International Journal of Applied Research

**ISSN Print:** 2394-7500
**ISSN Online:** 2394-5869
**Impact Factor:** 5.2
IJAR 2017; 3(1): 533-537
www.allresearchjournal.com
Received: 12-11-2016
Accepted: 13-12-2016

**Ritu Jaglan**
S.U.S. Govt. College, Matak
Majri, Karnal, Haryana, India

**Dr. Swantatar**
IKGPTU, Kapurthala,
Jalandhar, Punjab, India

**Correspondence**
**Ritu Jaglan**
S.U.S. Govt. College, Matak
Majri, Karnal, Haryana, India

# Proposed scheme to handle intrusion detection in manet

**Ritu Jaglan and Dr. Swantatar**

**Abstract**

MANETs are self-organising, infrastructureless spontaneous network and provides high degree of flexibility to its user. Security is the major concern among various research issues of MANETs. The paper proposes an algorithm for recovery from intruder based on AODV protocol. The intruder can be hacker from outside or within the MANET. The attack considered is direct or active. An algorithm has been proposed which takes care of intruder. Within the repair phase the proposed scheme is able to rectify the existing scheme and takes care of various metrics used for adhoc network like packet delivery ratio, throughput and average-delay produced.

**Keywords: MANET, AODV, Intrusion, Security, IDS (Intrusion Detection System)**

## Introduction

Networking technologies are going towards wireless communication and emphasis is on anytime anywhere connection establishment. MANETs are the best solution for it as they do not require any special intrastructre for connectivity and users are free to connect themselves as per their requirements. When such a free environment is available, security [3, 4] is of prime concern as anybody can have malafide intensions to compromise data or cause damage to the network. Intrusion may be external or internal in the network. Security in wireless [3, 4] network from intrusion is achieved either using prevention like encryption and authentication techniques or detection mechanism like IDS (Intrusion Detection System). The purpose of intrusion detection system is to alert the users about possible attacks on time so that they can be handled properly by the network. There are two main types of IDS [2] namely anomaly based IDS and misuse based IDS. In anomaly based intrusion detection system normal user profile are taken into consideration and any activity that differentiate from the normal one is considered as intrusion. Unknown attacks may be easily detected using anomaly based intrusion detection system [14]. Whereas in misuse based detection system stores the attacker's activity or intruder's profile and then match them with the activities of nodes in the network. Possibility of false detection is removed in misuse based IDS. When both anomaly and misuse based technique used collectively IDS is termed as hybrid IDS. While designing the intrusion detection system it has been assumed that attackers are intelligent enough and are of no shortage of resources. IDS detects the malacious node or intruder and avoid it and then remove the same from the network. It performs mainly three functions [1, 2]:

1. Observe the network and Collect information/data
2. Process and Analyse data
3. Detect intruder and Alert the system

There are two types of protocols used in MANET categorised as proactive and reactive routing protocols. The present work has been carried out using AODV (Adhoc OnDemand Distance Vector) which is a reactive routing [15] protocol. It consists of two phases namely [13]

- Route Discovery Phase uses Route Request (RREQ) and Route Reply (RREP) packets to discover the route from source to distination
- Route Maintanenace Phase uses HELLO packet and route error (RERR) packet in order to maintain the route and inform about the error.

## Literature Survey

The survey explains various IDS on the basis [1, 14] of their underlying protocols, architecture and types of attacks addressed by them. There are four types of architectures used in IDSs namely [2]

- Standalone IDS
- Distributed and collaborative IDS
- Hierarchical IDS
- Mobile agent IDS

The most favorable IDS architecture for ad hoc network may rely on infrastructure of the network itself. Wireless adhoc networks can be configured in either multi-layered or flat network infrastructure. Flat network infrastructure is suitable for the civilian application like a classroom or conference. It treats all nodes in the network at the equal level and all nodes may take part in the function of routing protocol. Whereas in multi-layered network infrastructure the nodes are organised in cluster according to their transmission ranges, and one node is to be designated as the cluster head to centralize the routing information among clusters. This kind of infrastructure is useful for in the military applications.

IDSX (2007) [5, 14] was a cluster-based solution which used an extended architecture.IDSX was compatible with any routing protocol. Simulation results show that the IDSX solution hardly produced any false positives. Type of attack addressed is dirty packet forwarding. Anomaly-based intrusion detection schemes could be deployed as the first line of defence. The proposed approach in [5] works within preset boundaries. In general, these are quite feasible and practical enough considering the nature of ad hoc networks. However, some of these may also be considered as the limiting constraints. IDSX has not been compared with any of the existing IDS solutions. Also, the proposed two-step approach would make the task ofintrusion detection expensive in terms of energy and resource consumption.

**Neural Network and Watermarking Technique (2007)**: In another innovative approach in [6], a solution is proposed using the concept of unsupervised learning in Artificial Neural Networks using Self-Organizing Maps. AODV is used as the underlying routing protocol. The technique named eSOM used a data structure called U-matrix which was used to represent data classes. Those regions which represented malicious information were watermarked using the Block-Wise method. Regions representing the benign data class was marked using the Lattice method. When a new attack is launched it causes changes in the pixel values. eSOM [14] and the Watermarking technique can together identify if any pixel has been modified. This makes it very sensitive towards detecting intrusions. The authors claim that the solution is 80% efficient and remains consistent even with variations in mobility. Some of the drawbacks of this work [6] are, the IDS employing eSOM would be trained in regular time periods. This results in additional overhead and takes a toll on the energy efficiency of the algorithm. However, the proposed intrusion detection engine has not been employed on various routing protocols for the detection of various types of attacks only roting behaviour and route utilization attack is considered.

**A leader election model (2008):** for IDS in MANET based on the Vicky, Clarke and Groves (VCG) Model was suggested in [7]. This requires every node to be as honest as possible. Leaders are elected in a manner which results in optimal resource utilization. Leaders are positively rewarded for participating honestly in the election process. By balancing the resource consumption amongst the nodes, a higher effective lifetime of the nodes was achieved. Experimental results indicate that the VCG model performs well during leader election by producing a higher percentage of alive nodes. However, the simulation results indicate that the normal nodes will carry out more duty of intrusion detection and die faster when there are more selfish nodes. Besides, as selfish nodes do not exhaust energy to run the IDS service, the percentage of packet analysis decreases with time. This is a severe security concern. In the case of static scenarios, the model elects the same node as leader repeatedly. This causes the normal nodes to die very fast.

CONFIDANT (2002) [8, 14], another approach, similar to Watchdog and Path-rater scheme used DSR as its underlying protocol, has been proposed to overcome the drawbacks of the Watchdog and Path-rater by ignoring misbehaving nodes in the routing process [8]. Every node identifies its neighbours as friends and enemies, based on trust. Friends are informed of enemies. CONFIDANT claims that the packet delivery ratio is very high (97% and above). However, CONFIDANT keeps the packet delivery ratio high even in a very hostile environment, with the assumption that enough redundant paths are available to reach the destination node, bypassing the malicious ones. This assumption may not always hold. Also, in comparing the throughput of clients and servers, the CONFIDANT fortified network performs very poorly in contrast to the benign network.

SCAN (2006) [9, 14] is based on two central ideas. First, each node monitors its neighbours for routing or packet forwarding misbehaviour, independently. Second, every node observes its neighbours by cross validating the overhead traffic with other nodes. Nodes are declared malicious by a majority decision. This assumes that the network density is sufficiently high. However, in SCAN the network services are temporarily halted during intrusion detection. The lack of mobility reduces the detection efficiency. The assumption that network density is high may not always hold. Increase in mobility results in higher false positives. Besides, the packet delivery ratio can be heavily affected in the interval during which an attack is launched and when it is detected. Also, the communication overhead for SCAN grows with increase in the percentage of malicious nodes and with mobility.

In HIDS (2008) [10, 14], another approach to the IDS has been proposed which addressed packet drop, black hole and resource utilization attacks. HIDS is based on trust or reputation or honesty values of the mobile nodes. The trust value of a node is dynamically increased or decreased depending on its behaviour. When a node behaves normally, it is positively rewarded; malicious activity results in negative rewards for that node. The trust on a node is recomputed based on its current honesty rate, and the rewards that it has earned. A comparative study between SCAN and HIDS shows that the latter involves lower storage and communicational overhead than SCAN. HIDS is inherently protected against false positives. However, maintaining up-to-date tables at different nodes, as required by HIDS, may not be an energy-efficient strategy. Also the proposed HIDS offers only a generic architecture for secure route detection. More detailed testing is required before it can be used for secure routing in MANET applications.

In OCEAN (2003) [11, 14] was proposed as another extension to the DSR protocol. OCEAN also uses a monitoring system and a reputation system. The proposed solution exchanges second-hand reputation messages. OCEAN implements a stand-alone architecture to avoid phantom intrusion detections. Depending on whether a node participates in the route discovery process, OCEAN can detect misbehaving nodes and selfish nodes. However, the detection efficiency of OCEAN rapidly decreases with increase in the density of misbehaving nodes. Simulation results show that at high threshold values, other second hand protocols perform better with high mobility of the nodes. Also, the mobility model simulated for OCEAN is not very realistic. At high mobility, OCEAN is very sensitive to change of the threshold parameter, while second hand protocols are more consistent over varying threshold limits. OCEAN is not quite effective in penalizing misleading nodes.

A hybrid solution (2010), proposed in [12], combines the Watchdog and Path-Raters scheme proposed by Marti *et al*. and SCAN [9]. However, neither SCAN nor Watchdog and Path-raters address the mobility issue that well. As a result, this hybrid solution also suffers from the same problems. Besides, there are no fixed nodes which can behave as umpires. There must be some kind of a leader election model which runs in every node to select the Umpire nodes. This results in an increased overhead and energy consumption. The authors did mention the scenario where Umpire nodes themselves can become malicious. However, it still remains as a drawback of the method. In order to detect DoS attacks like flooding, the criteria for attack detection cannot be so rigid. Also, the history of a node that had being behaving normal, should be taken in to consideration before writing it off as malicious as soon as it deviates from normal behaviour.

**Proposed Plan**

Detailed study of AODV routing protocol has been done. And a modified algorithm is designed where changes has been made in repair phase. AODV carries out local repair using TTL (time to live).Proposed scheme makes changes in its repair mechanism. Figures given below describe the proposed plan in clear and efficient manner. Route Request Phase is same as that of AODV. Route Reply Phase is same as that of AODV. Route repair mechanism of AODV protocol has been modified in two phases as explained here.

In Phase I intruder is detected using sequence number policy.

In Phase II algorithm is used to bypass the intruder and select a new path to carryout recovery of damage done by intruder.

Figure 1 describe the normal routing process of AODV protocol where route has been established between source node S and destination node D. It follows normal route request and reply phase using RREQ and RREP packet. The network consists of 9 nodes from sequence numbers 1 to 9.

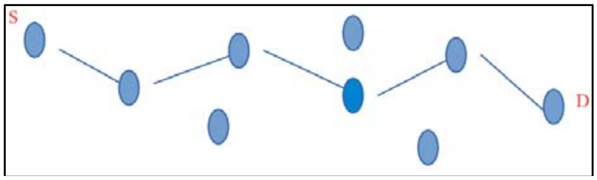


**Fig 1: Normal execution**

Phase I: Intruder Detection

- Nodes perform checkup of Route-Table.
- After reply phase when route is established, Seq. No. are checked after each bicon.
- If a particular sequence number is out of sequence or out of range, the node is treated as intruder.

Figure 2 explains how proposed algorithm detects the intruder during route recovery phase of AODV protocol. Here the node N shown in red colour is detected as false node or malafide node as its sequence number is found out of range in the MANET where valid sequence numbers are from 1 to 9.

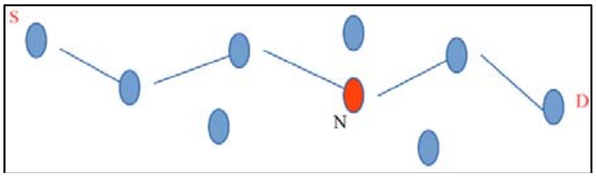


**Fig 2:** Intrusion by malafide node

Phase II: Repairing the intruder

- Makes changes in route request (RREQ) in enteries of routing table.
- A new route request is sent from node which is one hop back the intruder node (n to n-1).
- Then from node n-1 a new path is created and intruder is isolated or bypassed.

Figure 3 shows that the intruder node has been isolated and removed from the network and a new path as shown by different colour line has been created by the previous node from the intruder node N. In this way the network has been recovered by the proposed algorithm.

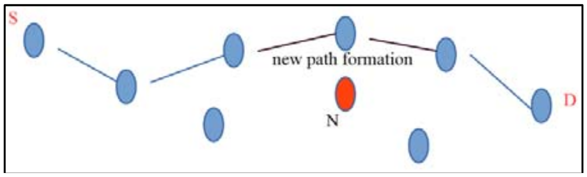
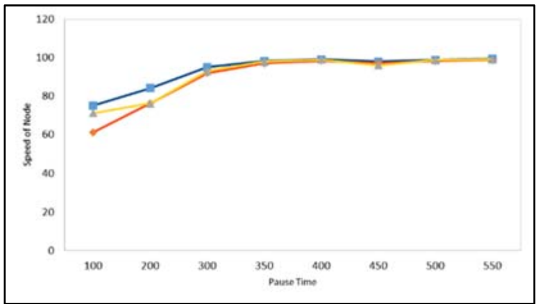


**Fig 3:** Recovery from intrusion

The performance of algoritm is checked using various metrics for mobile adhoc networks like packet delivery ratio, throughput and average-delay. The proposed algorithm is executed in NS2 simulator for small, medium and large network scenario taking 10, 20 and 50 nodes respectively. Pause time in ms and speed of node in m/s are taken as the parameter to check the results of different metrics. The result section includes the graphs which shows the performance of the modified algoritm.

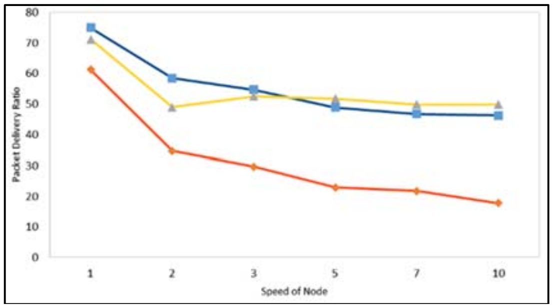
**Results**

Graphs are used to describe the results obtained from the execution of proposed plan. Each graph displays three scenarios of AODV routing protocol namely normal (in blue colour), after the intrusion (in red colour) when intruder enters the scene and creates havoc and then after the network is being repaired using the proposed algorithm is shown in yellow colour.



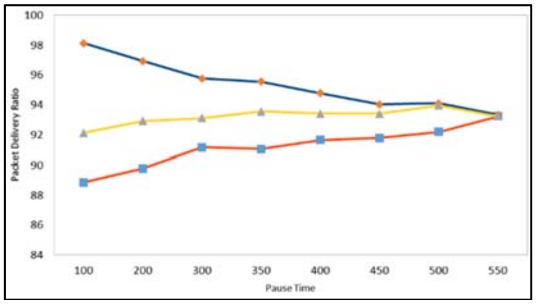
**Graph 1:** Performance of AODV protocol in MANET of 10 nodes

Graph 1 is description of 10 nodes scenario with pause time as a function in three different scenes. Pause time varies from 100 ms to 550 ms. Incase of 10 nodes intruder does not effect the network to large extent and thus situation is not so scritical, still it has been shown using red notation. And then proposed algorithm has been applied on the scenario. New scheme takes care of intruder, either byepasses it or removes it. Results shows that the new scheme has been able to modify the results in positive direction as displayed by yellow line. This is in accordance with the proposed scheme. More results has been taken using 20 and 50 nodes and there the situation will be more handy for expalination purposes.



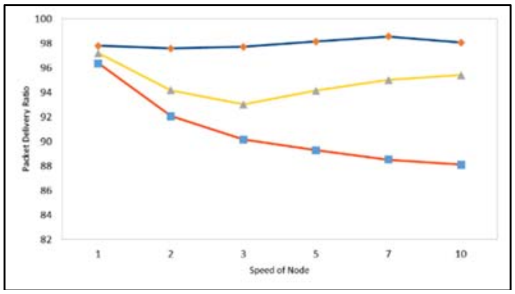
**Graph 2:** Performance of AODV protocol in a MANET of 10 nodes

The graph is representation of PDR with speed as a function for 10 nodes in three scenes of AODV routing protocol. Speed has been varied from 1 m/s to 10 m/s. Normal scenario is blue line notation and red line notation denotes entry of an intruder. Yellow line is depiction of recovery from intruder as proposped by new scheme. As desired the propsoed scheme is able to take care of PDR and is reaching the target at almost normal scene. As shown increase of 25% to 65 % is a great recovery particulary at higher speed of 10m/s.



**Graph 3:** Performance of AODV protocol in a MANET of 50 nodes

Graph 3 is shows the execution of AODV protocol in MANET of 50 nodes for varying pause time from 100 ms to 550 ms. Graph clearly depicts the huge reduction in packet delivery ratio caused by malacious node (intruder) as blue line is at comparatively much higher level/value than red line. The increased traffic may be the reason for intruder to effect the performance of neighbouring nodes. In case of 10 nodes this situation is not so critical since the traffic is very less. After applying the proposed algorithm to repair the false or malacious node considerable improvement in packet delivery ratio has been achieved shown in graph by yellow notation.This shows the proposed algorithm is working well to improve the performance of AODV protocol as the network becomes more denser.



**Graph 4:** Performance of AODV protocol in a MANET of 50 nodes

The graph is representation of PDR with speed as a function for 50 nodes in three scenes of AODV routing protocol. Speed has been varied from 1 m/s to 10 m/s. Normal scenario is blue line notation and red line notation denotes entry of an intruder. Yellow line is depiction of recovery from intruder as proposped by new scheme. As desired the propsoed scheme is able overcome the loss introduced by the intruder or malacious node and recover the PDR which is very close to normal profile of the network. The graph displays that as the speed of node increases the normal PDR reaching upto 98% and intruder reduces it to 88% which is recovered by the proposed scheme upto 96% is asignificant gain.

## Conclusion

The paper is a detailed study of AODV with three views as Normal, with intruder and Repair. The Repair has been done in second phase of the AODV. The Local Route repair has been modifed and various metrics has been used to verify the scheme. Two parameters as Speed and Pause time has been used with various scenes as 10, 20 and 50 nodes. The new scheme has been able to repair the existing scheme and results are shown using graphs. The whole work has been conducted using NS2 and using various scenarios with Random wayPoint Model.

More work will be conducted for other protocols also inclusing DSR and TORA. The effect of fading will also be considerd and more emphasis will be on use of stable routes.

## References

1. Novarun Deb, Manali Chakraborty, Nabendu Chaki, The evolution of IDS Solutions in Wireless Adhoc Networks to Wireless Mesh Network, IJNSA November, 2011, 3(6).
2. Ganesh J Solanke, Chandra PR. Literature Survey on IDS in MANET, IJSET, 2015, 4(1). ISSSN 2278-7798.

3. Kush A. Seema Evaluation of Routing Schemes for MANET in A. Mantri *et al.* (Eds.): HPAGC, CCIS 169, pp. © Springer-Verlag Berlin Heidelberg. 2011, 575-580.
4. Kush A, Divya, Vishal, Energy efficient Routing for MANET, Intl conf on applied and communication tech, Elsevier Pub. 2014, 189-194.
5. Chaki R, Chaki N. IDSX: A Cluster Based Collaborative Intrusion Detection Algorithm for Mobile Ad-Hoc Network, Proceedings of the IEEE International Conference on Computer Information Systems and Industrial Management Applications (CISIM), 2007.
6. Aikaterini Mitrokotsa, Nikos Komninos, Christos Douligeris, Intrusion Detection with Neural Networks and Watermarking Techniques for MANET, International Conference on Pervasive Services, pp., IEEE Int'l Conference on Pervasive Services, 2007; 118-127.
7. Noman Mohammed, Hadi Otrok, Lingyu Wang, Mourad Debbabi, Prabir Bhattacharya, Mechanism Design-Based Secure Leader Election Model for Intrusion Detection in MANET, IEEE Transactions on Dependable and Secure Computing, 2008, 99(1).
8. Buchegger S, Le J, Boudec, Performance Analysis of the CONFIDANT Protocol (Cooperation Of Nodes - Fairness In Dynamic Ad-hoc NeTworks), Proceedings of the 3rd ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc'02), 2002, 226-336.
9. Yang H, Shu J, Meng X, Lu S, SCAN: self-organized network-layer security in mobile ad hoc networks, IEEE J. on Sel. Areas in Communications, 2006; 24:261-273.
10. Sil P, Chaki R, Chaki N. HIDS: Honesty-rate based collaborative Intrusion Detection System for Mobile Ad-Hoc Networks, Proc. of 7th IEEE International Conference on Computer Information Systems and Industrial Management Applications (CISIM), 2008.
11. Bansal S, Baker M, Observation-Based Cooperation Enforcement in Ad hoc Networks, Research Report cs.NI/0307012, Stanford University, 2003.
12. Ayyaswamy Kathirvel, Enhanced Triple Umpiring System for Security and Performance Improvement in Wireless MANETS, International Journal of Communication Networks and Information Security (IJCNIS). 2010, 2(2).
13. Alex Hinds, Michael Ngulube, Shaoying Zhu, Hussain Al-Aqrabi. A Review of Routing Protocols for Mobile Adhoc Networks, International Journal of Information and Education Technology. 2013, 3(1).
14. Apurva Kulkarni, Prashant Rewagad, Mayur Agrawal, Literature Survey on IDS of MANET, International Journal of scientific research and management (IJSRM). 2015; 3(9):3549-3552. www.ijsrm.in ISSN (e): 2321-3418.
15. Taneja S, Kush DA, Makkar A. End to End Analysis of Prominent on Demand Routing protocols, International Journal of Computer Science and technology. 2011; 2(1):42-46.