J. Appl. Environ. Biol. Sci., 8(1)14-22, 2018

ISSN: 2090-4274
Journal of Applied Environmental and Biological Sciences
www.textroad.com

Formal Analysis of Malicious Attacks of Ad Hoc Distance Vector Protocol in Mobile Ad-hoc and Sensor Networks (MAHSNs)

Sana Yasin[1], Tariq Ali[1], Umar Draz[1], Low Tan Jung[1], M. Ayaz[2]

[1]CS. Department, (CIIT) Sahiwal, Pakistan
[2]Communication & sensor centre, UOT, KSA

Received: September5, 2017
Accepted: November 18, 2017

ABSTRACT

Mobile ad hoc and sensor networks (MAHSNs) are an infrastructure less network. The nature and organization of such networks make it attractive to various types of attackers. Attackers use different approaches to degrade the network performances like minimization in throughput, unnecessary delays, packet delivery ratio etc. The main focus is security issues which are necessary to provide secure communication not only for intra networks but for internetwork also. Security issues occur due to no central authority for the supervision of individual nodes. Security is a big challenge for the Ad hoc networks. In this paper, a novel formalized Attack Detection Model (ADM) is introduced for the security assessment of AODV protocol under malicious attacks. This model detects the attacks on the data traffic and control system of the network, efficiently. For the verification and validation purposes, Vienne development Method-Specification Language toolbox is used.
KEYWORDS—MAHSN; ADM; Attacks; VDM-SL, security attacks; Verification & Validation

I. INTRODUCTION

A mobile ad-hoc and sensor network (MAHSN) is a self-schedule network that consists of mobile nodes. In mobile ad hoc network (MAHSN) each node performs the dual functionality, host and a router to create the secure route to sink. MAHSN is getting more intension due to their wide range of applications in several areas. Security as a severe problem, the nature of ad-hoc networks makes them exceedingly defenseless to adversary's malicious attacks. Wireless links in MAHSN cause to be vulnerable attacks of various types like a black hole, gray-hole, and jellyfish attacks. These attacks occur on the data of the MAHSN [1-2]. Unlike wired networks where an adversary must gain a physical access to network wires or pass through several lines of defense at firewalls and gateways, attacks on the mobile ad-hoc network can come from all directions and target at any node. Compared to traditional wired networks (a network in which network traffic could be monitored at central devices such as switches and routers), mobile ad-hoc networks have no network concentration points to filter traffic. The use of wireless links, lack of fixed infrastructure and the characteristic of dynamic topology associated with ad-hoc networks make it impossible to use wired network security mechanism. Figure 1 represents the layout of MAHSN.

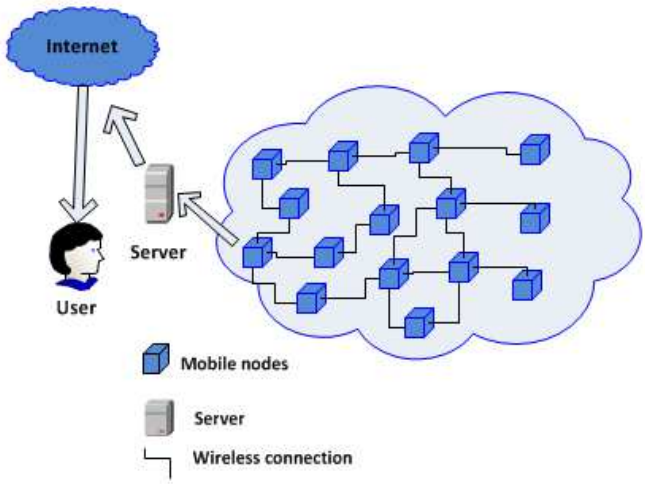

Fig. 1: Representation of Mobile ad-hoc & sensor network.

***Corresponding Author:** Sana Yasin, CS. Department, (CIIT) Sahiwal, Pakistan. Email; Sanayaseen42@yahoo.com

Every node in the network wants secured communication and reliable data delivery. Therefore, its need to provide the efficient architecture to secure the possible communication inside the network with the help of novel specifications like VDM-SL. By reviewing the extensive literature it is found that there is a lot of existing attacks that have similar features to each other's and classified into two different types of attacks based on their differentiation. The wicked nodes can attack in MAHSN using diverse behavior, such as transferring bogus messages for numerous periods of time, false routing information, and promoting bogus links to disorder routing operations.

In this paper, a formalism approach is introduced to detect and eliminate the attacks that are occurring on the data and control traffic on the network. In this approach, data control packets are placed in order to detect malicious nodes in a path. By use of data control packet, this approach detects all wicked nodes in the network and eliminates them by low packet overhead and delay. Furthermore, it increases network throughput by dividing all malicious nodes. MAHSN have several vulnerabilities that have the biggest flaw in the mobile ad-hoc network. It occurs due to the unauthorized data manipulation. A specific system may be vulnerable because it allows the data and control access without verifying the user's identity. The mobile ad-hoc network is extra vulnerable than a wired network. Some vulnerabilities of MAHSN are as follows (i). Unavailability of Central Point, there is no central management to monitor and manage the activities in MAHSN. Due to the absence of the central management, it is too much difficult to detect the attacks in highly dynamic and large-scale mobile ad-hoc network. (ii). Scalability is a major issue in MAHSN which causes several security issues in the network. Due to mobility, Topology of ad-hoc network changing all the time which make the network unsalable. (iii). Limited power nodes in MAHSN consume too much power due to self-scheduling and self-management which is a very limited resource. It's a root cause of several other issues in the network. Through the classification of Attacks, MAHSN attacks can be categorized into two main categories: Data traffic attacks and control traffic attacks.

Rest of this paper organized as section II describes the literature work. The high-level pseudo code of the proposed model and its algorithm is a deal in section III. Section IV presented the formal specification of the attacks and its algorithm. The formal soecification using VDM-SL is disscused in section V. the model anaylsis with proof of correctness and conclusion is discussed in section VI and VII.

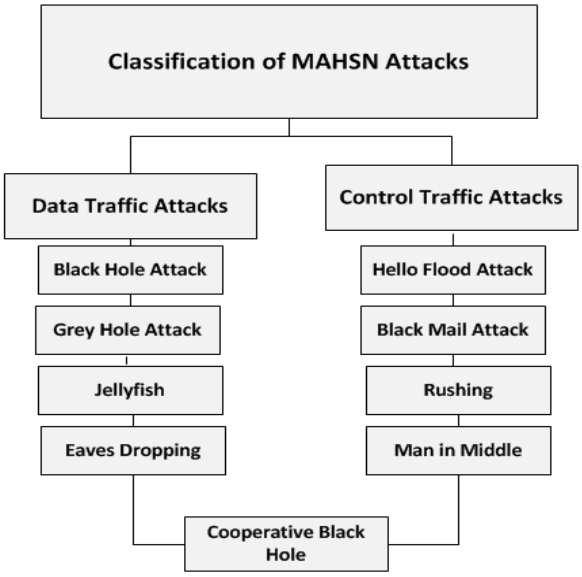

Fig. 2: Classification of MAHSNs Attacks

II. LITERATURE REVIEW

In literature, many techniques for the detection and elimination of attacks in MAHSN are proposed. In [1] MAHSN attacks are detected by using a secure zone routing protocol (SZRP). This protocol based on competent safe neighbor detection, protected routing packets, the discovery of malicious nodes, and preventing these nodes from demolishing the network. In [2] combating resource consumption and byzantine attacks is detected in MAHSN by adding alarm packet in the cooperative based detection scheme (CBDS) technique and name it Enhanced CBDS technique. In [5] wormhole attack is detected by taking a different type of protocol like DSDV, SEAD, and DSR. In [6] purposed a new technique that is based on the confirmation of the path. In this technique, the new best path is established by using the second path. It sends a confirmation packet when source node receives a route reply packet through the second best path to the goal. If the goal node has no route to these nodes, RREP generator, and its

Next-Hop-Node both will be considered as malicious nodes. This technique is very suitable if malicious nodes are less than two but in the case of more than two malicious nodes, this technique is useless. In [7] according to the survey the MAHSN security challenges and its countermeasures has been eleabroate in a well deciplined manners. All the efficient and proactive solution that has been done against these attacks is effectively discussed in this paper. In [8] denial of service attack is mitigating in MAHSN by incentive packet filling approach. This approach uses digital signatures to verify legitimate and drop packets that do not pass the confirmation. In [9] historical evidence-based trust management technique is purposed against black hole attack in MAHSN. Different strategy tries to stable the hope values from diverse neighbor nodes to alleviate the damage by their deceiving. In [10] author analyze the Black Hole attack by using AODV protocol and observe the packet drop ratio due to this attack. In [11] deal with the security of the network.

Deals with the comparison of proactive and reactive protocol in the mobile ad-hoc network, it has been observed that all the MAHSN protocols are based upon routing properties. Detection of sinkhole attack through AODV protocol is done in [13]. Firstly the effect of sinkhole attack is detected on AODV protocol then an efficient mechanism is purposed to remit this issue. In [14] security is provided to ad-hoc mobile distance vector AOMDV protocol with elliptic curve cryptography. Elliptic curve technique supplies security that has smaller key size with compared to other public key encryption. Configuration is also done on three different types of the environment using discrete event network simulator NS-2.35. In [15-17] attack detection techniques are used that detect the attacks in the network efficiently. In these papers, a different type of attacks are detected and prevented by using reverse trip time hop count, and link length between the nodes. It firstly detects the presence of malicious attack through from the hop count actual and then reverse trip time is determined and the comparison is done to calculate the calculated reverse trip time which provides a base to detect the attacks nodes through link length. The performance of the network is evaluated by the NS2 simulator which shows the improved value of throughput and packet delivery ratio [18]. Malicious attacks are a very critical issue in MAHSNs. Several improvements are made to resolve this issue but still, there is a rigorous need to work in this area. It occurs due to lack of security and flexible nature of the network. It can occur in any place in the network. Due to the malicious attacks, several problems occur in the network like network lifetime, unnecessary delays, packet drop ratio, throughput congestion etc that's why conventional attack detection problem requires a formalized solution that resolves this issue more efficiently.

III. FORMAL SPECIFICATION OF ATTACK DETECTION MODEL

This section represents the new purposed Attack detection model to detect the malicious attacks in the MAHSNs. This model based on the subnetting technique with actor head nodes that detect the attacks efficiently. After following the specific steps of the purposed model output will be achieved. In figure 3 the model is described that will be able to detect the attacks efficiently.

Attacks Detection Model ():
Begin
Step 1: Initiate the network and divide the whole network into small subnets with actor head nodes and each actor have some nodes
Step 2: The actor is selected based on election algorithm
Step3: Each node stores the information of its neighbor in its neighbor table
Step4: Source node S1 sends a HELLO packet to the intermediary node with destination node ID and actor ID
Step 5: **S1** starts timer, initializes **T1**
Step 6: When S1 gets acknowledgement from destination node stop timer, **T2**
Step 7: The expected round trip time is computed as **Tr = T2-T1**
Step 8: Source provides a unique sequence number to each packet and this number is known to Source, destination and actor head node only.
Step 9: Source node S sends a packet to destination node
Step 10: S starts timer TP1
Step 11: When S get acknowledgement from destination node stop timer, TP 2
Step 12: The round trip time is calculated as **Te = TP2 – TP1**
Step 13: If **Tr << Te**
Step 13.1: Inform actor head node
Step 13.2: The actor head node checks number of packet send by source node and number of packet receive by destination node.
Step 13.3: x = no of sent packet – n = no of received packet.
Step 13.4: If x > n then inform the source node to stop packet transfer.
Step 13.5: The source node stop packet transfer and inform the actor head node of outer layer to inform other actor head nodes.
Step 13.6: Actor head node discards that path and establishes a new path.
Step 14: Else Step 14.1: The actor head node calculates x.
Step 14.2: If x is not zero then go to Step 13.1
End.

Fig. 3: Semi-formal specification of ADM

IV. ALGORITHM OF ATTACKS DETECTION MODEL

The proposed algorithm against the high-level pseudo code of the security assessment model is presented in Fig. 4. Several nodes are deployed in the form of subnets (line1) with actor head nodes that are selected through the selected algorithm. Source node S1 sends the hello message to all the intermediately nodes with actor and destination ID and start the Timer T1 (line 2-3).When the source node S1 receives the acknowledgment from the destination node it stops timer T2 and calculates the round trip time (3-5). Source node S1 again send a message to intermediate nodes and after receiving the acknowledgment by the destination node stop timer T2 (line 6-8). It did the comparison between the expected turnaround time and actual turnaround time. If the actual turnaround time is less than the expected turnaround time then attack is detected. Source node informs the all actor head nodes. They stop the packet transfer and established a new path for the transmission.

Algorithm1. The pseudo code of the Attack Detection Model

INPUT: *Mobile adhoc and sensor network with malicious nodes.*
OUTPUT: *malicious node free network*
Initiate the subnet based network with Actor head nodes that are selected through elected algorithm.

1. $\forall$ *intermediate nodes* M_k *for* $K = 1,2,\ldots\ldots n$
2. *Hello message (Di,Ai) //Send hello message with Destination &Actor id*
3. **S1** starts timer, initializes **T1**
4. Get Acknowledgement() → stop timer, **T2**
5. Compute Round trip time() → **Tr = T2 – T1**
6. S starts timer TP1
7. Packet Acknowledgement() → stop timer, **TP 2**
8. **Te = TP2 – TP1**
9. If **Tr << Te**
10. Inform actor()
11. Check Packets(Si,Di) // Si=source node Di=Destination node
12. Z= x –n // number of sent packet – n = number of received packet.
13. If x > n
14. stop packet transfer (Ai) // inform actor head node to stop transfer
15. Discard path(Pi,Pn) //Pi = malicious path Pn=New established path
16. *This process continues until all the malicious node will be removed*
17. ***End if***

Fig. 3. The High-level pseudo-code for Security Assessment

V. FORMAL SPECIFICATION USING VDM-SL

In this section formal specification of the security assessment model of AODV protocol is illustrated by using VDM-SL. Several composite objects, sets, invariants pre postconditions are used for the maturity of the formal specification. The static and vibrant models are defined for the detection of the attacks in MAHSNs. The static model includes the different types of attacks while the dynamic model specifies the state and operations that are required to identify properly which attack is on the data traffic of the network or which is on the control traffic of the MAHSNs network. Figure 5 illustrates the sample connected MAHSNs network. Table 1 represents the hop to hop connections.

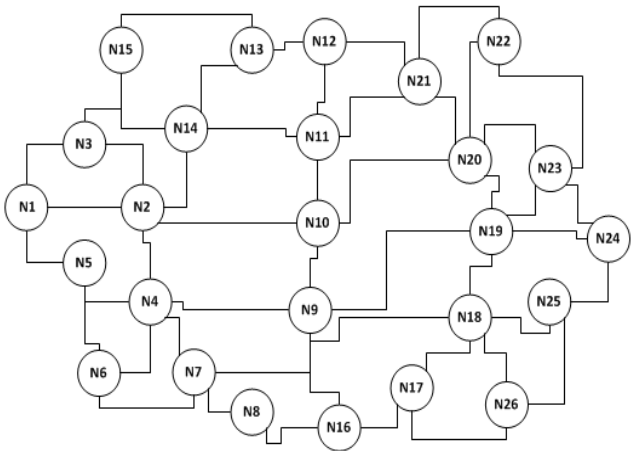

Fig.5: A sample connected MAHSNs

Table1. 1-Hop, 2-Hop and 3 Hop Connection list of N1

1-Hop Connection List	2-Hop Connection List	3-Hop Connection List
N1-N2	N1-N2	N1-N2
N1-N3	N1-N3	N1-N3
N1-N5	N1-N5	N1-N5
	N2-N3	N2-N3
	N2-N14	N2-N4
	N2-N4	N2-N10
	N2-N10	N2-N14
	N3-N14	N3-N15
	N5-N4	N3-N14
	N5-N6	N5-N4
		N5-N6
		N4-N5
		N4-N6
		N4-N7
		N4-N9
		N14-N11
		N14-N15
		N14-N13

MAHSNs consist of different type of mobile actor and sensor nodes which have some basic common characteristics and are described with the help of a composite object. Composite object *node* contains six fields. *Node_id that is the first field* indicates the distinctive identifier of a node. Node *mode that is the second field of the composite object* shows either node inactive or in sleep. The third field shows the power *of the node whether it is high or low*. The fourth field *connected* is used to find out either a node is connected or not. Position field that is the fifth field of the composite object report the position of a node. The *attack info field* is used for the detection of the attacks in the networks.

types node = **token**;
Source_id=**token**;
Destination Id = **token**; Sensor *Mode* = <SLEEP> | <ACTIVE>;
Node _Power = <HIGH> |<LOW>;
***Node :: Node**_id : node mode : Node power : Power*
connected : ***bool position*** *: int attack info: Attack info;*
Connection_Type *= <CONNECTED> | <DISCONNECTED>*
Link::node1:node
node2:node

The connection between the two nodes is described by a *Link* and the relationship of the whole network is described by the *Link* relation. Two nodes can communicate only if they have a symmetric relation between them. Any two nodes n1, n2 in the network can do communication if n1 have symmetric relation with n2. In this specification, no node is connected to itself which represent that there is no circuit or loop in the network.

inv mk_Link (node1, node2) == node1 <> node2;
Infrastructure::nodes:set of node
links: a set of links
inv mk_Infrastructure *(nodes, links) ==* ***forall*** *links in set links &*
li.node1 in set nodes and li.node2 in set nodes and
a forall node **in set** nodes & (**exists** li **in set** links &
(node = li.node1 **or** node = li.node2));
values
LIMIT:nat=4;

A subnet *SBHead* is declared with two fields. A subnet the head is assumed as actor head node which is specified by the field *actor*. The field *s-neighbors* show that an actor head node has neighbor nodes. Invariants: (1) A subnet head is identified as a unique node. (2) A subnet head actor node is connected to the network if and only if the neighbors set are non-empty, otherwise, it is disconnected.

SBHead : : *actor* : *Actor*
s-neighbours : set of *Node*
inv *mk* *SBHead(actor , s-neighbours)*
actor . r nd not in set *s-neighbours* and
actor.r nd.conn **«CONNECT»** <=> *s-neighbours* <> {}
and
actors.r nd.conn **«DISCONNECT»** <=> *s-neighbours*
{} ;

The formal specification of a Data traffic attack is specified as a composite object having four fields. The first field behavior shows the behavior of the nodes when attacks occur. The second field Drop ratio shows the number of packets that are dropped due to malicious attack. The third field PDR records the delivery time of the packets. The fourth field Delay shows the delay between the nodes. To detect the attack efficiently, a unique sensor node is attached. The node is active if and only if the attack is detected. The sensor stops sensing and takes another path for data transmission if the attack is detected. If above indication is not truly identified, then node remains in the sleeping mode

Data Traffic Attack = **token**; *ABehavior* = <ABNORMAL> |
<Drop ratio> | <PDR> | <Delay>;
Traffic :: *bttaff* : **int** *nbtraff* : **int**;
DSensor :: *as node* : *Node*
m sensor : **set of** *malicious sensor traff* : *Traff*
abehavior : *ABehavior*
inv mk_*ASensor*(*asnode*, *sensor*, *traff*,
abehavior) == **forall** *an* **in set** *m_sensor* &
an = *asnode.nid* **and** *asnode.mode* = <ACTIVE>
<=> *traff.btraff* < *traff.nbtraff* **or**
traff.btraff > *trff.nbtraff* => *abehavior* =
<ABNORMAL> **or** *abehavior* = <Drop ratio> **and**
Abehavior =<PDR> **and**
asnode.mode = <SLEEP> <=>
traff.btraff=traff.nbtraff=>abehavior=<ABNORMAL>;

Sensor node that detecting an attack on the control traffic is defined as a composite objects Control _Attack which consist of three numbers of fields. The first field cdsnode take the control of the node object. The second field cdsdeployed indicate a number of nodes that are deployed in control area. The field cattack is used to control the attack when an attack occurs on the control. The control attack sensor is active if and only if the attack occurs otherwise it always remains in sleep mode.

Control Traffic A ttack= **token**; *Id* = **token**;
Location :: *lug* : *control-traffic attacklg* : *Id*;
Control_Attack :: *wp* : **int** *twp* : **int**;
Control Detected Sensor :: *cdsnode* : *Node*
cdsdeployed : **map set of** *Id* **to** *Location*
cattack : *Control_Attack*
inv mk_*Control Detected Sensor*(*wpsnode*, *cdsdeployed*,
cattack) == **forall** *n* **in set dom** *cdsdeployed*
& *n* = {*cdsnode.nid*} **and** *cdsnode.mode* =
<ACTIVE> <=> *cattack.cd* >= *cattack.twp*
and *cdsnode.mode* = <SLEEP> <=>
cattack.wp < *cattack.twp*;

Three types of MAHSNs nodes is used in this model. These nodes are connected to each other through a wireless connection. There are some invariants in this model that must be fulfilled throughout the model. ***Invariants:*** *(1)* The cardinality of the nodes must be less than the pre-defined limit. It does not exceed the defined limit. *(2)* There must be wireless edges between the actor, sensor and mobile nodes.
Initializations: MAHSNs nodes should be empty before initialization of the model. There should be not any type of node in the network before modeling.

state MAHSN of
Mobile_nodes:set of nodes
node edges:set of Edges
sensors: set of Sensor
drop_packects:set of packets
delay packets:set of packets
*sink:**set of nodes***
*subnetId:**subnet***
*inv mk MAHSN(nodes)== **card** nodes<=**LIMIT***
inv mk_MAHSN(mobile_nodes,node_adges,sensors,drop_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 MAHSN(nodes)==nodes={}
end

There are multiple operations that are done in the purposed model to detect the different type of malicious attacks in MAHSNs. Detect Data _traffic _Attack function take subnet id as an input writes clause the dropped packet and delay packets and detect the data traffic attack by fining the ratio of the drop and delay packets within the subnet. Subnet approach provides an efficient way to find out attacks in the network. If the ratio of the drop and delay packets is less than the actual value then attack will be detected and actor node eliminates the malicious path and established the new path for the data transmission. Data _control _ also takes subnet id of type subnet as an input. It writes clauses the drop and delay packets in the network and finds out the attack at the control traffic of the network. There are some preconditions before the creation of the subnet and sink node.

Pre-conditions: Unique newly created nodes must belong to the set of nodes field before creation and it should be less than the pre-defined limit.

operations
Detect Data Traffic Attacks(subnetIn:subnet)query:bool
*ext rd drop_packects:**set of packets***
*ext rd delay_packets:**set of packets***
*pre nodeId in set nodes and nodeId <**LIMIT***
post query <=>mk_Block(drop_packets,drop_packets) in set datatraffic;

Detect controll_Attacks(nodeIn:nodes)query:bool
ext** rd drop_packects:**set of packets
ext** rd delay_packets:**set of packets
pre true
post query <=>mk_Block(drop_packets,drop_packets) in set datacontroll;

Actor nodes play a head node role in Security assessment Model. These nodes are responsible to detect the malicious attacks at subnet level. Unique actor nodes in the subnets collaborate with each other to find out the attack and to efficient action that will be taken against that attack in the network. Detect jellyfish Attack take subnet id as an input. It writes clause the delay packet in the network and detects the attack by identifying the number of delay packets within the subnet. Wormhole attack is detected by finding the short circuit in the subnet. If any type of short circuit is an exit in the links of the nodes then wormhole attack is detected.

Detect Jellyfish Attack(subnetId:subnet)
ext rd delay_packets:set of packets
pre true
post query <=> nodeIn in set jellyfish;
Detect wormhole Attack(nodeIn:nodes)
ext rd short circuit:set of links
pre true
post query <=> nodeIn in set short_circuit;
Detect HelloFlood Attock(subnetIn:subnet)
ext rd drop_packet:set of packets
ext rd pdr:packet ratio
post query <=> nodeIn in set drop_packet and pdr;

VI. MODEL ANALYSIS

The formal specification of the ADM model has been analyzed and verified by VDM-SL Toolbox. The specification is checked by the C++ code generator, type checker, and syntax checker. Dynamic checking is used to identify the error at the runtime. The formal specification of the ADM model is conceded successfully from all the syntax and type checking and the proof of correctness of the purposed ADM model is shown in figure 6. Table 3 represents all the formal specifications is checked correctly in terms of syntax and semantics.

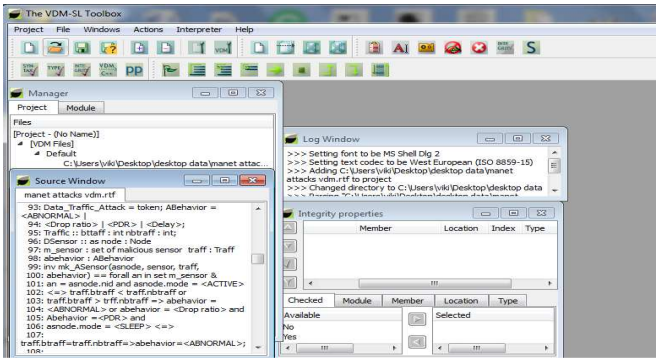

Figure 9. Proof of Correctness

Table 3. Analysis of structure, state, and operation

Composite object, State, Function, and Operations	*Syntax Check*	*Type Check*	*Pretty Check*	*Integrity Check*
Object	Y	Y	Y	Y
Attacks	Y	Y	Y	Y
Edges	Y	Y	Y	Y
Activation	Y	Y	Y	Y
Drop packet	Y	Y	-	Y
Delay packet	Y	Y	-	Y
Subnetting	Y	Y	-	Y
Values	Y	Y	-	Y
Invariants	Y	Y	-	Y
Execution	Y	Y	Y	Y
Pre/post conditions	Y	Y	Y	Y
Verification and validation	Y	Y	Y	Y

VII. CONCLUSIONS

The malicious attacks can be detected using attack detection model (ADM) and extinguished using subnetting based actor head nodes. In this paper, new attack detection model and algorithm is purposed for the security assessment of AODV protocol under data and control traffic attacks in mobile ad-hoc and sensor network (MAHSNs). This model explores the different type of attacks in MAHSNs. The Purposed ADM is verified and validated through Vienna development method–specification language Tool Box. The topology of wireless network like MAHSNs is difficult to control due to various attacks. The approach we have used can be applied and implement any type of algorithm in wireless sensor network. This is because we have observed that all types of attacks only detected when they are enter the system. Through VDM-SL specifications these types of attacks not only detect before entering the system but also provide the reliable mechanism to handle the outside attacks. So it has become possible through large and complex network can easily be handle for all types of attacks that disturb inter and intra communication of the networks.

VIII. REFERENCES

1. Murali, K., Rahul, M., Venkateshwaran, G., & Pariselvam, S. (2017). Detecting Attacks in MAHSN using Secure Zone Routing Protocol. *International Journal of Engineering Science*, *10182*.
2. Sharma, M. (2017). Combating Resource Consumption and Byzantine Attacks in MAHSN through Enhanced CBDS Technique.
3. Brar, S., & Angurala, M. (2016). Review on Grey-Hole Attack Detection and Prevention.

4. Faisal, M., Kumar, M., & Ahmed, A. (2013). ATTACKS IN MAHSN. *International Journal of Research in Engineering and Technology*, *2*(10), 273-276.
5. Maulik, R., & Chaki, N. (2011). A study on wormhole attacks in MAHSN. *International Journal of Computer Information Systems and Industrial Management Applications*, *3*(1), 271-279.
6. Lo, N. W., & Liu, F. L. (2013). A secure routing protocol to prevent cooperative black hole attack in MAHSN. In *Intelligent technologies and engineering systems* (pp. 59-65). Springer, New York, NY.
7. Ponsam, J. G., & Srinivasan, R. (2014). A survey on MAHSN security challenges, attacks and its countermeasures. *International Journal of Emerging Trends & Technology in Computer Science (IJETTCS)*, *3*(1).
8. Wu, X., & Yau, D. K. (2007, September). Mitigating denial-of-service attacks in MAHSN by incentive-based packet filtering: A game-theoretic approach. In *Security and Privacy in Communications Networks and the Workshops, 2007. SecureComm 2007. Third International Conference on* (pp. 310-319). IEEE.
9. Yang, B., Yamamoto, R., & Tanaka, Y. (2012, February). Historical evidence based trust management strategy against black hole attacks in MAHSN. In *Advanced Communication Technology (ICACT), 2012 14th International Conference on* (pp. 394-399). IEEE.
10. Badiwal, S., Kulshrestha, A., & Garg, N. (2017). Analysis of Black Hole Attack in MAHSN using AODV Routing Protocol. *International Journal of Computer Applications*, *168*(8).
11. Lalar, S. (2014). Security in MAHSN: Vulnerabilities, Attacks & Solutions. *Intational J. Multidiscip. Curr. Res*, *2*, 62-69.
12. Shivahare, B. D., Wahi, C., & Shivhare, S. (2012). Comparison of proactive and reactive routing protocols in mobile adhoc network using routing protocol property. *International Journal of Emerging Technology and Advanced Engineering*, *2*(3), 356-359.
13. Gandhewar, N., & Patel, R. (2012, November). Detection and Prevention of sinkhole attack on AODV Protocol in Mobile Adhoc Network. In *Computational Intelligence and Communication Networks (CICN), 2012 Fourth International Conference on* (pp. 714-718). IEEE.
14. Sultana, J., & Ahmed, T. (2017, February). Securing AOMDV protocol in mobile adhoc network with elliptic curve cryptography. In *Electrical, Computer and Communication Engineering (ECCE), International Conference on* (pp. 539-543). IEEE.
15. Abbas, S., Merabti, M., Llewellyn-Jones, D., & Kifayat, K. (2013). Lightweight sybil attack detection in MAHSNs. *IEEE systems journal*, *7*(2), 236-248.
16. Kumar, A., & Chawla, M. (2012). Destination based group Gray hole attack detection in MAHSN through AODV. *International Journal of Computer Sciences*, *9*(4).
17. Nayak, D., & Kiran, Y. C. (2017). Malicious Node Detection by Identification of Gray and Black Hole Attacks using Control Packets in MAHSNs. *Imperial Journal of Interdisciplinary Research*, *3*(7).
18. Mejri, M. N., & Ben-Othman, J. (2017). GDVAN: A New Greedy Behavior Attack Detection Algorithm for VANETs. *IEEE Transactions on Mobile Computing*, *16*(3), 759-771.
19. Prasad, P. S., & Rao, S. K. M. (2017). HIASA: Hybrid Improved Artificial Bee Colony and Simulated Annealing based Attack Detection Algorithm in Mobile Ad-hoc Networks (MAHSNs). *Bonfring International Journal of Industrial Engineering and Management Science*, *7*(2), 01-12.
20. Li, T., Ma, J., & Sun, C. (2017). NetPro: detecting attacks in MAHSN routing with provenance and verification. *Science China Information Sciences*, *60*(11), 118101.
21. Dhyani, I., Goel, N., Sharma, G., & Mallick, B. (2017). A Reliable Tactic for Detecting Black Hole Attack in Vehicular Ad Hoc Networks. In *Advances in Computer and Computational Sciences*(pp. 333-343). Springer, Singapore.
22. Khan, F. A., Imran, M., Abbas, H., & Durad, M. H. (2017). A detection and prevention system against collaborative attacks in Mobile Ad hoc Networks. *Future Generation Computer Systems*, *68*, 416-427.
23. Khare, A. K., Rana, J. L., & Jain, R. C. (2017). Detection of Wormhole, Blackhole and DDOS Attack in MAHSN using Trust Estimation under Fuzzy Logic Methodology.
24. Brar, S., & Angurala, M. (2016). Review on Grey-Hole Attack Detection and Prevention.
25. Somasundaram, K. (2016). An Effective CBHDAP Protocol for Black Hole Attack Detection in MAHSN. *Indian Journal of Science and Technology*, *9*(36).