International Journal of Computer Networks and Communications Security

VOL. 2, NO. 8, AUGUST 2014, 242–249
Available online at: www.ijcncs.org
ISSN 2308-9830

# Time Dependent Finite State Machine based Method for Intrusion Detection in Mobile Ad Hoc Networks

**MAHDA NOURA[1], SINA MANAVI[2], NASRIN KHANEZAEI[3]**

[1, 2, 3] Faculty of Computer Science and IT, U.P.M. University, Kuala Lumpur, Malaysia

*E-mail: [1]mahdanoura@gmail.com, [2]manavi.sina@gmail.com, [3]nasrin.khanzaei@gmail.com*

## ABSTRACT

The Ad hoc On-Demand Distance Vector (AODV) routing protocol designed with the purpose of mobile ad hoc networks has numerous advantages such as low network utilization, fast adjustments to link conditions and low memory and processing overheads. However, if security is not considered in this protocol it is at risk to many attacks. The conventional methods such as firewalls, encryption is no longer adequate. In this paper, we identify three types of threats against AODV which influence the routing message in MANET. Our solution is based on the use of Time based Finite State Machine to identify correct and malicious behavior in AODV. The TFSM have been modelled using JFLAP and simulated in MANET environment using C#.

**Keywords:** *AODV, MANET, Intrusion Detection, Time Finite State Machine, Automata, JFLAP, C#.*

## 1 INTRODUCTION

Mobile Ad Hoc Networks (MANETs) is known as a collection of wireless computers with communication between them which are able to move freely without any dependency on the infrastructures. Base stations or access points are great examples of such independent mobile systems [1]. In the MANET, nodes forward the packets among each other, to contribute the routing functionality and provide indirect wireless transmission; acting as both hosts and routers. Since MANET is a decentralized administration and does not need a fixed network infrastructure, it can be set up quickly and inexpensively on demand, it can be applied in different scenarios such as military applications [2], [3], emergent application [4], [5], and Personal Digital Assistants (PDAs) [6], civilian application like an ad-hoc meeting or ad hoc classrooms. De Morais Cordeiro discussed deeper about mobile ad hoc network applications and their theory in his book [7].

While wired networks are strongly secure in gateways and routers, MANET security challenges raise due to its dynamic nature, significant dependency to node cooperation, lack of centralized administration [8], [9]. Since MANET's topology is progressing and growing, there is no standard defined boundary, consequently, firewall access control mechanism cannot be applied properly on such networks. On the other hand, crypto systems cannot be applied on it due to lacks of centralized administration, which allow a malicious user to take control of the whole network. Increasing the number of nodes in this network requires to provide higher level of security [10]. To Identify the malicious user and intrusion over the network, MANET needs a precise security mechanism. This research has focused on dropping attack, resource consumption and sequence number attack. The propose method in this study is based on Time based Finite State Machine (TFSM) for Intrusion Detection System (IDS) using JFLAP software to detect attacks on the Ad Hoc On-demand Distance Vector (AODV) routing protocol. To identify the aforementioned attack types, the AODV, it is implemented in MANET.

The Rest of this work is organized as follows: background of IDS, AODV security, and IDS over the ad hoc networks has been reviewed in section II. In Section III, three vulnerabilities of MANET and AODV have been discussed. The proposed TFSM model is given in section 4. The 5th section, illustrates the AODV model with the JFLAP software, and implemented simulation software has been demonstrated by the research. The last section, conclude the research and discuss about future works of this criteria.

## 2 BACKGROUND

### *2.1 Intrusion Detection System (IDS)*

Intrusion are defined as any malicious activity which compromise the availability, confidentiality or integrity of computer resources in digital world [11] and to detect these intrusion, Intrusion Detection System is proposed. Data collection, detection and response are the three main components of the IDS. The first component in IDS is known as data collection that is responsible to collect and basic processes such as data transfer to the standard format, store and replicate them to the detection modules [11].

The input data sources for the IDS can vary from system logs, network packets and etc. detection components is another key feature of the IDS to analysis the received information from data collection components and detect the possible intrusions. And finally once this component identifies any intrusions, it sends them to the response component. Intrusion Detection System is applicable for vulnerability scanning and assessments. It utilize two common techniques signature based detection and anomaly based detection [12].

Signature based IDS monitors regarding behaviors that match predefined patterns which define a known threat. A key benefit of this method is that creating and understanding signatures are simple when we know what network activities we are trying to identify [13]. There is an attack signature database that keeps record of all the different types of attacks that may occur on the network. Anytime a sensor sends information down on to the collector it will compare that information against the attack database and if it finds a match it knows that the system is under attack. However, if there is no match it is going to assume that everything is normal. They can’t identify an attack they do not know about.

In an anomaly based system there is a network history database instead of an attack database. A network history database collects information about normal behavior in the network and overtime it establishes relatively accurate baseline of what regular behavior is. Then anytime there is a deviation from normal behavior it would be compared against the baseline and a determination would be made as to whether or not that an attack has occurred [12], [13].

One of the disadvantages of anomaly based is that there is a potential for more false positives because of the fact that it is not locked in an absolute signature of attack. It’s looking at behaviors on the network and there is a chance that what might be normal behavior may be misunderstood as an attack and some false positives may occur. An upshot to anomaly based is the fact that it is not locked down to a signature database.

And finally the last response component once alarmed by the previous component, act based on the response policy actively or passively. An active response IDSs is used to take some kind of action automatically in response to a suspicious activity in order to stop the attack at the entry point. The action depends on the critically of the attack. It can communicate with the networking devices and can send meaningful instructions to those devices in order to be able to get to do something to block that. One active response is gathering extra information about the suspicious attack and the intruder by the increasing the sensitivity level of an IDS. Another active response is to stop an attack and subsequently block further access of the intruder to the system. This could be done by changing the configuration of firewall and routers. Another active response is invasion back which is illegal and launches attacks against the intruder.

A passive IDPS is a system that is designed to monitor and analyze activities of network traffic and inform other parties about the occurrence of an attack. A passive IDPS does not automatically respond to an intrusion and relies on human interventions like a system administrator to respond to the alarm, take a suitable action to stop the attack. Some IDS, simply log suspicious activities in a log file and the system administrator would be informed for example by email or pager. Alarms and notifications varies widely, ranging from an onscreen alert, email, pager, cellular phones to SNMP trap messages and plug-ins.

### *2.2 Intrusion Detection Issues in MANETS*

Wireless Links: eavesdropping attack is one of the vulnerability which takes place due to the use of wireless links in MANETs. While in the wired attack, intruder requires to have a physical access, in MANETs, he can compromise the system without any physical access. Another disadvantage of the wireless networks is low bandwidth; as a result, by consuming the bandwidth by the malicious user, authorized nodes may lose their accessibility and normal communication [11].

Dynamic Topology: the main reason that network topology changes frequently is that, MANET nodes can freely move from one network to another, leave or joint another network. Thus this dynamic environment brings difficulties in differentiating the abnormal behaviour from normal behaviour. Moreover, all the nodes has the mobility characteristic, and servers neither other critical nodes are exception, therefore these critical nodes are not as well as wired critical nodes, in a locked place which increases the risk of being compromised [11].

Cooperativeness: since mostly in MANET nodes are assumed as cooperative and non-malicious, malicious attacker easily can take control the network as a routing agent and disrupt the network operations [14].

Lack of clear line of defence: MANETS can be under attack from all direction, because there is no clear line of defence in MANET. On the other hand, there is no boundary to separate the inside network from outside world. Meaning there is no defined area for monitoring the traffic and applying access control mechanisms. Unlike Wired networks that all network packets pass from gateways, routers or switches, MANET network data is distributed in the transmission range [14].

Limited Resources: MANET support different type of devices from laptops to mobile phones and PDAs with different computing power and storage capacities. The mobile nodes can be alive by the battery's power, which attracts attackers to develop new type of attack targeting the power consumption called Sleep Deprivation Torture". Applying the new security mechanism to protect these networks from such attacks itself, demands more computing and communication resources. This is another problem that rise in MANET networks [14].

### *2.3 Overview of AODV protocol*

Many routing protocols have been introduced to suit the diverse needs of MANETs. In this section we will explain how AODV works to understand better the routing attacks which are later explained. There are three main types of messages in AODV: route request (RREQ), route reply (RREP), and route error (RERR) messages. At first, when a node wants to communicate with another node in the network and does not have a fresh route to this destination, it starts the route discovery process by broadcasting a RREQ message for the destination node into the network. Intermediate nodes that receive this request either send a RREP to the source node if they have a fresh route to the destination node and the "destination only" flag is not set, or forward the RREQ message to other nodes. A fresh route is a valid route entry whose sequence number is equal to or greater than that contained in the RREQ message. If the request packet has been forwarded by this intermediate node before, the RREQ message is dropped. When the destination node receives a RREQ for itself, it sends back a RREP message on the reverse route. The node which initiated the request and the nodes which received the RREP messages on the route update their routing tables with the new route. Fig 1, demonstrates the visualized concept of AODV.

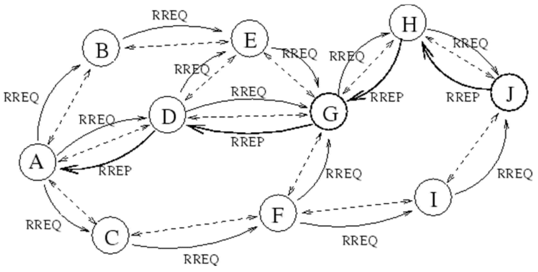


*Fig. 1. AODV Concept*

## 3 ATTACKS ON MANETS AND AODV PROTOCOL

MANET security just similar to other networks relies on authentication, confidentiality, integrity, availability and non-reputation [15]. To verify the identity of the source information, authentication mechanism is applied to verify the identification of source information. To avoid any unauthorized access to the resources, confidentiality mechanism is applied. To provide the on demand accessibility to the nodes and resources by the authorized user, availability mechanism is provided. Denial of Service (DoS) attack is one attack against availability. Lastly, non-repudiation ensures that the actions that are done by someone cannot be denied. In MANETs security objectives can vary in different modes and situation (e.g. war time, peace time etc.). MANETs characteristics make them vulnerable to net attacks. Here we will focus on active attacks that exist in MANET such as sequence number attack, dropping attack and resource consumption attack.

### *3.1 Sequence Number Attack*

In AODV protocol routes are created and maintained by assigning increasing sequence numbers to routes for a particular destination. Because a fresh route is determined by the destination sequence number and indeed fresh routes are better, a malicious node can send incorrect routing information to the network. When the malicious node receives a RREQ even if it does not have a fresh route in its routing table it creates a RREP with fake information about the sequence number and the next hop. The malicious node puts a high number to the destination sequence number in order for the fake information to be chosen. If the RREP from the malicious node is received before the one from the legitimate source node then the malicious node will be put in the route. Therefore, it can capture the routing packets or perform a black hole attack. Even if the RREP of the legitimate node is received first, finally it will reach and because the destination sequence number is bigger than the original route it will be replaced by the incorrect route.

### *3.2 Dropping Attack*

Malicious or selfish nodes intentionally drop all the packets that are not destined for them. The aim of selfish nodes is to reserve their resources. If the dropping node is at an important location dropping attacks can avoid end-end communication between nodes. It may also reduce the network performance by causing packets to be retransmitted, new route discovery and so on. Except DSR protocol, most of the routing protocols are unable to identify whether data packets have been forwarded by intermediate nodes or not. But, attacks against a node can be identified through passive acknowledgements by its neighbour [11].

### *3.3 Resource Consumption Attack*

In this kind of attack, malicious user targets the MANET by sending the pointless routing traffic such as PREQ and RERR packets to flood the network bandwidth with the false and irrelevant routing packets. Thus consuming the energy and processing power of the nodes.

## 4 TIME BASED FINITE STATE MACHINE DETECTION FOR AODV

The time-dependent Finite State Machine is an extension to FSM. In any TFSM a time interval is considered between receiving inputs in order to identify a member of a language. Using TFSM is extremely valuable when identifying threats in a network because many threats rely on the duration between the arrivals of packets. In the following the design of the TFSM related to the detection of three types of attacks have been deliberated.

### *4.1 Sequence number attack*

In order to identify the sequence number attack correctly two different TFSMs are required.

In Fig2 the TFSM is triggered whenever a node initiates a route discovery process. If a RREP message does not arrive within a predefined time period (Time-Out) the TDFA timeouts and resets to its initial state (init_0). When the first RREP message is received the machine checks if the included destination sequence number (RREP-dest-seq) is much higher than the sequence number which is in the RREQ (origin-dest-seq). If it is very high it goes directly to the alarm state (Alarm). If it is not, it stays in the same state (state 1) for time t. If the timer expires without receiving another RREP it goes to the accept state. If within the time limit another RREP(s) arrives, destination sequence number is checked to see if it is valid, similarly a decision is taken whether to move to an alarm state. When an alarm occurs the source node knows that the information in the RREP is forged and that it must not update the routing table with the invalid routing information. The machine goes to the state 0 when the sender initiates a RREQ.

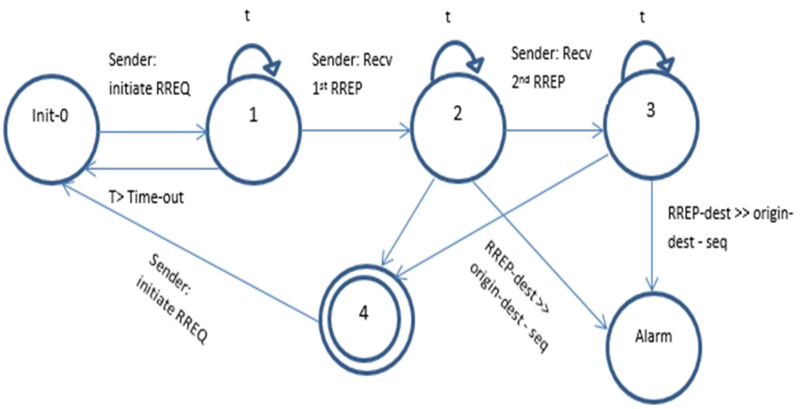


*Fig. 2. Initiating a route discovery process*

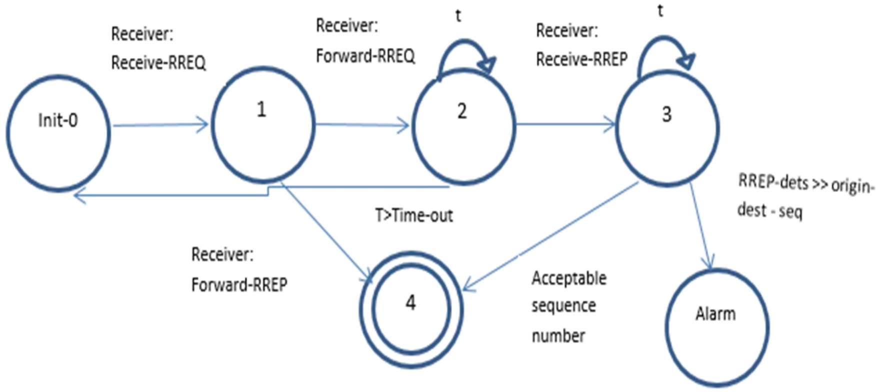


*Fig. 3. Protecting the intermediate nodes*

The second TFSM (Fig 3) for this attack protects the intermediate nodes that receive the RREQ initiated for the source node. When an intermediate node receives a RREQ there are 2 actions that can be taken:

- The intermediate node itself has a fresh enough route to the destination. In this case it sends a RREP message and the TFSM moves to accept state (state 4).
- The intermediate node does not have the necessary information to reply to this RREQ. In this case it forwards the RREQ packet downstream and moves to state 2. The TFSM stays in this state for time t. If the timer expires it moves to the initial state and resets. If it receives a RREP before the timeout, it moves to state 3. In state it must check to see whether the sequence number is valid or not. It is the same as the previous TFSM. If the sequence number is acceptable within the time limits it goes to accept state. Otherwise, it should go to the Alarm state and should not add this fake route to its routing table. The intermediate node cannot drop the RREP message even though it has recognized a forgery. Thus in the Alarm state the RREP message is sent to the initial node.

### 4.2 Dropping Routing Packet

The neighboring nodes can identify whether a malicious node has forwarded a routing packet. However, there is a challenge because the neighboring node may have not forwarded the packet due to traffic overload and this will produce false alarm. So, at first it is moved to a pre-alarm state and in this state it unicasts the routing packet to the offending node again.

The TFSM in Figure 4 is triggered whenever a node sends or forwards a RREQ or a RREP packet. It stays in state 2 for time t waiting for the node to forward/reply to the routing packet. If the node replies or forwards the packet it normally resets the TFSM with N_RESET.

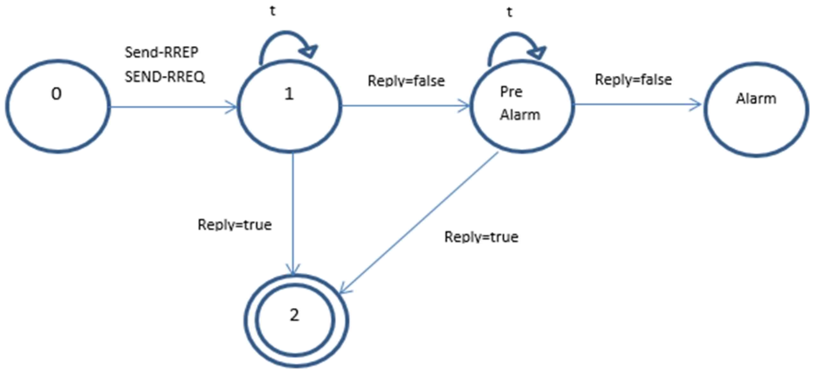


*Fig. 4. Sending RREP or RREQ*

If the node fails to appropriately respond to the forwarder routing traffic the TFSM moves to a Pre-Alarm state and remains there for time t. If the node is able to respond appropriately by forwarding the routing traffic or by replying to a RREQ it moves to the accept state. Otherwise, the machine goes to an alarm state and this node is marked as malicious, thus it does not forward any kind of traffic through this node and it also sends a RRER packet to the upstream neighbors in order to prevent them from sending traffic through the malicious node.

### 4.3 *Resource Consumption Attack*

The resource consumption detection TFSM is triggered for every different node that sends a routing packet. The observing node keeps a list with all the nodes from which it has recently received routing traffic as well as a counter that states the number of packets that the specific node sent and a timer.

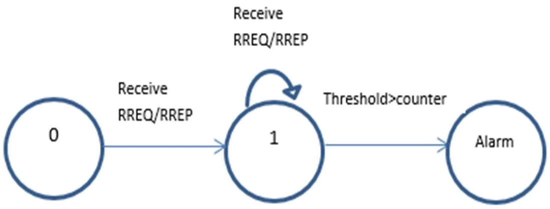


*Fig. 5. Receiving new routing packets*

In Fig 5 the TFSM increments the counter for every new routing packet received from this node. It remains in the state 1 for time t. If the counter reaches the threshold value it means that it has detected abnormal traffic generation and it moves to the Alarm state. When an alarm is triggered the node drops all the incoming routing traffic from the offending node for finite time interval so that it does not consume network and node resources.

## 5 SIMULATION

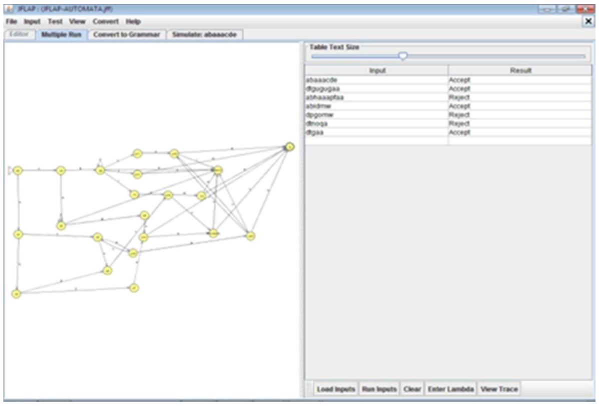
### 5.1 *JFLAP Modelling*

JFLAP (Java Formal Languages and Automata Package) is an widespread visual and interactive tool for designing and experimenting with different types of automata and grammars, studying proofs by the construction of examples, studying parsing through LL, SLR and brute force methods, and transforming grammars.

| | |
|---|---|
| Receive packet, PREQ, PREP | a |
| Packet type: PREQ | b |
| Have fresh route | c |
| Send/Forward packet, PREQ, PREP | d |
| Normal packet | e |
| Packet type: PREP | f |
| Packet type: PREQ | g |
| Threshold>>counter | h |
| No fresh route | i |
| Repeated packet | j |
| Drop packet | k |
| Abnormal packet | l |
| Reply with PREP | m |
| PREP-dest!>>origin-dest-seq | n |
| Is destination | o |
| Not destination | p |
| Neighbor has forward PREQ | q |
| Neighbor has not forward2nd packet | r |
| Neighbour has not forwarded PREQ | s |
| Originated packet | t |
| Timeout and not received PREP | u |
| PREP-dest!>>origin-dest-seq and timeout | v |
| PREP-dest>>origin-dest-seq | w |

*Fig. 6. Table of content*

Using JFLAP, we have modelled the DFA and NFA for this work. The table of content is shown in Figure 6, and the model is shown in Fig 7-9. The following model accurately identifies the attacks based on the strings given to the DFA and NFA.



| Input | Result |
|---|---|
| abaaacde | Accept |
| dfgugugaa | Accept |
| abhaaapfaa | Reject |
| abidmw | Accept |
| dpgomw | Reject |
| dtnoqa | Reject |
| dfgaa | Accept |

Fig. 7. AODV Acceptance and Rejection

### 5.2 *Interface*

We will simulate aspects of intrusive behaviour of malicious hosts using Visual C sharp with a selfmade simulation. In this work the simulation environment includes dynamic topology of network with Random Way Point as the mobility model. The interface of the simulation that we have designed is shown in Figure 10. This figure illustrates the starting steps and before the transmission has occurred.

There is some field relevant to this interface:

Mobile: This field is the number of mobile nodes that we could have.

Source: This field gets an integer between 0 and the number of mobile nodes minus one. It shows the source nodes identification for the sending process.

Destiny: This field gets an integer between 0 and the number of mobile nodes minus one. It shows the destination nodes identification for the receiving process. The source destination fields show that the neighbour discovery packet is sent from the source node to the destination.

No of Data: This field gets an integer from 1 to 150 as the maximum number of packets that is allowed to be transferred.

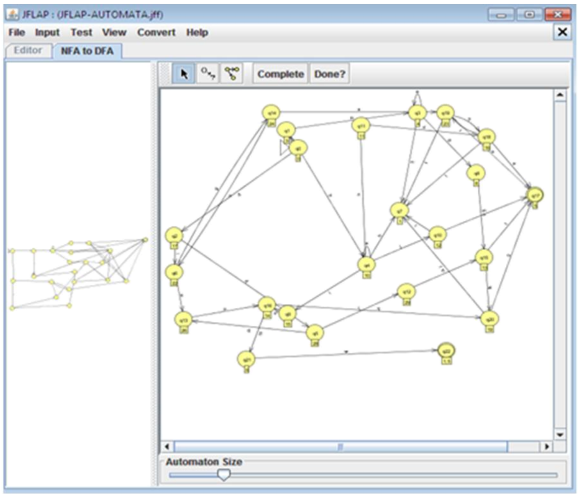

JFLAP : (JFLAP-AUTOMATA.jff)
File Input Test View Convert Help
Editor
NFA to DFA
Complete
Done?
Automaton Size

*Fig. 8. AODV Model*

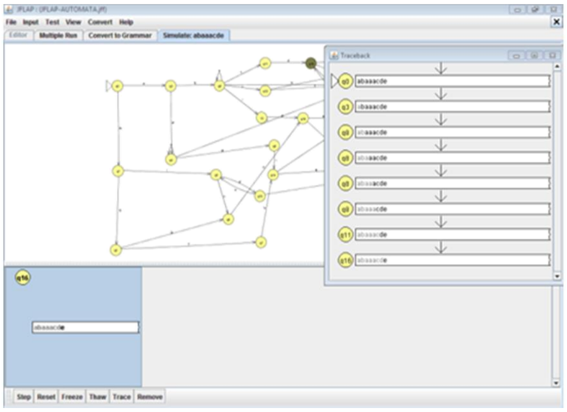

JFLAP : (JFLAP-AUTOMATA.jff)
File Input Test View Convert Help
Editor
Multiple Run
Convert to Grammar
Simulate: abaaacde
Traceback
Step Reset Freeze Thaw Trace Remove

*Fig. 9. AODV Final State*

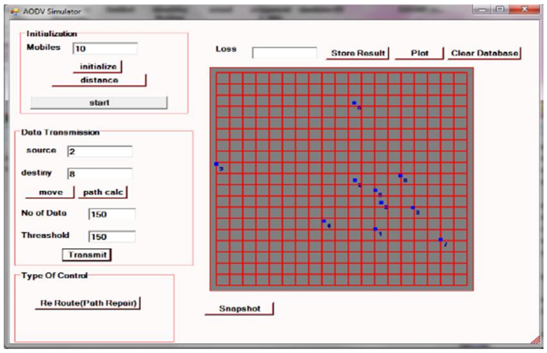
*Loss*: After the simulation has finished the number of packets that has been lost will be shown in this field and by clicking on the STORE RESULT field this field will be recorded in the database as the result.

*Initialize*: By clicking on this button the number of mobile nodes would be instantiated and will be shown on the screen.

*Distance:* This button calculates the distance between each of the mobile nodes.

*Path Calc*: This button calculates the shortest path between the source node and the destination node.

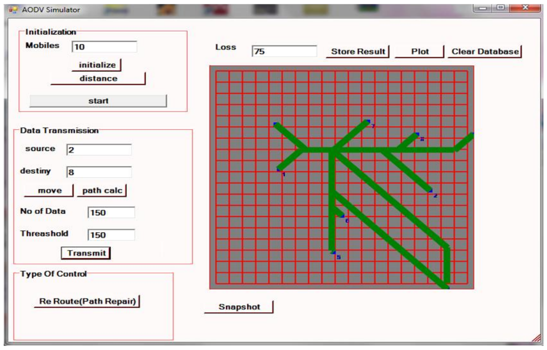
*Transmit:* This is the last button that should be clicked and it starts the process of sending a RREQ packet. The nodes in the scenario start sending packets to each other.



Mobiles: 10
Loss:
source: 2
destiny: 8
No of Data: 150
Threshold: 150

*Fig 10. Interface Simulation with starting steps*

When all the required fields have been filled and after the TRANSMIT button has been pressed the sending and receiving process and RREQ and RREP messages is started. The mechanism of this has been explained earlier. This is shown in Figure 11.



Mobiles: 10
Loss: 75
source: 2
destiny: 8
No of Data: 150
Threshold: 150

*Fig. 11. Transmission steps*

The TFSM of the three types of attacks have been implemented. When an intrusion is identified in the system an alarm is generated in the form of a message box stating the node that is malicious as well as the type of attack that it has identified.

## 6 CONCLUSION AND FUTURE WORKS

The intrusion detection system that has been proposed and implemented in this paper is based on TFSM and can identify the three main types of attacks on the AODV protocol in MANET environment. The system can detect intrusions and correct behavior in the network accurately. The chief performance metric in any intrusion detection system is false alarms; an alarm is triggered incorrectly in a non-malicious behavior. However, in this paper false alarm rates were not considered and as future work the evaluation of the present solution must be considered.

## 7 REFERENCES

[1] M. Bansal, R. Rajput, and G. Gupta, “Mobile ad hoc networking (MANET): Routing protocol performance issues and evaluation considerations,” Internet Soc., 1999.

[2] T. Plesse, C. Adjih, P. Minet, A. Laouiti, A. Plakoo, M. Badel, P. Muhlethaler, P. Jacquet, and J. Lecomte, “OLSR performance measurement in a military mobile ad hoc network,” Ad Hoc Networks, vol. 3, no. 5, pp. 575–588, 2005.

[3] J.-H. Cho, A. Swami, and R. Chen, “A survey on trust management for mobile ad hoc networks,” Commun. Surv. Tutorials, IEEE, vol. 13, no. 4, pp. 562–583, 2011.

[4] H. Wang and L. Song, “Architecture Design and Implementation Methods of Heterogeneous Emergency Communication Network,” in Advanced Research on Electronic Commerce, Web Application, and Communication, Springer, 2011, pp. 122–127.

[5] V. Callaghan, G. Clarke, M. Colley, H. Hagras, J. S. Y. Chin, and F. Doctor, “Inhabited intelligent environments,” BT Technol. J., vol. 22, no. 3, pp. 233–247, 2004.

[6] S. A. K. Al-Omari and P. Sumari, “An overview of mobile ad hoc networks for the existing protocols and applications,” arXiv Prepr. arXiv1003.3565, 2010.

[7] C. de Morais Cordeiro and D. P. Agrawal, Ad hoc and sensor networks: theory and applications. World Scientific, 2011.

[8] E. O. Ochola, M. M. Eloff, and J. A. van der Poll, “Mobile Ad-hoc Network Security Challenges under AODV Routing Protocol,” in Proceedings of the Ninth International Network Conference (INC 2012), 2012, p. 113.

[9] S. Agrawal, S. Jain, and S. Sharma, “A survey of routing attacks and security measures in mobile ad-hoc networks,” arXiv Prepr. arXiv1105.5623, 2011.

[10] P. Yi, Y. Zhong, and S. Zhang, “A novel intrusion detection method for mobile ad hoc networks,” in Advances in Grid Computing-EGC 2005, Springer, 2005, pp. 1183–1192.

[11] K. Biswas and M. L. Ali, “Security threats in mobile Ad Hoc network,” Dep. Interact. Syst. Des. Sch. Eng. march2007, pp. 9–26, 2007.

[12] V. Marinova-Boncheva, “A short survey of intrusion detection systems,” Probl. Eng. Cybern. Robot., vol. 58, pp. 23–30, 2007.

[13] R. Shanmugavadivu and D. N. Nagarajan, “Network intrusion detection system using fuzzy logic,” Indian J. Comput. Sci. Eng., vol. 2, no. 1, pp. 101–111, 2011.

[14] S. A. Razak, S. M. Furnell, and P. J. Brooke, “Attacks against mobile ad hoc networks routing protocols,” in Proceedings of 5th Annual Postgraduate Symposium on the Convergence of Telecommunications, Networking & Broadcasting (PGNET04), 2004.

[15] L. Ertaul and N. Chavan, “Security of ad hoc networks and threshold cryptography,” in Wireless Networks, Communications and Mobile Computing, 2005 International Conference on, 2005, vol. 1, pp. 69–74. “http://www.jflap.org.” .