International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

Intrusion Secure Algorithm for AODV

Ekta[1], Nasib Singh Gill[2]

[1,2]Department of Computer Science & Applications Maharshi Dayanand University Rohtak, India

Abstract: ***A mobile Adhoc network (MANET) is distinguished by their mobile nodes, multihop wireless connectivity, absence of infrastructure, communicating environment and its dynamic topology. In Ad hoc network routing is reactive on-demand philosophy where the routes are established only when required. Whereas stable routing, security and power efficiency are considered the major issues in this field. As far as the Adhoc environment is concerned, the network is accessible to both the legitimate and malicious nodes. Many security models have been proposed to detect these malicious nodes. The proposed approach named malicious node detection IDS is intended to incorporate security aspect on existing protocols. This paper checks the attacks occurring in MANETS and tries to detect those attacks by understanding the situation in case of attack. Scheme has been incorporated on AODV and results have been calculated using NS2.***

Keywords: Adhoc networks, AODV, IDS, Performance Evaluation

1. Introduction

An Ad hoc is a wireless network working technique which is a collection of several dynamic mobile devices with interfaces and networking capability. These devices have inbuilt routers and are adaptive in nature. The developed network can be formed and deformed according to the requirement without any help of a central system administration in the network. These days the network of such characteristics are widely used in designing of virtual classrooms, military communications, vehicular communications, emergency searches and rescue operation, personal communications, communication setup in meetings, conferences and exhibitions. Moreover, these networks are lifesaving systems as used by soldiers in battle fields to coordinate defense or several attacks, at airport and railway terminals for sharing important documents with the workers. It is a well-known fact that security of any system is the utmost concern and cannot be compromised at any cost. Manets are spreading at much higher rate in each and every sphere of life. Thus the security is pre-eminence and compelling topic. Several competitive approaches have been designed to detect the intruders in the networks. It is a tough task to beat the challenges present in wireless technology. These challenges include open network architecture, dynamic nodes, shared communicating medium, and continuously changing topology which is prone to multiple mobile attacks. Some main security attributes that are used to inspect the security state of the mobile Adhoc networks are- Availability, Integrity, Confidentiality, Authenticity, Non repudiation, Authorization and Anonymity. In this paper, a new IDS algorithm is proposed to detect the intruder in the network and to isolate the malicious node from the network. The proposed approach is implemented and analyzed in NS2 while graphs are plotted using Excel2013.

2. Intrusion Detection System

Manets being wireless systems are more prone to attacks by intruders as compared to wired networks. The flexibility provided by the open broadcast medium and the cooperativeness of the mobile devices (which have generally different resource and computational capacities, and run usually on battery power) introduces new security risks. Till today many IDS are proposed for wired systems. As MANETS developing features make them differ from wired, so new IDS are required for MANETS. So today new approaches are required to be designed to detect the attacks occurring in MANETS. Intrusion is any set of actions that attempt to compromise the integrity, confidentiality, or availability of a resource [1] and an intrusion detection system (IDS) is a system for the detection of such intrusions. There are three main components of an IDS: data collection, detection and response. Thus IDS are designed on attacks detection and their removal from the network.

3. Literature Review

The misbehaving node is mitigated instead of the whole route since there may be only one route to reach the destination and in removing the route would have made the destination unreachable. Also Identifies dishonest peers by constant evaluation on the node behavior. No false alarms can be raised by individual nodes. AODV routing protocol reduces overhead and does not require to update tables frequently. Security Aware AODV mitigates the malicious nodes [2].Several issues concerning developing reputation based selfish node detection in mobile ad-hoc networks have been discussed. Selfish or misbehaving nodes degrade overall system performance and cause a serious threat to multihop routing in MANETs. Reputation based models play an important role in detecting and isolating selfish nodes. Many approaches are available in the literature. But no approach provides a finite solution to the selfish nodes problem. [3] The mobile nodes interact with other for delivering packets from source to destination. The main function of the ad hoc routing protocols is to provide routing among nodes. They exchange routing messages between different mobile nodes in order to maintain routing information at each node. The data forwarding service consists of correctly relaying the received packets from node to node until they reach their final destination, following the routes selected and maintained by the routing protocol. Both of these applications are vulnerable to malicious attacks, which will lead to various types of malfunction in network layer [4]. The trust models based on certification-based

category are surveyed in the literature by M.Omar[5].Yih-Chun Hu et al. [6] used symmetric cryptography to secure adhoc networks by using one way hash chains or Markle hash tree as part of SEAD protocol for proactive routing. The problems identified with SEAD protocol are no provision of a secure initial key distribution, greater network traffic and count-to-infinity problem. Zapata [7] in its proposed protocol uses a new one-way hash chain for each Route Discovery to secure the metric field in an RREQ packet. It also uses asymmetric cryptography to initially authenticate participating nodes.

4. Security Service

he classification of security services is as follows [8]:

1. **Confidentiality:** Ensures that the information in a computer system and transmitted information are accessible only for reading by authorized parties. This type of access includes printing, displaying and other forms of disclosure, including simply revealing the existence of an object.
2. **Authentication:** Ensures that the origin of a message or electronic document is correctly identified, with an assurance that the identity is not false.
3. **Integrity:** Ensures that only authorized parties are able to modify transmitted information. Modification includes writing, changing, changing status, deleting, creating and delaying or replaying of transmitted information.
4. **Non repudiation:** Requires that neither the sender nor the receiver of a message be able to deny the transmission.
5. **Availability:** Requires that computer system assets be available to authorized parties when needed.

5. Proposed Algorithm

5.1 Assumptions

The following assumptions are considered in order to design the proposed algorithm:-

- A node interacts with its 1-hop neighbors directly and even with other mobile nodes through intermediate nodes using, multi-hop packet forwarding technique.
- Every mobile node is uniquely identified using unique_id in the network. This identification is provided to every node entering the network according to the existing mobile nodes in the network.
- The network is considered to be layered.
- The source and destination are not the intruders.

5.2 Steps of Algorithm

1: Route Request phase RREQ (same as AODV)

- Start route Request RREQ
- Initialize sequence numbers 1 to N as number of nodes varying 1 to N
- Designate Source node as ‘S’ and Destination as ‘D’
- RREQ is forwarded as Source routing
- AODV RREQ is followed
- Route reply is confirmed based on Shortest path as in AODV
- Route is established
- Call INTRUDETECT

2: Local Repair LREPAIR [9]

- Check link break = true
- Node upstream repair the route locally
- If destination not farther than MAX_REPAIR_TTL
- Node increments sequence number for destination broadcasts RREQ
- When node is discovered it waits for RREP
- Route is established
- Else call INTRUDETECT

3: Intrusion detection INTRUDETECT

- Check route table entry for each node
- If sequence number is greater than assigned N , follow steps 3 else return
- Check for node having higher sequence No.
- Block the node as M-Node
- Initialize Route request again
- Call RREQ
- Call INTRUISOLATE

4: Intrusion isolation INTRUISOLATE

- Source sends ICMP packets to route path.
- Route path sends ICMP packets to the neighboring intermediate nodes and update the route table and delete M-node entry
- ISOLATE the node as M-node.
- Initialize Route request again
- Call RREQ

6. Implementation of Proposed Algorithm and Result Analysis

When MANETS routing is discussed then its working is called better only according to the actual packets transferred between source and destination successfully without packets loss. This requires proper selection of routing path and algorithm designed for its working. AODV and proposed AODV concept have been used in this paper for the solution purpose. All simulations are performed in NS-2.34[10] on the platform Ubuntu13. The source destination pairs are spread randomly over the network. The mobility model is spread in area 1000x1000 with 10, 20 and 50 nodes. During this simulation, each node starts journey randomly from one point to other and source and destination are randomly chosen. The system is analyzed based on three parameters average delay, throughput and packet delivery ratio (PDR) with respect to pause time and speed respectively. Where pause time is considered as the time after which the node starts transmitting while speed is considered as the velocity with which the nodes are moving in the network. Following are the NS-2 animations which show the working of proposed approach in the network simulator according to the parameters considered for the system.

6.1 Metrics

- Delay: -The average end-to-end delay of data packets is the interval between the data packet generation time and the time when the last bit arrives at the destination.
- Throughput:-It is one of the dimensional parameters of the network which gives the fraction of the channel capacity used for useful transmission selects a destination at the beginning of the simulation i.e., information whether or not data packets correctly delivered to the destinations.
- Packet Delivery Ratio:-It is the percentage of number of packets received and dropped by total number of packets sent.

6.2 Parameters

The following are the network parameters considered for the proposed approach performance evaluation:-

- **Pause Time:** This is the time when all nodes in the network are motion less while the transmission is continued.
- **Speed:** This is the velocity with which nodes are moving in the network**.**

6.3 Simulation Environment

Table 1: Experimental Setup

Environment Size	1000 X 1000
Packet Size	512 BYTES
Queue Type	DROP TAIL/FIFO
Queue Length	50,60
Traffic Source	TCP
Protocols	AODV,DSR
Number Of Nodes	10,20,50
Pause Time	100,200,300,400,500
Speed	1,2,3,5,7,10
Simulation Duration	500,600 Sec

The following are the NAM files for the considered simulation environment:-

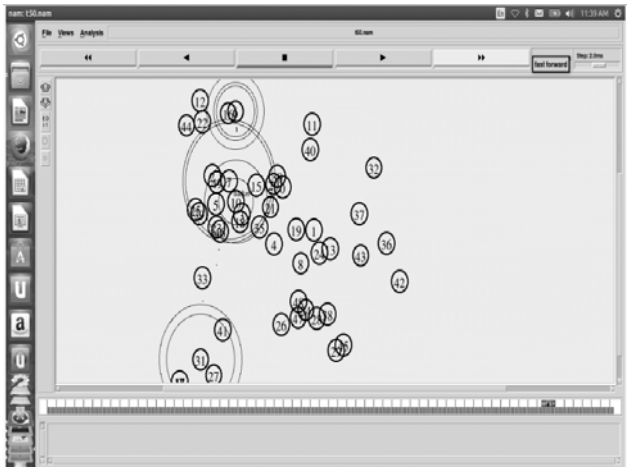

Figure 1: Shows working of AODV with hacker

The fig1. Shows the network simulation with hacker which clearly displays the dropping of packets during communication between the nodes in the network for given simulation time.

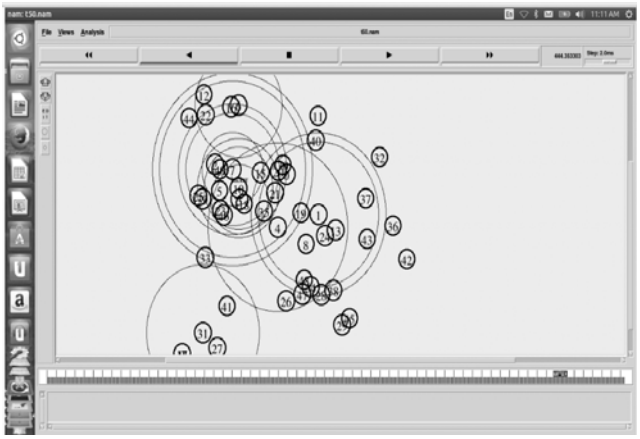

Figure 2: Shows working of AODV during transmission

The fig2 shows the transmission of packets among the different nodes using tcp connections.

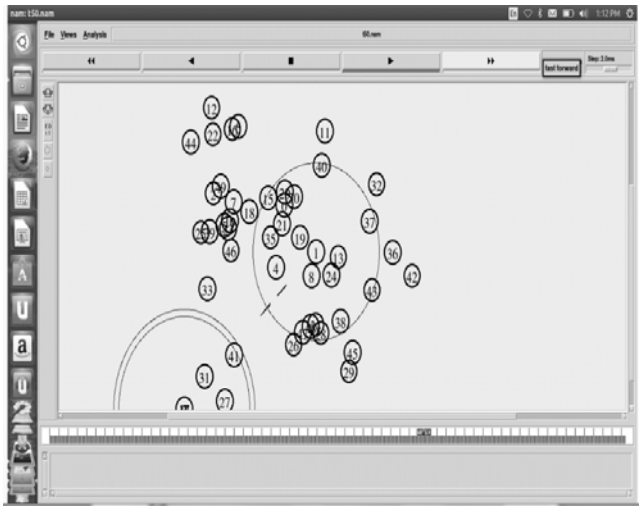

Figure 3: Shows working of AODV with proposed Approach

The fig3. Shows the working of the proposed approach, packets transmission among the different nodes during communication in the considered simulation time.

6.4 Graphs for Proposed Approach

The following are the graphs obtained for the proposed approach for 50 nodes:-

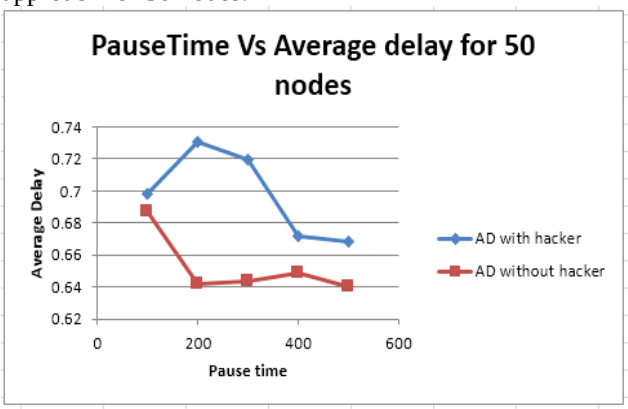

Figure 4: Graph for Pause time Vs Average Delay for 50 nodes

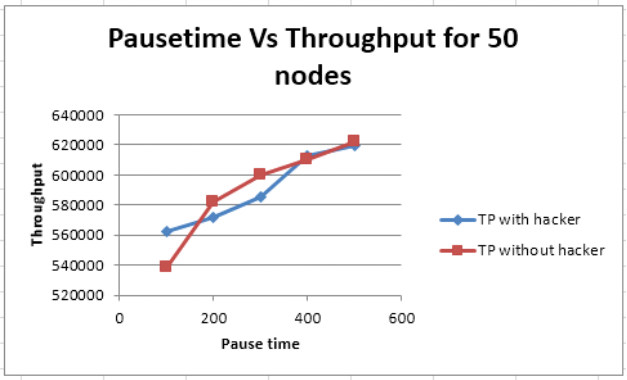

Figure 5: Graph for Pause time Vs. Throughput for 50 nodes

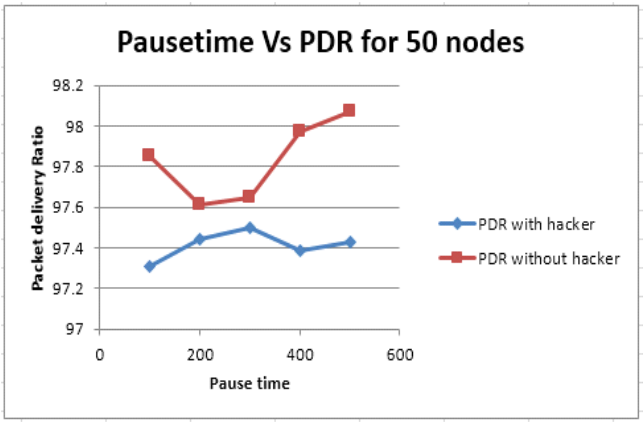

Figure 6: Graph for Pause time Vs. PDR for 50 nodes

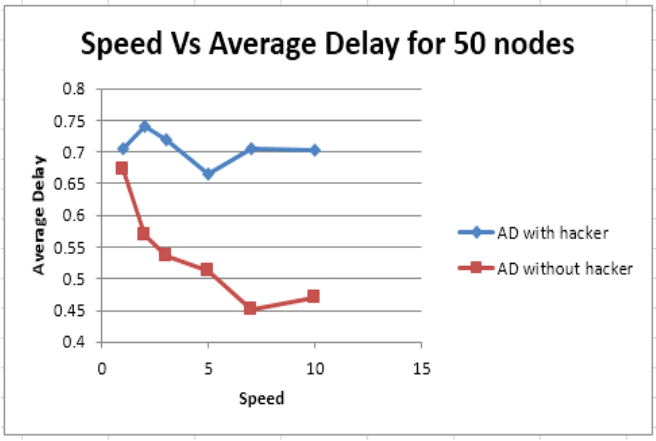

Figure 7: Graph for Speed Vs. Average delay for 50 nodes

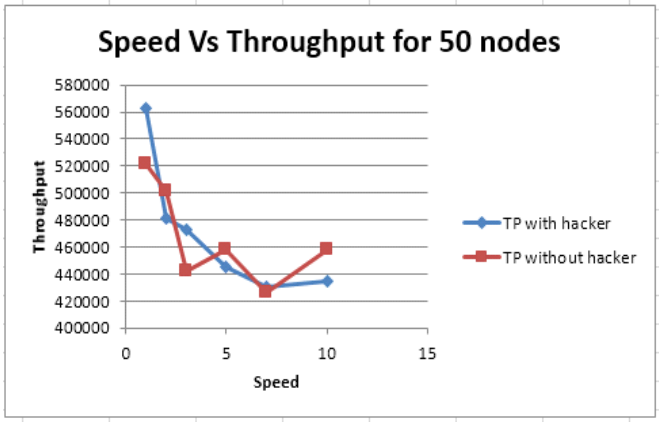

Figure 7: Graph for Speed Vs Throughput for 50 nodes

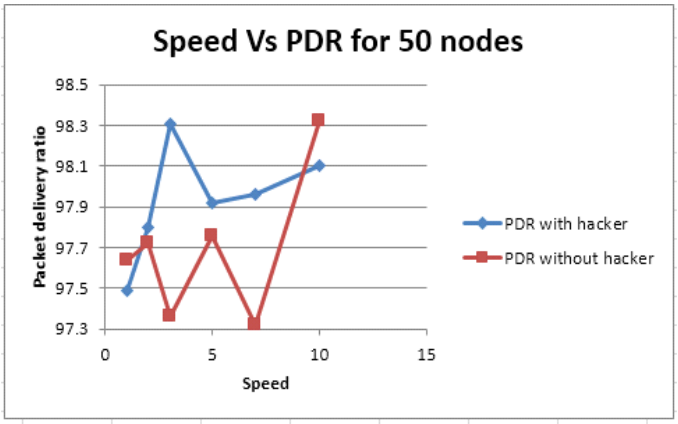

Figure 8: Graph for Speed Vs PDR for 50 nodes

The fig (2-7) shows the variations in the network while varying specified parameters. The graphs shows that the proposed plan works better although due to malicious nodes the performance of the network decreases to a limit which is as per the theory.

7. Conclusion

The routing protocols proposed for Mobile Ad hoc networks seem to meet the basic requirements like dynamically changing network topologies rather well. However, the security issues have been left primarily ignored. The MANET routing protocols must be secured from the viewpoint of the authentication, integrity and privacy. Moreover, the protection means can be optimized for every protocol based on the approach taken to routing.

Some MANET routing protocol developers suggest the application of IPSEC within the protocol to achieve the necessary security goals. This kind of approach is not totally adequate, due to the problems of replay etc. Moreover, the traditional security mechanisms such as link-level encryption or bi-directional tunnels are not adequate, due to the dynamic and unpredictable nature of MANET networks. The proposed is a security algorithm for routing protocols for detection of malicious nodes present in the network. The proposed approach presented a scheme to proactively prevent external attacks. The solution is specifically targeted for AODV protocol. The results of our implementation show that the effect of the overheads caused by our scheme is marginal and has negligible effects on network performance.

8. Future Work

This thesis, addressed the security issues pertaining to the routing protocols. The focus has been on on-demand protocols, specifically AODV. It would be interesting to study the issues specific to table driven protocols and look into schemes that work optimally when integrated with them. Though the proposed approach has done a very limited analysis of the internal attacks. Some of the attacks, especially those that are not deterministic, have not been handled. Intrusion detection schemes that analyze traffic profiles to detect intruders would be another challenging area to explore.

The detection of compromised nodes is a very tough problem especially in a dynamically changing network. In future we will try to enhance the capability of our IDS by making it more robust to detect the intrusions of all the types and to overcome the damage caused to the system during the hacking or intruding phase. The IDS capability to withstand more dynamic threats is to be enhanced more in future. And proposed algorithm can be enhanced more in terms of Quality of Service (QOS).

References

[1] Heady R, Luger G, Maccabe A, Servilla M (1990) The Architecture of a Network Level Intrusion Detection System. Technical Report, Computer Science Department, University of New Mexico
[2] ACEEE Int. J. on Network Security, Vol. 02, No. 01, Jan 2011
[3] S.SENTHILKUMAR,,J.WILLIAM "A Survey On Reputation Based Selfish Node Detection Techniques in Mobile Adhoc Network "E-ISSN: 1817-3195, http://www.jatit.org/volumes/Vol60No2/3Vol60No2.pdf Journal of Theoretical and Applied Information Technology20thFebruary 2014. Vol. 60 No.2
[4] S. Djahel,F. Nait-Ab desselam,Z. Zhang,Mitigating Packet Dropping Problem in Mobile Ad Hoc Networks: Proposals and Challenges,IEEE Communications Surveys and Tutorials, 13 (2011),658-672.
[5] M. Omar, Y. Challal, A. Bouabdallah, Certification-based trust models in mobile ad hoc networks: A survey and taxonomy, Journal of Network and Computer Applications 35 (2012) 268–286
[6] Kush A., Hwang C., "Proposed Protocol for Hash-Secured Routing Adhoc Networks", Masaum Journal Of Computing (iMJC), Volume 1, Issue 2, pp. 221-226, 2009.
[7] Kush A., Gupta P., Hwang C., "Secured Routing Scheme for Adhoc Networks", International Journal of Computer Theory and Engineering (IJCTE), Volume 3. pp. 1793-1799, 2009.
[8] William Stallings. Cryptography and Network Security: Principles and Practice, pages 3–12. Second edition.
[9] http://www.ietf.org/rfc/rfc3561.txt
[10] http://www.isi.edu/nsnam/ns/

Author Profile

Ekta, received B. Tech Degree in Information Technology from Kurukshetra University, Kurukshetra and pursuing M.Tech degree in Computer Science from Department of Computer Science & Applications, Maharshi Dayanand University Rohtak, Haryana, India.

Dr. Nasib Singh Gill, Professor Department of Computer Science & Applications; Director, Directorate of Distance Education and Director, MDU Alumni, Maharshi Dayanand University Rohtak, Haryana, India.