International Journal of Current Trends in Engineering & Technology
www.ijctet.org, ISSN: 2395-3152
Volume: 04, Issue: 02 (March- April, 2018)

A Novel Intrusion Detection Method for Wireless Ad-hoc Network

Anuj Jain[1], Prof. Ranjeet Osari[2]
Department of CSE, IIST, Indore
[1]anuj.jain24@yahoo.in, [2]ranjeet.osari@indoreinstitute.com

Abstract- *as security perspective, mobile ad-hoc network is much targeting rather than wired networks. Reason behind this is open environment and lack of physical tight proximity property of mobile ad-hoc networks. Therefore offenders get chance to commit crime using the weak surface. Numerous kinds of attacks committed by attackers to influence network functioning and performance. Attacks committed by intruders that are part of network and compromised. In this paper, different activity of intruders observed and evaluates existing intrusion detection approach with proposed one. Proposed approach, detect intruders via third node acknowledge policy. Proposed approach has evaluated with existing techniques in aspect of packet delivery ratio, routing overhead, throughput etc.*

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

I. INTRODUCTION

Mobile ad-hoc network is short-time network and volatile in environment. An ad-hoc network has lack of permanent infrastructure for the data transmission. In this, every node can communicate directly with other nodes without need of any center access point. Additionally, each device can act as a router or host rather than dedicated router. These networks have dynamic topology [1] [2]. Dynamic topology means nodes are movable with respect of time and speed or velocity [3]. This network is weak to unauthorized access because of open environment. Some weaknesses are given below [4]:

- **Absence of centralized management:** 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.
- **Mobility:** 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 on the basis of device cooperation. In ideal situation, it assumes that every device in the network is cooperative and not compromised. But it may be possible that device becomes compromised or non-cooperative referred as intruder.

II. BACKGROUND

Ad-hoc networks are extremely a challenging in context of security. Understanding various forms of threads is always initial step regarding evolving better defense solutions. Security is required for secure transmission of data. This network is much vulnerable to cyber attacks rather than conventional network. Several kinds of attacks that influence networks which are classified into two 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 basically analyzes the ongoing traffic. Later, gathered information may be utilized by attacker.
- **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

A lot of efforts have putted by various researchers and practitioners to detect intruders. Few are described 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

SNACK approach deals with resource wastage activities of attack such as high consumption of battery power and bandwidth of nodes. This approach is limited to handle messages modifications and fake data injection activities of attack. To deals these activities of attack which are not focused by SNACK approach, a scheme will be proposed which use concept of selective and negative acknowledgement of data packet for the TCP connection. The use of selective and negative acknowledgement works in scheme judgemental based. Proposed scheme will results improved with compare of SNACK, SACK and NACK.

A. Algorithm

Algorithm is designed for proposed approach which is consists of different steps.

```
Algorithm NA3ACK (N, i)
{
        SET THACK, ACK , DataPacket
//Here SRC = Source, Dest = Destination, T = Total
Time
        SET Node, SRC, TimeOut, T
        RouteDiscovery(N,i)
        //Data Packet Transmission:-
        //Source sends Data Packet to the Destination
        Dest = SRC->DataPacket
        //Source Expect ACK from Destination
        If(ACK!= NULL and TimeOut<T)
                {
                Display “Source received ACK
Successfully”
                }
        elseif (THACK!=NULL and TimeOut<T)
                {
                        “Source received ACK from
Third Node”
                }
        Else
                {
                        Display “Malicious activity”
                }
        //find Position of Malicious Node
        If (nb_Node->ACK!= NUL)
                {
                        Display” node[i] is Malicious”
                }
        Else
                {
                Display “ node[i+1] is malicious”
                }
}
```

V. SIMULATION AND RESULT ANALYSIS

Proposed approach is simulated in Network Simulator-2(NS-2) tool considering different network matrices that shown in table 1.

Table I. Network Parameters and Values

Parameters Name	Values
Number of nodes	20,40,60,80,100
Topography area	800×600
Time in Seconds	100
Transmission range	300m
Traffic Class	CBR, 3pkts/s
Data Packet size (bytes)	512
Routing Protocol	AODV
Connection Class	TCP

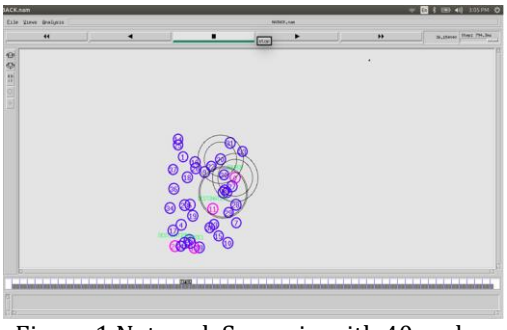

Figure 1 Network Scenario with 40 nodes

A. Simulation Scenario

To simulate proposed approach considers several network scenarios with different normal nodes, intruder node and sender receiver. Figure 1 show one network scenario among of them which consider 40 nodes, 2 senders, 2 receivers, and an intruder.

B. Evaluation Parameters

The performance is evaluated after simulating proposed approach by considering following evaluation parameters. Throughput- Data units received in form of bits, bytes or packets per unit time are known as throughput.

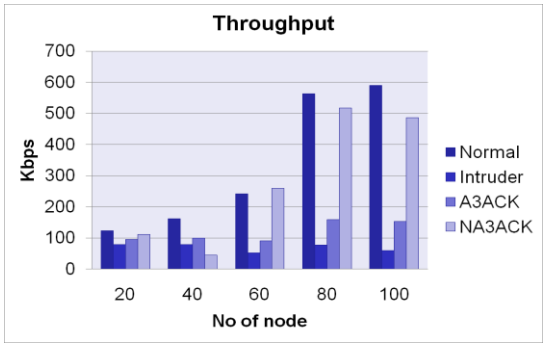

Figure 2 Throughput Graph

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

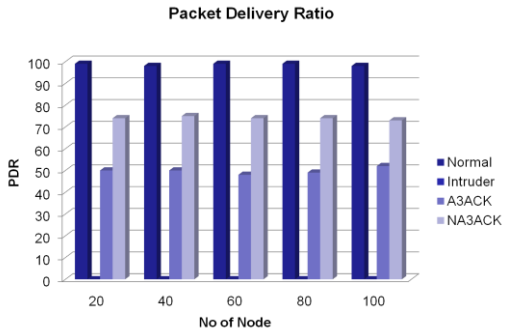

Figure 3 Packet Delivery Ratio Graph

Consumed Energy- The consumed energy of nodes in the network during the network functioning is known as consumed energy.

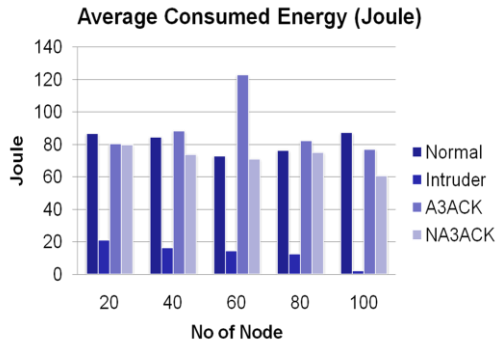

Figure 4 Average Consumed Energy Graph.

VI. CONCLUSION

Nowadays, mobile ad-hoc networks are very frequently targeted by offenders to do some unethical things. So it requires more attention in term of safety and security. To do this, an approach is proposed to detect intruders to make reliable and to improve the performance, lifetime of network. Proposed approach simulated in network simulator NS-2 considering some network parameters and evaluated by some network evaluation parameters.

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 Behavior of a Node and its Defensive Methods in Ad Hoc Network" International Journal of Computer Applications, 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 Routing Protocols for Mobile Ad Hoc Networks" 978-1-4577-0787-2/2011 IEEE.

[5]. 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.

[6]. 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.

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

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

[9]. 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).