International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

An Novel Intrusion Detection System for Mobile Ad-hoc Network

Kushagra Jain[1], *Prof. Smitha G R*[2]

[1]Bachelor of Engineering RV College of Engineering kushagrajain.is19@rvce.edu.in
[2]Information Science and Engineering RV College of Engineering smithagr@rvce.edu.in

ABSTRACT-

Security is one of the most important constraints for the mobile ad-hoc network performance. Variety of attacks, degrade network lifetime and performance by influencing network resources such as battery power, bandwidth and data loss. Denial of Service is a type of attack in which the traffic is choked by the malicious node that denied network service for user. In order to provide secure communication and transmission, the researcher worked specifically on the security issues in mobile ad-hoc network, and many secure routing protocols and security measures within the networks were proposed. The motive of the work is to study about Denial of Service attack and how it can detected in the network. In the paper, an intrusion detection system is presented and experimented on NS-2. Performance of network is evaluated based on packet delivery ratio and throughput.

Keywords- Mobile Ad-hoc Network, Attacks, Intruder, Intruder Detection System

I. INTRODUCTION

Wireless mobile ad-hoc networks are getting popularity day by day due to its interesting facilities, every user wants wireless connectivity without bothering geographic position[1] [2]. There is some security concern, which increases fear of attacks on the wireless sensor network [3]. One of the major concerns in mobile ad-hoc network is Denial of Service attack in which the traffic is choked by the malicious node that denied network service for user. In order to provide secure communication and transmission, the researcher worked specifically on the security issues in mobile ad-hoc network, and many secure routing protocols and security measures within the networks were proposed. The motive of the work is to study about Denial of Service attack and how it can detected in the network. There are several constrained for mobile ad-hoc network which are discussed here [4].

- **Self-configurable:** In mobile ad-hoc, every node manages and configures itself due to absence of central point. So it is difficult to detect intruder or non cooperative device because each one has entire access of networks resources.
- **Dynamic Topology:** Mobility deals with frequent reconfiguration of network topology. So it leads routing cost in term of maintenance as well as other network resources such as network lifetime.
- **Cooperativeness:** Mobile ad-hoc network functions based on device cooperation. In ideal situation, it assumes that every device in the network is cooperative and not compromised. However, it may be possible that device becomes compromised or non-cooperative referred as intruder.

II. BACKGROUND

Wireless mobile ad-hoc networks are vulnerable for different type of attacks. Therefore, security is essential factor to increase reliability for the users. There are numerous attacks, which affects networks resources, which are classified into below categories:

- **External Attack:** This type of attack is committed outside device, which is not part of network or extruder. It intended to make service unavailability and increase congestion.
- **Internal Attack:** This attack is commits by internal device, which is compromised, or non-cooperative. In this, device takes unauthorized access and act as an authentic node. Internal device may monitor traffic of network and may play some role in different activities of network.
- **Denial of Service Attack:** This is type of internal attack that goal is to deny of any service or information. For example, genuine node request route information to other, if other node is non-cooperative then it deny request. If the attack commit successful then services are denied.
- **Impersonation:** When confirmation procedure is not properly accomplished, an attacker treats as an authentic one and observes the network traffic. It may also transmit false routing packets, and gain access on confidential information.
- **Eavesdropping:** This is type of passive attack. In this, attacker analyzes the ongoing traffic. Later, attacker may utilize gathered information.

- **Routing Attacks:** Routing is required operation in mobile ad-hoc network because entire functioning depends on it.

Without routing, no one can send data to others. Generally, attackers targets routing mechanism to block whole system. Attacker can commit two types of routing attack. First attack commits on routing protocol and second one is attack on data packet forwarding or transmission.

III. RELATED WORK

Researchers have tried to propose and implements intrusion detection system for the mobile ad-hoc networks. Few efforts presented here.

To increase network performances and secure transmissions presence of intruder, two approaches suggested in [5]. One was used for detection of intruder in the network that deny for forwarding of packets after agreement. Second were used for ignoring intruder in route in the future transmissions [5]. The integration of both approaches leads improvement in network performance significantly.

Network layer acknowledgement approach named as TWOACK advised in [6]. This scheme deals with weakness of Watchdog approach that is receiver collision and limited transmission power. In this approach, node verifies whether a packet is received by the two hop node from packet sending node. It is done by approving data packets between continuous three nodes in active path.

To detect hidden and exposed terminal wormhole attack, an approach was proposed named as DelPHI in [7]. Approach efforts to discover route between source and destination by computing delay of packets with average delay per hop along each route.

To control the maximum transmission range of packets created by intruder, an approach was proposed that named as packet leash in [8]. It is classified in geographic and temporal.

In this, node transmits a packet to other node that includes its location information and time of packet sending. Distance is calculated between one to another node.

An approach was proposed in [9] that location information and clock synchronization not considered. It used mutual authentication with distance bounding method. In this, node compute distance to another node by sending one-bit flag.

An intrusion detection approach named as A3ACKs was proposed in [10]. It deals with three issues of watchdog approach that is receiver collision, limited transmission power and collaborative attacks. This approach verifies packet delivery between four consecutive nodes of active route in the network.

IV. PROPOSED METHODOLOGY

An intrusion detection system will implements through following tasks that referred as methodology.

Task-1: Download and install NS-2 on Ubuntu virtual machine.

Task-2: Create a mobile ad-hoc network scenario in NS-2 where nodes are free to move anywhere.

Task-3: Create denial of service attack through flooding of routing messages.

Task-4: Observe communication and collect evidence.

Task-5: Analysis of collected evidence or data.

Task-6: Identify potential intrusions of network and report countermeasures

All tasks of the proposed methodology depicted in the figure1.

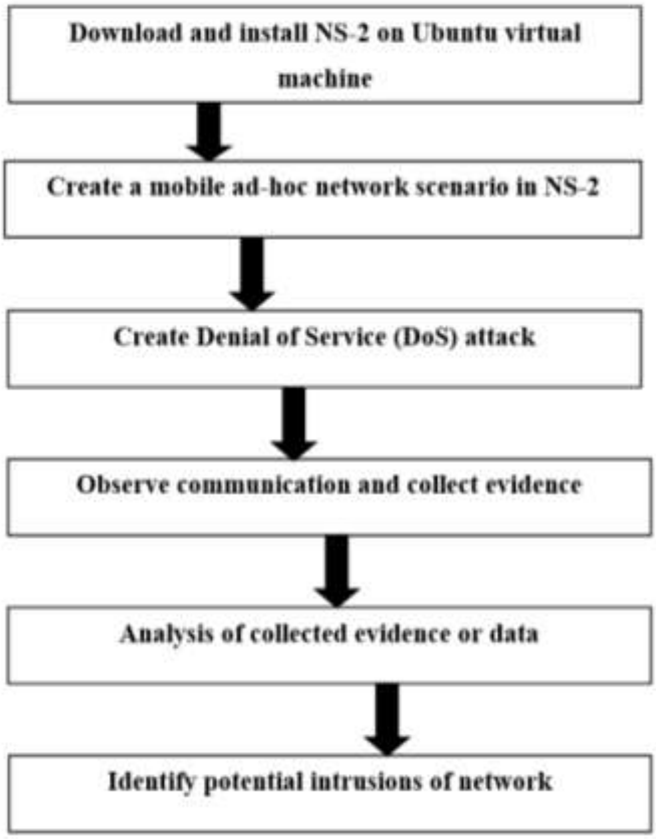
Download and install NS-2 on Ubuntu virtual machine
Create a mobile ad-hoc network scenario in NS-2
Create Denial of Service (DoS) attack
Observe communication and collect evidence
Analysis of collected evidence or data
Identify potential intrusions of network

Figure-1: Proposed Methodology

V. IMPLEMENTATION AND TESTING

Parameters Name	Values
Number of Nodes	25,50,75,100
Topography Area	800×600
Execution Time in Seconds	100
Transmission Coverage	300m
Traffic Class	CBR, 3pkts/s
Data Packet size (bytes)	512
Routing Protocol	AODV

A. Implementation

To create network scenario and intruder scenario, a tcl program is implemented which create different number of nodes as test cases. Figure 2 show one network scenario among of them that comprises of 50 nodes, 2 senders, 2 receivers, and an intruder.

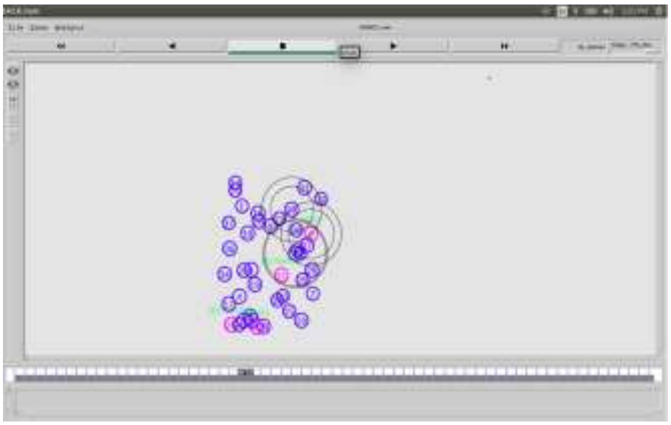

Figure 2 Experimental Scenario

B. Testing

To test and evaluate an intrusion detection system, few test cases are created and evaluated based on packet delivery ratio and throughput.
Test Case-1

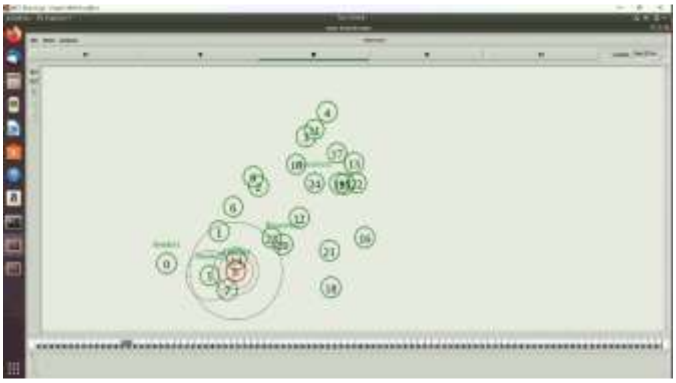

Figure 3 Test Case-1: Attack Scenario

Packet Delivery Ratio- Packet Delivery Ratio is fraction of received packets to the sent packet. It can be measure in percentage

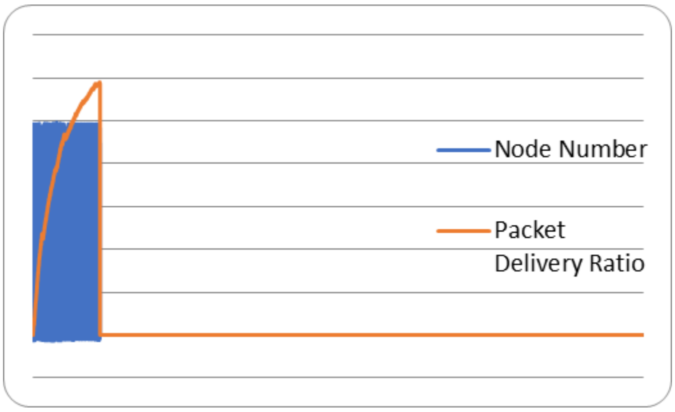

Figure 4 Packet Delivery Ratio Graph

Throughput- Data units received in form of bits, bytes or packets per unit time are known as throughput.

Figure 5 Throughput

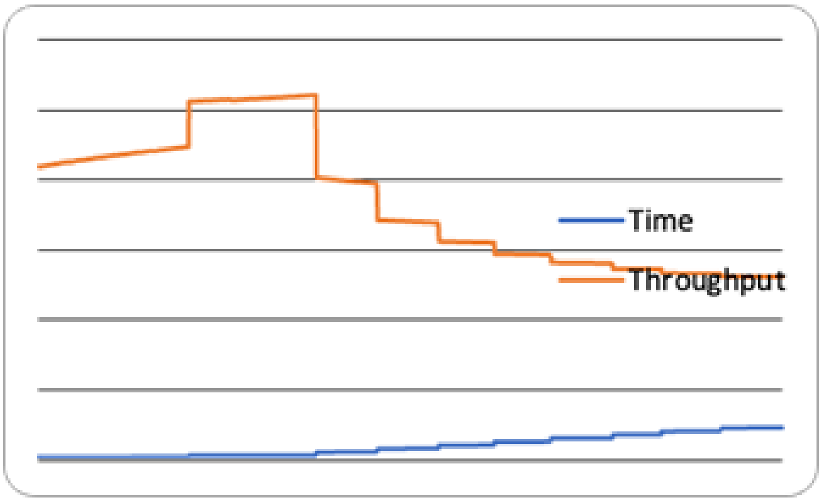

Figure 6 Throughput Graph

Test Case-2

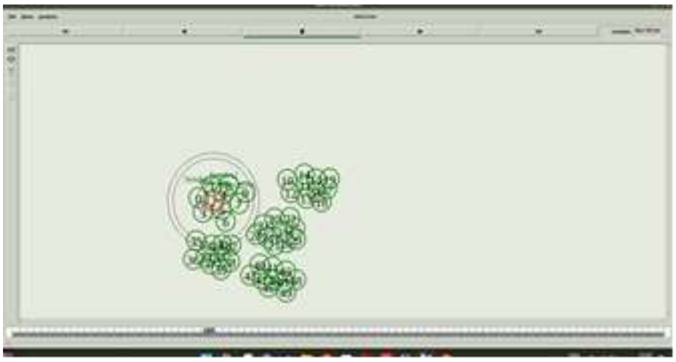

Figure 7 Test Case-2: Attack Scenario

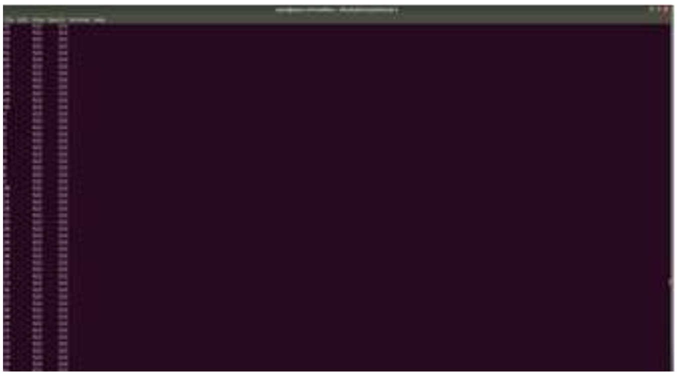

Figure 8 Test Case-2: Packet Delivery Ratio

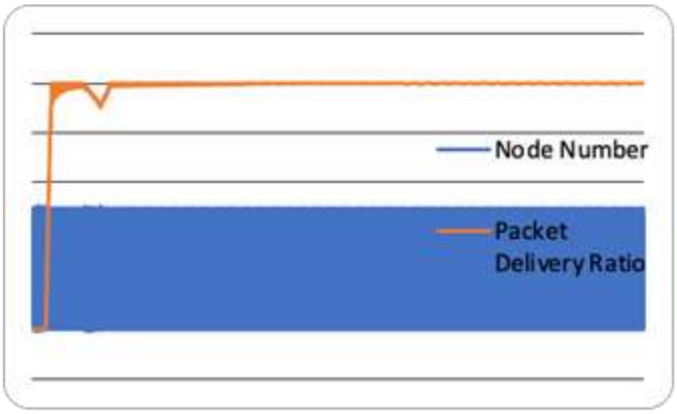

Figure 9 Test Case-2: Packet Delivery Ratio Graph

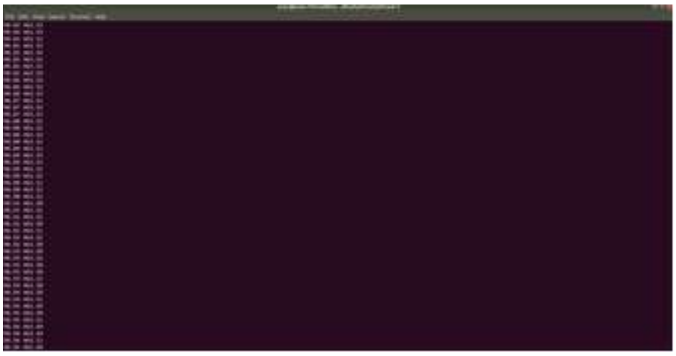

Figure 10 Throughput

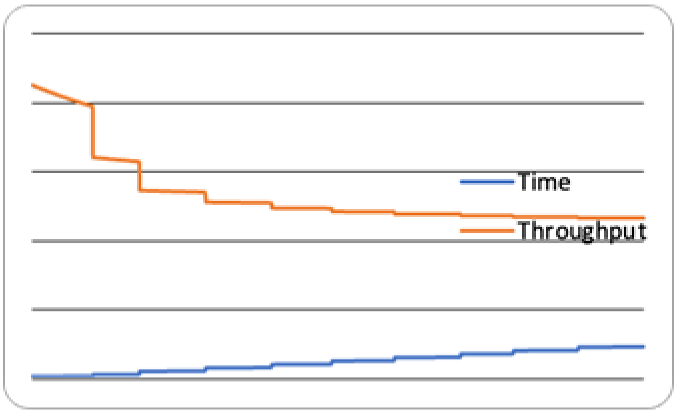

Figure 11 Throughput

VI. CONCLUSION

Wireless mobile ad-hoc network is more vulnerable to attacks compare to conventional network due to lack of physical connections. Therefore, security is major concern for reliable communication. Here, an intrusion detection system implemented in NS-2 and tested for the mobile ad-hoc network.

VII. REFERENCES

[1] Pallavi Sharma, Aditya Trivedi, “An Approach to Defend Against Wormhole Attacks in Ad Hoc Network using Digital Signature”. IEEE ISSN 978-1-61284-486-2/2011.

[2] Radhika Saini, Manju Khari, “Defining Malicious Behaviour of a Node and its Defensive Methods in Ad Hoc Network” International Journal of Computer Applications (0975-8887) Volume 20-No.4, April 2011.

[3] Rajbir Kaur, M.S. Gaur, V. Laxmi. “ A Novel Attack Model Simulation in DSDV Routing” 978-1-4244-8704-2 IEEE 2011.

[4] E.A. Mary Anita, V. Thulasi Bai, “Defending Against Wormhole Attacks in Multicast Roruting Protocols for Mobile Ad Hoc Networks” 978-1-4577-0787-2/2011 IEEE.

[6] Balakrishnan, K.; Jing Deng; Varshney, V.K., "TWOACK: preventing selfishness in mobile ad hoc networks," Wireless Communications and Networking Conference, 2005 IEEE , vol.4, no., pp. 2137-2142 Vol. 4, 13-17 March 2005.

[7] Chiu, HS; Wong Lui, “DelPHI: wormhole detection mechanism for ad hoc wireless networks”, The 1st International Symposium on Wireless Pervasive Computing, Phuket, Thailand, 16-18 January 2013

[8] Yih-Chun Hu, Adrian Perrig, David B. Johnson, “Packet Leashes: A Defense against Wormhole Attacks in Wireless Networks”, Carnegie Mellon University.

[9] Srdjan Capkun, Levente Buttyan, Jean-Pierre Hubaux, SECTOR: Secure Tracking of Node Encounters in Multi-hop Wireless Networks, ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN), October 31, 2003, Washington, USA.

[10] Abdulsalam Basabaaa, Tarek Sheltamia and Elhadi Shakshukib , Implementation of A3ACKs intrusion detection system under various mobility speeds , 5th International Conference on Ambient Systems, Networks and Technologies (ANT-2014)