: Nodes will be added to the network.

```
Operations

create_cluster(NettId:Node)
ext wr cluster: set of Nodes
pre NetIn not in set cluster and card
cluster <LIMIT
post cluster= cluster~ union {NettIn};

create_Destination_node(NodeId:Node)
ext wr cluster: set of Nodes
pre NetIn not in set cluster and card
cluster <1
post cluster= cluster~ union {NodeIn};
post Destination= Destination~ union
{NodeIn};

create_Secondory_node(NodeId:Node)
ext wr cluster: set of Nodes
ext wr secondory: set of Secondory
pre NodeIn not in set cluster and card
cluster <LIMIT and
 NodeIn not in set secondory and card
secondory <LIMIT
post cluster= cluster~ union {NodeIn}
post secondory= secondory~ union {NodeIn};

create_sensornode(NodeId:Node)
ext wr cluster: set of Nodes
ext wr sensors: set of Nodes
pre NodeIn not in set sensors and card
sensors <LIMIT
post cluster= cluster~ union {NodeIn};
post sensors= sensors~ union {NodeIn};

create_Backupnode(NodeId:Node)
ext wr cluster: set of Nodes
ext wr sensors: set of Nodes
pre NodeIn not in set sensors and card
sensors <LIMIT
post cluster= cluster~ union {NodeIn};
post sensors= sensors~ union {NodeIn};
```

Detect Active Attack function detects the malicious attacks that are directly destroying the network take and loss the information and data in the network. It takes cluster id as an input checks the packet loss ratio and the unnecessary delay in the network. If the packet is loss and delay are exist in the network then secondary nodes that are the cluster head nodes take action against them.

Detect passive attack function takes the cluster id as input and finds out the passive attack in the network. It checks

the information that is sent by the source node to the sink node. It checks the ports and delays in the network if these are available in the network and information is altered then the secondary node takes it as a passive attack and takes action that is planned for the passive attacks.

```
Detect_Acctive_Attacks(clusterIn:cluster)qu
ery:bool
ext rd loss_packets:set of packets
ext rd delay_packets:set of packets
pre true
post query
<=>mk_Block(drop_packets,drop_packets) in
set data;

Detect_Passive_Attacks(nodeIn:nodes)query:b
ool

ext rd information:set of information
ext rd delay_packets:set of packets
ext rd ports:set of ports

post query <=>mk_Block
(drop_packets,drop_packets) in set
dataInformationl;
```

Detect black hole attack function detects the black hole attack in the network. It checks the unnecessary delay in the network. If it is existing then cluster head nodes take it as a black hole attack and take action against it. Detect wormhole attacks are appear on the network. These attacks are detected through the short circuits. If some shoot circuits exist in the network then head node takes it as wormhole attack and take action accordingly.

```
Detect Blackhole_ Attack(nodeIn:nodes)
ext rd delay_packets:set of packets
pre true
post query <=> nodeIn in set blackhole;

Detect wormhole Attack(nodeIn:nodes)
ext rd short_circuit:set of links
pre true
post query <=> nodeIn in set short_circuit;
```

Denials of service attacks occur at wireless adversary of the network and affect the packet delivery ratio of the network. To detect these types of attacks cluster head node read the wireless adversary and packet delivery ratio. If it is less than the actual ratio then the head node takes it as a DOS attack and take action against it. Session hijacking attack occurs on the session of the web pages it affects the routing path of the network and alters it. As a result, the packet does not reach a destination and packet loss ratio is detected. Cluster head node detects these types of attacks by measuring the routing path and loss ratio. If it is available then attack is detected and action is taken against them. Detect routing attacks are detected through the routing path. If it is vulnerable then attack is detected and action is taken against them.

```
Detect DOS Attock(clusterIn:cluster)
ext rd wireless_adversery:set of  emmiting
signal
ext rd pdr:packet ratio
post query <=> nodeIn in set emmiting and
pdr;

Detect
Session_Hijecking_Attack(clusterIn:cluster)

ext rd cookies:set of cookies
ext rd session:set of sessions
post query <=> nodeIn in set cookies and
sessions;

Detect Routing_Attack(clusterIn:cluster)
ext rd routing path:set of path
post query <=> nodeIn in set path
```

Vulnerabilities Solution Function is designed to resolve the issue of the vulnerary attack in the network. This function provides an efficient solution through round-trip time and backup nodes. This function replaces the vulnerable nodes with the backup nodes to maintain the functionality of the network.

```
Vulnerabilities_Solution(NodeIn:nodes)
ext rd round_trip_time: set of times
ext wr expected_round_trip_time: set of
times

ext rd sensors: set of Nodes
ext rd loss_packets:set of packets
ext rd delay_packets:set of packets

pre NodeIn exist in cluster and attack
post cluster= cluster~\ {NodeIn};
post attack= attack~union {NodeIn};
post Backupnode= Backupnode~\ {V_Id};
```

Total cluster Function returns the total number of the cluster in the network that will be very helpful for the detection of the failure cluster in the network. Establish a connection function is used to establish the connection between the nodes and the clusters. This function provides the wireless connectivity from the sensor to the sensor, sensor to node and destination node to destination nodes, etc.

```
TotalClusters()total:nat
ext rd cluster: set of Nodes

pre true
post  total= card cluster;

Establish_Connection(sensor_1:sensors,Secon
dory_1:Secondory,sink_1:sink)
create_pathway::sensor_1:sensor
Secondory_1:Secondory,sink_1:sink;

inv mk_Edge(sensor_1, Secondory_1,sink_1)
== sensor_1 <> Secondory_1<>sink_1;
```

5. Model analysis

The cluster-based technique is design and formalized under the umbrella of FMs. Some of the invariants are used for designing the formal specifications and pre/postconditions. These invariants play part and parcel role to make any type of formal specification into formal notations. To check the correctness, consistency and its integration among the module correctly, VDM-SL provides the platform in this regard. The VDM-SL toolbox provides support to check all the related invariants in a different mode.

To check all the composite objects, state, function, and operations the VDM-SL checking window provides the syntax check, type check, pretty and integrity check. All the simulation work does not provide the correctness of the model, technique, and algorithm but FMs are enough flexible and give the proof of the proposed technique or algorithm that is design inside the tool box.

Table 1 and fig. 10 describe the verification of the model against all related possible functions. It ensures that the proposed design specification is correctly verified and validated.

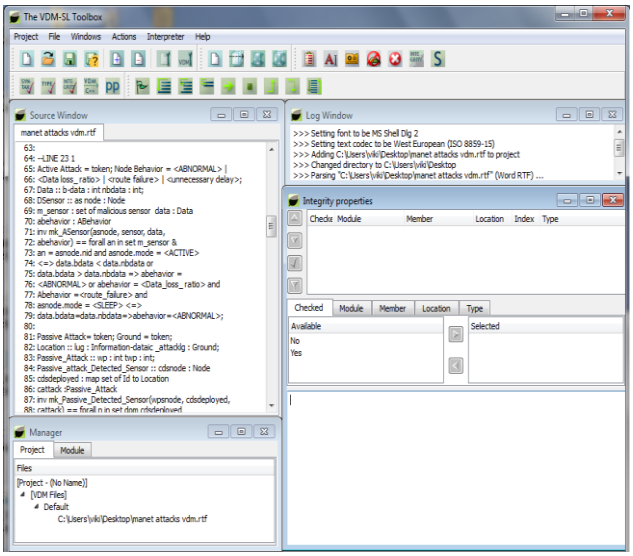

Fig. 10 Proof of correctness

Table 1: Analysis Of Structure, Operation, And State

Parameters of Different objects	Semantic Check	Sequence Check	Mode testing	Function testing
Connections	ok	ok	ok	ok
Detection	ok	ok	ok	ok
External/Internal Attacks	ok	ok	ok	ok
Active & Passive Attacks	ok	ok	ok	ok
Cluster Heads	ok	ok	ok	ok
Operator	ok	ok	ok	-
Attacks defined	ok	ok	ok	-
Node Sequence	ok	ok	ok	-
Cluster	ok	ok	ok	-
Option	ok	ok	ok	-
Modes	ok	ok	ok	-
Sessions	ok	ok	ok	ok
Functions	ok	ok	ok	ok
Active & Sleep	ok	ok	ok	ok
Links & Edges	ok	ok	ok	ok
Mobility nodes	ok	ok	ok	ok
Implementation	ok	ok	ok	ok
Possible conditions	ok	ok	ok	-
Validity	ok	ok	ok	-
Total Clusters	ok	ok	-	-
RTT	ok	ok	-	-
S/A Field	ok	ok	-	-

6. Conclusion

Mobile Ad-hoc Networks (MANETs) have become one of the most popular research areas due to its wide variety of applications. Rapid advancement in the ad-hoc network creates a need to secure this type of network against different attacks. It is because of, indeed; the secure network has a great impact on overall performance and quality of the services (QoS) parameters like communication delay, packet delivery/loss ratio and bandwidth. With the increasing trend of MANETs networks, security has need much attention of researchers. In order to use the MANETs network in the future, there is a need to make safe and sound routing inside the MANETs. Most of the work of the MANETs network is simulation-based that does not provide the correctness and authentication of the solution. Formal Methods (FMs) provides the correctness and validation of the work. For verification and validation, the formal methods helps the assurance about the proposed work but also provide the way to extend the work in various direction. In this paper, FMs are used to explore the solution of possible MANETs attacks by using the VDM-SL toolbox. It has been observed that, from proof of correctness window all types of attacks are formally verified with its pre/post conditions.

Acknowledgment

The authors would like to express their cordial thanks to Dr. Tariq Ali Gill for his valuable advice.

References

[1] Nadeem, A., & Howarth, M. P. (2013). A survey of MANET intrusion detection & prevention approaches for network layer attacks. IEEE communications surveys & tutorials, 15(4), 2027-2045.

[2] Kannhavong, B., Nakayama, H., Nemoto, Y., Kato, N., & Jamalipour, A. (2007). A survey of routing attacks in mobile

ad hoc networks. IEEE Wireless communications, 14(5), 85-91.
[3] Rahman, A. H. A., & Zukarnain, Z. A. (2009). Performance comparison of AODV, DSDV and I-DSDV routing protocols in mobile ad hoc networks. European Journal of Scientific Research, 31(4), 566-576.
[4] Ogier, R., Templin, F., & Lewis, M. (2004). Topology dissemination based on reverse-path forwarding (TBRPF)(No. RFC 3684).
[5] Clausen, T., & Jacquet, P. (2003). Optimized link state routing protocol (OLSR) (No. RFC 3626).
[6] Pathan, A.-S.K., Security of self-organizing networks: MANET, WSN, WMN, VANET. 2016: CRC press.
[7] Patel, M., & Sharma, S. (2013, February). Detection of malicious attack in MANET a behavioral approach. In 2013 3rd IEEE International Advance Computing Conference (IACC) (pp. 388-393). IEEE.
[8] Kaur, R., & Singh, P. (2014). Review of black hole and grey hole attack. The International Journal of Multimedia & Its Applications, 6(6), 35.
[9] Draz, U., Ali, T., Yasin, S., Waqas, U., & Rafiq, U. (2019, February). Towards Formalism of Link Failure Detection Algorithm for Wireless Sensor and Actor Networks. In 2019 International Conference on Engineering and Emerging Technologies (ICEET) (pp. 1-6). IEEE.
[10] Draz, U., Ali, T., Yasin, S., Waqas, U., & Rafiq, U. (2019, February). EADSA: Energy-Aware Distributed Sink Algorithm for Hotspot Problem in Wireless Sensor and Actor Networks. In 2019 International Conference on Engineering and Emerging Technologies (ICEET) (pp. 1-6). IEEE.
[11] Draz, M. U., Ali, T., Yasin, S., & Waqas, U. (2018, December). Towards Formal Modeling of Hotspot Issue by Watch-Man Nodes in Wireless Sensor and Actor Network. In 2018 International Conference on Frontiers of Information Technology (FIT) (pp. 321-326). IEEE.
[12] Ali, T., Yasin, S., Draz, U., & Ayaz, M. (2019). Towards Formal Modeling of Subnet Based Hotspot Algorithm in Wireless Sensor Networks. Wireless Personal Communications, 1-34.
[13] Riaz, S., Afzaal, H., Imran, M., Zafar, N. A., & Aksoy, M. S. (2015). Formalizing mobile ad hoc and sensor networks Using VDM-SL. Procedia Computer Science, 63, 148-153.
[14] Afzaal, H., Imran, M., & Zafar, N. A. (2015, December). Implementing partitioning detection and connectivity restoration in WSAN using VDM-SL. In 2015 13th International Conference on Frontiers of Information Technology (FIT) (pp. 71-76). IEEE.
[15] Chandra, A., & Thakur, S. (2015). Qualitative analysis of hybrid routing protocols against network layer attacks in MANET. Apoorva Chandra et al, International Journal of Computer Science and Mobile Computing, 4(6), 538-543.
[16] Gokhale, V., Ghosh, S. K., & Gupta, A. (2016). Classification of attacks on wireless mobile ad hoc networks and vehicular ad hoc networks. Security of Self-Organizing Networks, 195.
[17] Ponsam, J.G. and R. Srinivasan, A survey on MANET security challenges, attacks, and its countermeasures. International Journal of Emerging Trends & Technology in Computer Science (IJETTCS), 2014. 3(1).
[18] Pathan, A.-S.K., Security of self-organizing networks: MANET, WSN, WMN, VANET. 2016: CRC press.
[19] Anbarasan, M., Prakash, S., Antonidoss, A., & Anand, M. (2018). Improved encryption protocol for secure communication in trusted MANETs against denial of service attacks. Multimedia Tools and Applications, 1-21.
[20] Mathur, A., Newe, T., & Rao, M. (2016). Defence against black hole and selective forwarding attacks for medical WSNs in the IoT. Sensors, 16(1), 118.
[21] Draz, U., Ali, T., Yasin, S., & Shaf, A. (2018, March). Evaluation based analysis of packet delivery ratio for AODV and DSR under UDP and TCP environment. In 2018 International Conference on Computing, Mathematics and Engineering Technologies (iCoMET) (pp. 1-7). IEEE.
[22] Shaf, A., Ali, T., Draz, U., & Yasin, S. (2018). Energy Based Performance analysis of AODV Routing Protocol under TCP and UDP Environments. EAI Endorsed Trans. Ener
[23] Draz, U., Ali, T., & Yasin, S. (2018, November). Cloud Based Watchman Inlets for Flood Recovery System Using Wireless Sensor and Actor Networks. In 2018 IEEE 21st International Multi-Topic Conference (INMIC) (pp. 1-6). IEEE.
[24] Draz, M. U., Ali, T., Yasin, S., & Waqas, U. (2018, December). Towards Formal Modeling of Hotspot Issue by Watch-Man Nodes in Wireless Sensor and Actor Network. In 2018 International Conference on Frontiers of Information Technology (FIT) (pp. 321-326). IEEE.
[25] Maulik, R. and N. Chaki. A comprehensive review on wormhole attacks in MANET. in Computer Information Systems and Industrial Management Applications (CISIM), 2010 International Conference on. 2010. IEEE.

Umar Draz received Bachler's degree from BZ University and a Master degree from COMSATS University Islamabad in 2013 and 2018 respectively. Currently, he is serving as Senior Lecturer at GC University Faisalabad, Sahiwal Campus. He worked as a distinguished Youngest Master Trainer (MT) at Govt. Elementary Teaching Training Collage, Sahiwal and Visiting Lecturer at University of Central Punjab (UCP), JV PMAS ARID University Sahiwal Campus. He has received Best presenter and research paper award from several IEEE international conference. In addition; recently he received World Best Paper Award from La-Taroob University Australia in 1st World Conference. As a co-founder of NetCom Lab, done several research projects of wireless communication with Dr. Tariq Ali. Recently, he joined the different international conference as permanent TPC member and guest editor. He has more than 30 research publications in international reputed journals and conferences under the umbrella of Dr. Tariq Ali. Currently, his research specialization area belongs to Terrestrial and Underwater networks, Li-Fi communication and IoT.

Tariq Ali received his Ph.D. in IT from University Teknologi PETRO-NAS, Malaysia in 2015 and his M.S. degree in Computer Science from SZABIST Islamabad Pakistan in 2006. During M.S his specialization area belongs to Networks and Communication. He worked as a Lecturer at the computer science department of Gordon College, Rawalpindi, Pakistan from 2007 to 2009. He has served more than 2 years as an IT-Manager for the IT Department of Govt. Pakistan. He is currently the Assistant Professor and In-charge in the Computer Science Department of COMSATS University Islamabad, Sahiwal. He was also a founder of NetCom Lab and Editor-in-chief of different reputed journals. During Ph.D., his specialization area belongs to Underwater Wireless Sensor Networks (UWSN). His research interests include mobile and sensor networks, routing protocols and underwater acoustic sensor networks.

Khurshid Asghar is working as Assistant Professor/Head Department of Computer Science University of Okara, Pakistan. Dr. Asghar worked as a research associate for one year at Cardiff School of Computer Science and Informatics, Cardiff University, UK. He earned his Ph.D. (Computer Science) from COMSATS University Islamabad, Lahore Campus in the field of artificial intelligence. His current research interest includes image processing, image forensics, video forensics, machine learning, deep learning, network security, biometrics, medical imaging, and brain signals.

Asis Jamal has done his MS from the USA. He is currently working as an Assistant Professor and In-charge CS at Barani Institute of Sciences a JV PMAS ARID University Sahiwal Campus. His Research interests broadly span the areas of Computer Graphics, including Computer Aided Geometric Design, Data Visualization, Geometric Modeling, Reverse Engineering of Images, Path Planning, Robotics, Computer Vision, and Digital Image Processing.

Aimen Anum is doing her MS Computer Science from Comsats University Islamabad, Sahiwal Campus and received her BS degree from Islamia University of Bahawalpur, Bahawalnagar. Her area of interest is Distributed Systems, Cloud Computing and Computer Networks.

Sarah Javed,is currently a student of the Final semester of Her MSCS from the COMSATS University Islamabad Sahiwal Campus. She also had been working as a Lab Engineer at BARANI Institute of Sciences Sahiwal. Her research area is Software Defined networks, machine learning, and information security /cyber security.

Sana Yasin received bachelor's degree from COMSATS University Islamabad, Sahiwal in 2016 and received Master degree (MSCS) at COMSATS University Islamabad as a highest CGPA. Currently, she is serving as Senior Lecturer at GC University Faisalabad, Sahiwal Campus since 2017. She is also a co-research partner in several projects of wireless communication at NetCom Lab. She has more than 25 publications in reputed journals and conferences. She received fully funded educational scholarships (two times) for her higher study from the government of Islamic Republic of Pakistan. Her research interest includes wireless communication, wireless routing protocols, Underwater Wireless Sensor Networks (UWSNs) and Bioinformatics Big Data.