International Journal of Applied Engineering Research ISSN 0973-4562 Volume 12, Number 9 (2017) pp. 1956-1961

Intrusion Detection using RREP Messages Of AODV Routing Protocol

Deepak Kumar Verma
Department of Computer Science and Engineering, UIET, CSJM University Kanpur-208024, India.
Email Id: deepak300572@gmail.com

Renu Jain
Department of Computer Science and Engineering, UIET, CSJM University, Kanpur-208024, India.
Email Id: jainrenu@gmail.com

Ashwani Kush
Department of Computer Science, University College, Kurukshetra University Kurukshetra, India.
Email Id: akush20@gmail.com

Abstract
In this paper destination sequence number and hop count fields of RREP message of AODV are used to identify the malicious node in a mobile ad hoc network. A malicious node in MANET has a tendency of attracting traffic towards itself so that it can perform various type of attacks like dropping the packet, misrouting the packet, altering the information in the packet etc. To accomplish the motive malicious node sends reply for a RREQ message it receives from source. The vital information which is fictitiously set by malicious node is destination sequence number and hop count in the RREP. This fictitious information compels the source node to route the information through the malicious node. The proposed method analyses all the received RREP messages, received from various nodes in the MANET to identify the malicious node if any, before deciding the node through which the data is to be routed.

Keywords: AODV, MANET, RREP, RREQ

Nomenclature

AODV	Ad hoc on demand distance vector
MANET	Mobile ad hoc network
RREP	Route reply
RREQ	Route request

INTRODUCTION

Network in digital communication has become an inevitable part. To remain connected with mobility is one of the major requirement rather one of the major factor for popularity of such mobile networks. MANETs are the boon to the network needs because they serve the purpose in situations when the network is to be established in a very short span of time and for a short duration. Also the cost of establishing the network is negligible. Mobile ad hoc networks are network of standalone nodes which work with collaborative effort of all the mobile nodes in the network. Each node has the responsibility of routing the message from source to destination, it could be a source or a destination at another time. MANETs do not require any fixed infrastructure. The medium for communication is wireless. These networks are useful in scenarios where it is difficult to establish a wired network, the network is to be short lived, network is required to be established within a very short span of time.

Since MANETs are infrastructure less they do not have any central authority to manage the network. It is assumed that each node in the network contribute towards forwarding and managing the network connectivity.

These networks apart from having benefits also have inherent demerits these come from their being open to air communication i.e. they have wireless connectivity and hence are vulnerable to several kind of attacks both from insider and outsider [7]. Also the bandwidth is limited for communication unlike wired scenario. Nodes being mobile have limited power which becomes a bottleneck for processing of control messages.

These limitations have attracted researchers. One of the major thrust is on Intrusion detection systems, which safe guards against several type of attacks may it be from within the network due to a malicious node or from outside the network wherein an external node does an eavesdropping.

Several intrusion detection techniques [8][9][10][11][12][13] have been proposed which could be classified as follows.

a. Those that identify unexpected working of nodes called anomaly based intrusion detection
b. Those that identify nodes against pre known behavior called signature based intrusion detection.

The proposed method is an anomaly based intrusion detection method which is to be used by every legitimate node of the network to identify the insider attack by a malicious node in the ad hoc network.

The remainder of this paper is organized as follows. Section II gives background information about AODV protocol. Section III discusses the proposed method. Section IV shows the simulation results. Section V and VI focuses on the related work and conclusion respectively. Finally, Section VII is references.

Ad-Hoc ON DEMAND DISTANCE VECTOR ROUTING: AODV

AODV [1] is a routing protocol which activates only when a node wants to send data packets to desired destination but could not find the route. This protocol does the job of letting a source node decide to which neighbor data packets should be forwarded so as to reach the desired destination. For this AODV uses two control messages namely RREQ i.e. route request message and RREP i.e. route reply message. RREQ messages are broadcasted from one node to another if node does not know of a fresh enough rote to the destination. This process continues till either route request reaches the destination itself or to an intermediate node which has a fresh enough route to destination.

Apart from routing table every node maintains a reverse routes so as to send back the RREP message to source. For every node RREQ message broadcasted has an associated RREQ ID which combined with IP address of that node uniquely identifies a RREQ message. Nodes also use their

own sequence number which keep routes free from loops and also help in updating routing information about other nodes in the MANET. Only the first copy of received RREQ message is entertained by nodes repeated RREQ messages are dropped. AODV uses RERR i.e. route error message for route maintenance i.e. whenever a node finds a link break to its neighbor or an active route it sends a RERR message upstream.

PROPOSED METHOD

The way a malicious node for AODV protocol tries to misguide a source node, is by sending a RREP (route reply) message to source node having high value of Destination sequence number which shows that this node is having the latest route to destination and/or low value of Hop count which shows it has the shortest route to destination. The proposed method works on these two values i.e. value of destination sequence number and hop count received through route reply message and utilizes clustering algorithm which separates messages which have being fabricated and sent by a malicious node. The segregation of messages is done based on both the parameters separately and merged to get a complete list of malicious nodes IP addresses. A source node can now ensure that it does not chooses to send the data packets through such nodes.

To find malicious nodes attempting for an attack the proposed algorithm for AODV protocol is as follows.

A. Algorithm for proposed method

Step1. Source node requiring data transfer to a destination node broadcast's a RREQ message as normal AODV operation.

Step2. Source node collects all the RREP (route reply) messages it gets in response to the RREQ message broadcasted in step1. For collecting all the RREP messages this source node waits for pre-defined time i.e. NET-TRAVERSAL-TIME or binary back off time set by node as per AODV protocol which depends on retry attempt for RREP message.

Step3. Source node finds if destination node has sent a RREP message if yes this message is stored separately. Remaining RREP messages are stored in a table called intermediate-RREP-table

Step4. If RREP from Destination node is not received by source node, see step3 above. Follow step5 to step 9 Else follow step10 to step12.

Step5. Clustering algorithm is applied by the source node on the RREP messages stored in table intermediate-RREP-table to obtain two clusters of nodes based on Destination sequence numbers in the RREP messages.

Step6. Source node inserts all the RREP messages from the minor cluster (having less number of IP addresses) to a table called malicious-table.

Step7. Clustering algorithm is applied by the source node on the RREP messages stored in table intermediate-RREP-table to obtain two clusters of nodes based on Hop count in the RREP messages.

Step8. Source node appends all the RREP messages from the minor cluster (having less number of IP addresses) to malicious-table, duplicate RREP messages are to be stored once.

Step9. Source node choose to send data to destination through intermediate node except those in malicious-table.

Step10. Clustering algorithm is applied by the source node on the RREP messages stored in table intermediate-RREP-table to obtain two clusters of nodes based on Destination sequence numbers in the RREP messages. Keeping Destination sequence number of RREP message received from "destination as center of one of the two clusters".

Step11. Source node inserts all the RREP messages from the minor cluster (having less number of IP addresses) to a table called malicious-table.

Step12. Source node choose to send data to destination through intermediate node except once in table malicious-table.

B. Flow Chart

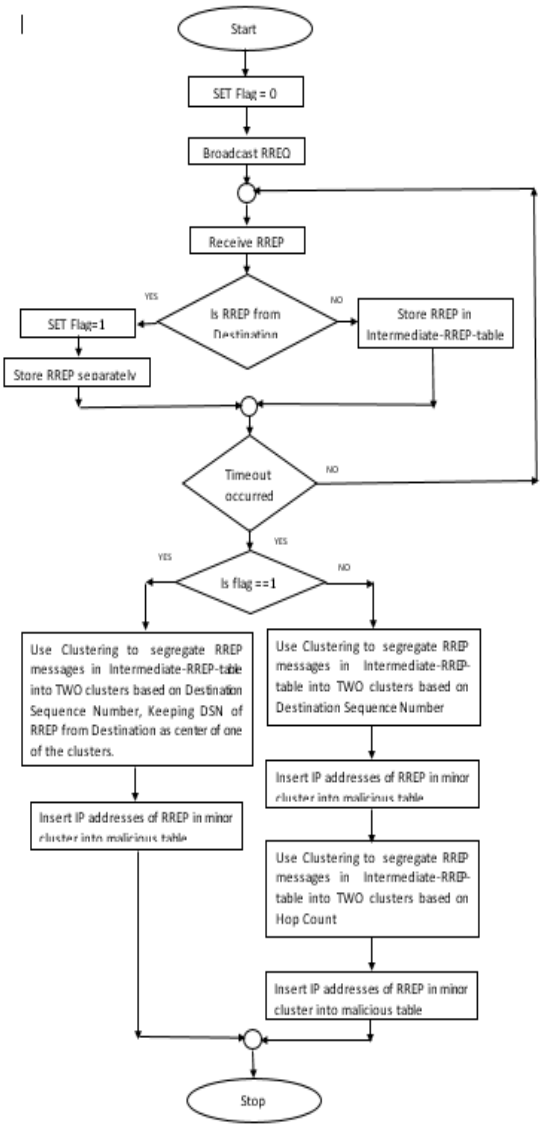

Figure 1: Flow chart for proposed algorithm

SIMULATION RESULTS

Simulation has been done on simulator NS2.35 with following parameters

Simulator	NS2.35
Channel	Wireless Channel
Propagation Model	Two Ray ground
Queue	Drop Tail
Antenna	Omni antenna
Routing Protocol	AODV
Simulation Area	670 X 670
Communication Type	CBR
Number of Nodes	10

Figure 2: Simulation Parameters

The simulation has been done for (a) Normal AODV protocol without any malicious node (b) Normal AODV protocol with malicious node(s) and (c) AODV with proposed method.
For each of the three simulation scenarios following parameters have been collected and graphs plotted to study the results. K-Means algorithm has been used for clustering of RREP messages received by the source.

Parameter	Constant	No. of Nodes
PDR versus Pause Time	Speed	10
Throughput versus Pause Time	Speed	10
Delay versus Pause Time	Speed	10
PDR versus Speed	Pause Time	10
Throughput versus Speed	Pause time	10
Delay versus Speed	Pause Time	10

Figure 3: Parameters computed

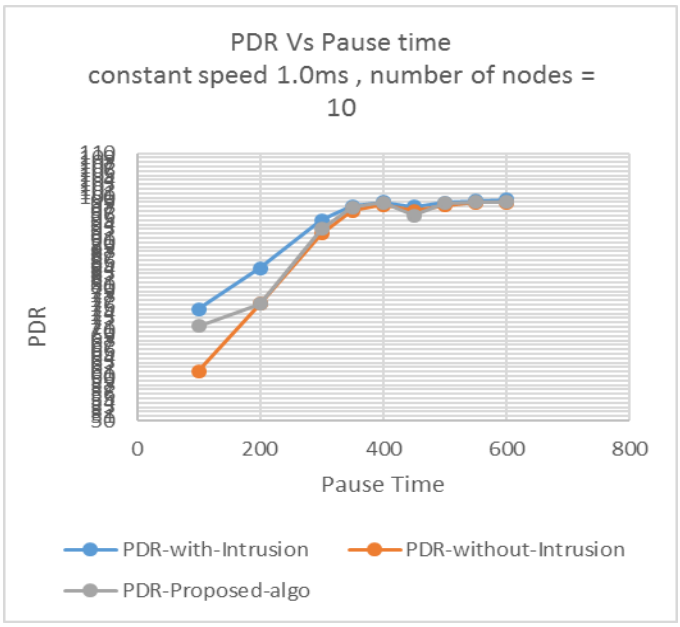

Figure 4: PDR Vs Pause time keeping constant Speed

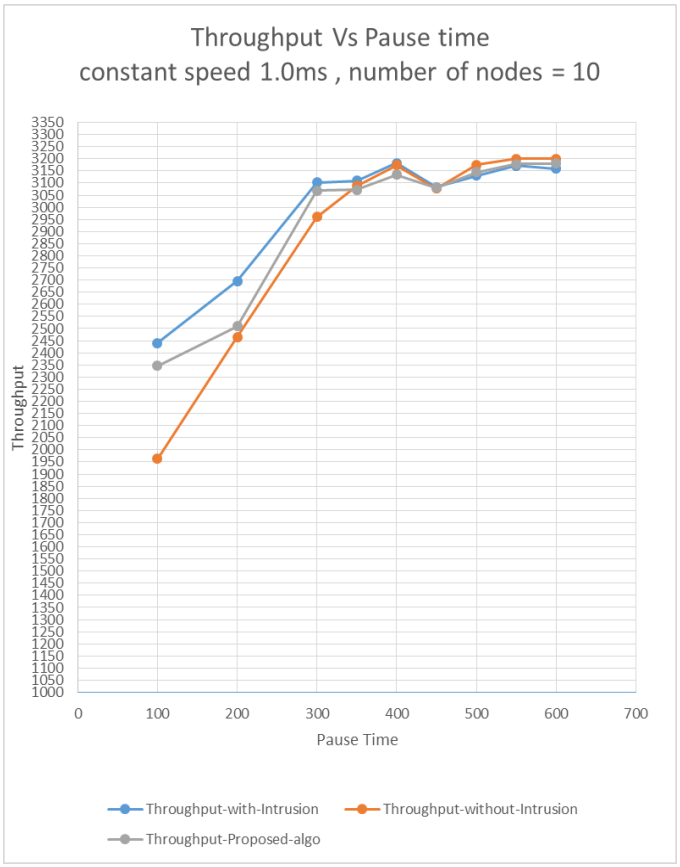

Figure 5: Throughput Vs Pause time keeping constant Speed

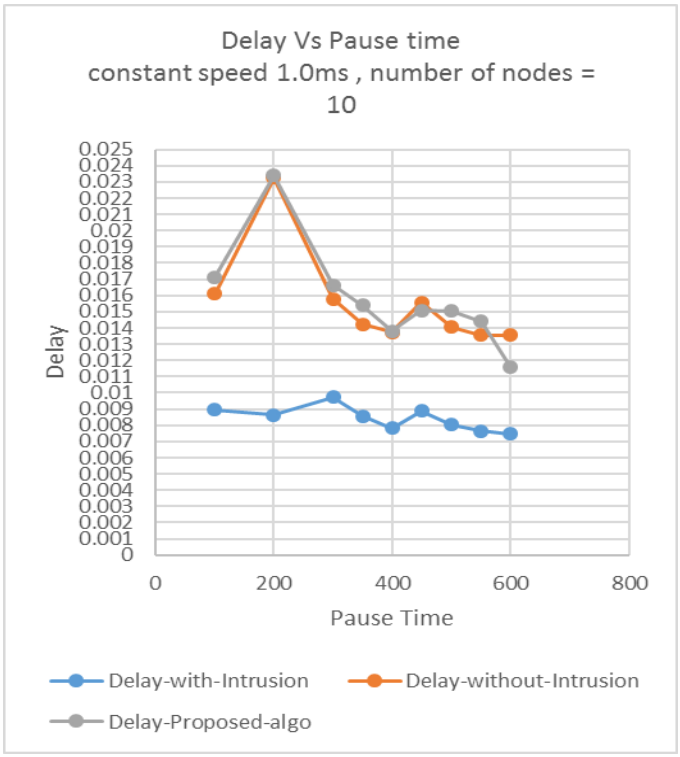

Figure 6: Delay Vs Pause time keeping constant Speed

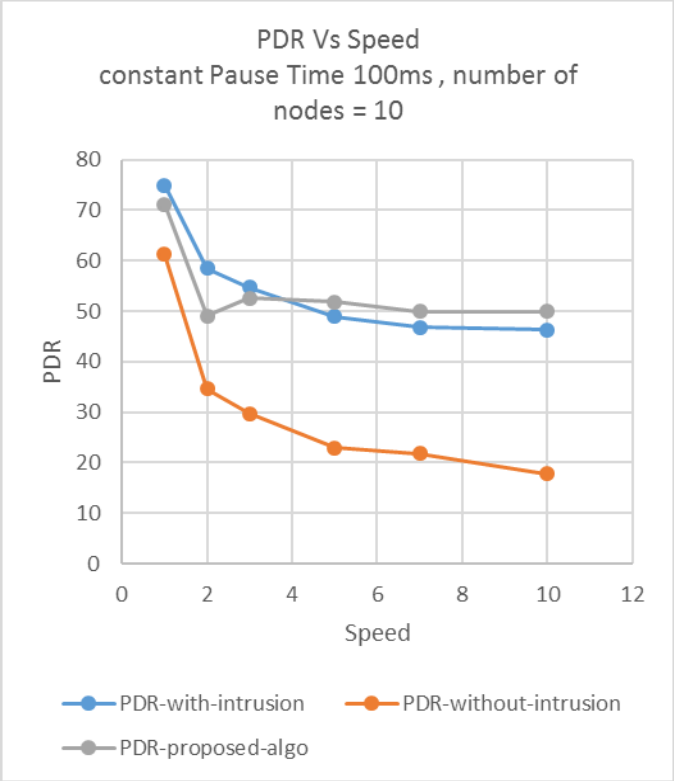

Figure 7: PDR Vs Speed keeping constant Pause Time

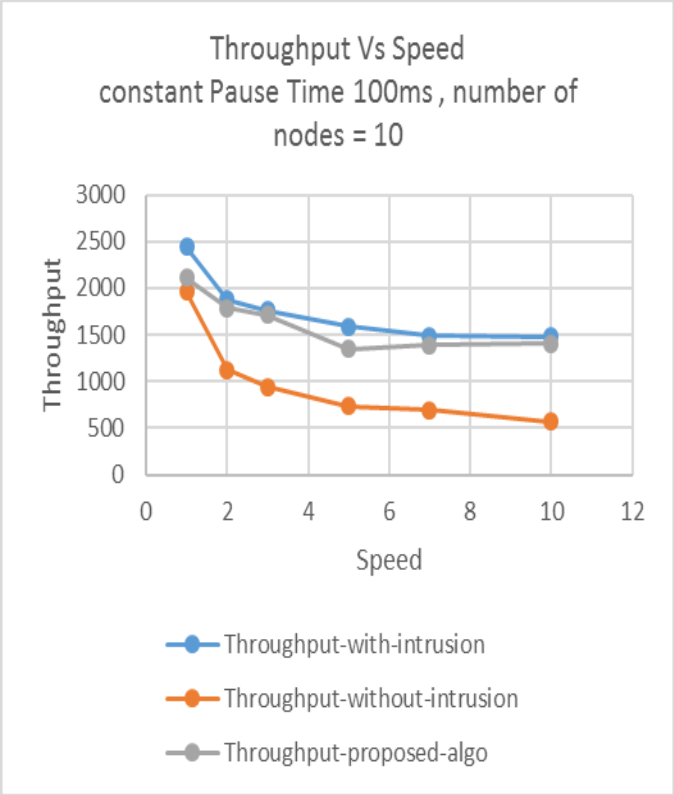

Figure 8: Throughput Vs Speed keeping constant Pause Time

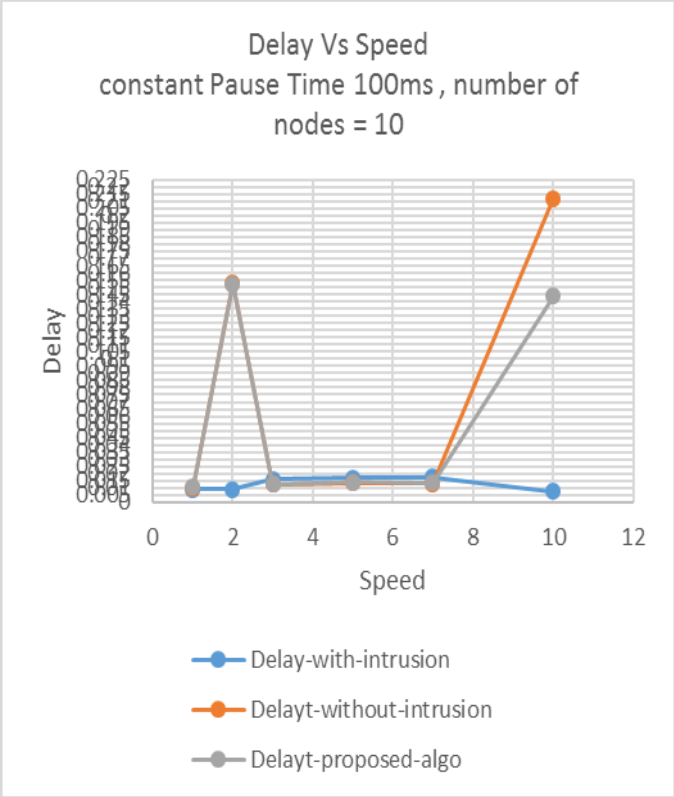

Figure 9: Delay Vs Speed keeping constant Pause Time

The results show that the proposed method is able to handle the intrusion in time in most of the cases. the delay is slightly more but that is due to excessive calculation that occur during route repair. Packet delivery improves which is major deciding factor in any protocol. Average accuracy achieved in terms of PDF is from 5 to 15 percent.

RELATED WORK

Routing protocols for MANETs do not provide provisions for security of networks, they assume that the nodes work in a genuine manner and cooperate in routing the data packets from source to destination. The major reason for this is limitations of resources like power and bandwidth. Researchers have proposed intrusion detection systems which are either anomaly based or signature based systems. These proposed methods by researchers either work standalone on each legitimate node or work corporately involving cluster heads etc.

Marti et al [2] elucidate method called watchdog, which dynamically measures behavior of nodes to identify normal and malicious nodes. Such nodes which are deemed to be malicious are bypassed using mechanism called Pathrater. Their work is based on DSR protocol. Implementing the said method authors observed that the throughput is increased under all levels of node mobility's. Watchdog works in promiscuous mode by listening to neighbors to find whether they have forwarded the sent packet or not. Pathrater works on information gathered by watchdog to decide whether to send the next packet to neighbor in question or not. Watchdog has certain weaknesses due to which it may lose to detect a

misbehaving node. The reasons could be due to ambiguous collision, collision at receiver or if a node has limited transmission power. Pathrater computes path reliability metric for various possible paths to a destination and chooses one with highest reliability.

Peng Ning and Kun Sun [3] have performed a case study of various insider attacks for AODV protocol. This paper elucidate how AODV routing messages could be aimed for various attacks from within the Ad hoc network. Authors have categorized attacks to be atomic misuse type or compound misuse type. They have implemented these attacks and have studied their impact. Actions have been identified that an attacker within the network can take to change routing messages and what all misuse goals can be achieved by these changes. Actions on which work has been done are dropping of routing messages, modifying and forwarding routing messages, sending a faked message as reply and sending a faked message on its own without being asked for. As a result of these actions a malicious node can perform attacks like route disruption, route invasion, node isolation or resource consumption.

A Al-Roubaiey et al [4] in this paper authors have worked with DSR
Protocol and basis of the work is watchdog algorithm. This paper proposes solution for receiver collision problem of watchdog. Earlier a solution was proposed which was TWOACK scheme but this incurred much overhead. The proposed solution in this paper has used end-to-end acknowledgement which will reduce the overhead. Nodes in the network by default work in adaptive acknowledgement mode but after a predefined period the node work in TWOACK mode on the basis of whether the acknowledgement has been received or not received within timeout period. Involvement of additional mode detects the malicious node without incurring high overhead.

Adnan Nadeem and Michael P. Howarth [5] elucidate method which rests on anomaly and knowledge based intrusion detection technique. The mechanism gives weightage to flexible intrusion response mechanism based on factors like severity of attack, degradation of performance of network and what will be the impact of actions taken against the detected intrusion. Authors use clustered manet organization, implementation has been done for AODV protocol. The solution incurs very low overhead on network traffic.

A. R. Rajeswari et al [6] in this paper authors have used clustering approach wherein each node can work as a slave or a master node. Cluster is formed of concentric circular arears, cluster head being at the center of the cluster. Each layer is assigned a layer number. Starting from inner most circle assigned layer number zero and increasing outwards. Back-off duration determines who would be the cluster head. Determination of back-off duration of a node is based on residual energy and maximum energy of the node. Cluster head broadcasts packet with certain TTL value which controls the concentric layers and cluster members, it also maintains the cluster table to determine the number of nodes in the cluster. Cluster key is used by cluster head while transmitting the data packets. Cluster key together with information stored in cluster table is used to identify a hidden malicious node.

CONCLUSION

Method proposed in this paper is based on collecting the RREP messages from intermediate nodes and the destination, thereafter messages are clustered using K-means algorithm. The results show that the proposed scheme works as per the plan described. Accuracy factor in terms of PDR increases and it gives more robust and stable delivery. System is able to cope with more than one intruder in most of the cases. Though the delay is increased slightly but it is bearable when delivery gets more smooth and better in most of the cases. Some of the fading effects are yet to be taken care of. The proposed scheme will be able to deal with this issue as well. Work is on to deal with this factor.

REFERENCES

[1] C. Perkins “Ad Hoc On-Demand Distance Vector (AODV) Routing”, Network Working Group RFC 3561, 2003
[2] Sergio Marti et al Mitigating Routing Misbehavior in Mobile Ad Hoc Networks”, Mobicom 2000 proceedings of the 6th annual international conference on Mobile computing and networking page 255-265
[3] Peng Ning and Kun Sun “How to misuse AODV: a case study of insider attacks against mobile ad-hoc routing protocols” Elsevier, Ad Hoc networks, 2004
[4] A. Al-Roubaiey et al “AACK: Adaptive Acknowledgement Intrusion Detection for MANET with Node Detection Enhancement”, 24th IEEE international conference on advanced information networking and applications, 2010
[5] Adnan Nadeem and Michael P. Howarth “An intrusion detection & adaptive response mechanism for MANETs”, Elsevier Ad Hoc networks, vol 13 part B, 2014, page 368-380
[6] A. R. Rajeswari et al, “Malicious Nodes Detection in MANET Using Back-Off Clustering Approach”, Circuits and Systems, 2016,7,2070-2079
[7] Bing Wu et al, “A Survey on Attacks and Countermeasures in Mobile Ad Hoc Networks”, Wireless/Mobile Networks Security, Springer, 2006
[8] Peyman Kabiri and Mehran Aghaei, “Feature Analysis for Intrusion Detection in Mobile Ad-hoc Networks”, International Journal of Network Security, Vol 12, No.1, page 42-49, 2011
[9] Farhan Abdel-Fattah et al, “Dynamic Intrusion Detection Method for Mobile Ad Hoc Network Using CPDOD Algorithm”, IJCA Special Issue on “Mobile Ad-hoc Networks”, 2010
[10] Kemal Bicakci and Bulent Tavli, “Denial-of-Servive attacks and countermeasures in IEEE 802.11 wireless networks”, Elsevier Computer Standards & Interfaces, 31, 2009
[11] Ningrinla Marchang and Raja Datta, “ Collaborative technique for intrusion detection in mobile ad-hoc networks”, Elsevier Ad Hoc Networks, 2007

[12] Sergio Pastrana et al, "Evaluation of classification algorithms for intrusion detection in MANETs", Journal: Knowledge-Based Systems, Vol 36, page 217-225, 2012

[13] P.M. Mafra et al, "Algorithms for a distributed IDS in MANETs", Journal of Computer and System Sciences, Vol 80, issue 3, page 554-570, 2014