International Journal of Engineering Research and General Science Volume 2, Issue 5, August-September, 2014
ISSN 2091-2730

A Hybrid Dynamic Clustering Based Approach for Malicious Nodes Detection in AODV Based Manets

Alka Sachdeva [1], Ameeta[2], Babita[3]

[1]Department of ECE, PCET, Lalru Mandi PTU Jalandhar, Punjab

[2]Asst. Professor, Department of ECE, PCET, Lalru Mandi PTU Jalandhar, Punjab

[2]Asst. Professor, Computer Science and Engineering Department, PCET, Lalru Mandi PTU Jalandhar, Punjab

E-mail- alkasachdevapcet@gmail.com

Abstract:- A Mobile ad hoc network (MANET) is a continuously self configuring infrastructure-less network of mobile devices connected without wires.MANETS are extensively used these days for communication and there are various communication networks with different standards and computing techniques, different Zone Routing Protocol by varying transmission range and mobility of MANETS are used. As days are passing by the size of MANETS is increasing day by day and its expansion is inevitable due to its high penetration and popularity for the usage of mobile application but at the same time it is also prone to many attacks and network failure due to technical vulnerability of the network. This paper discussed the detection and isolation of genuine node from the main network under DOS attack using Watchdog approach. Therefore we need a mechanism which would need to overcome such scenarios. Simulation results shows better results for packet loss ratio, throughput, packet delivery ratio and other parameters by detecting malicious for proper and smooth functioning of MANETS.

I.INTRODUCTION

1.1 Mobile ad-hoc Networks:-An ad hoc network is the cooperative engagement of a collection of mobile nodes without the required intervention of any centralized access point or existing infrastructure. Ad hoc networking for commercial uses; however, the main applications lie in military, tactical and other security-sensitive operations. In these applications, secure routing is an important issue. Most of the protocols proposed for Secure Routing are either proactive or reactive. In MANETS mobility is the major issue. There are several problems in routing with mobile ad hoc network like asymmetric links, routing overhead, dynamic topology and inference.

2. SECURITY GOALS:- Mobile ad-hoc networks (MANETS) are prone to a number of security threats.

There are five major security goals that need to be addressed in order to maintain a reliable and secure ad-hoc network environment. The mechanisms which are used to detect, prevent and respond to security attacks They are mainly:

(i) Confidentiality: Protection of any information from being exposed to unintended entities. In ad hoc networks this is more difficult to achieve because intermediates nodes receive the packets for other recipients, so they can easily eavesdrop the information being routed.

(ii) Availability: Services should be available whenever required. There should be an assurance of survivability despite a Denial of Service (DOS) attack. On physical and media access control layer attacker can use jamming techniques to interfere with communication on physical channel. On network layer the attacker can disrupt the routing protocol. On higher layers; the attacker could bring down high level services.

(iii) Authentication: Assurance that an entity of concern or the origin of a communication is what it claims to be or from. Without which an attacker would impersonate a node, thus gaining unauthorized access to resource and sensitive information and interfering with operation of other nodes.

(iv) Integrity: Message being transmitted is never altered.

(v) Non-repudiation: Ensures that sending and receiving parties can never deny ever sending or receiving the message.

2.1 DENIAL OF SERVICES ATTACK:-Denial of service (DoS) is another type of attack, where the attacker injects a large amount of junk packets into the network. These packets overspend a significant portion of network resources, and introduce wireless channel contention and network contention in the MANET. A routing table overflow attack and sleep deprivation attack are two other types of the DoS attacks. In the routing table overflow attack, an attacker attempts to create routes to nonexistent nodes. Meanwhile the sleep deprivation attack aims to consume the batteries of a victim node. For example, consider the following Fig. 3. Assume a shortest path exists from **S** to **X** and **C** and **X** cannot hear each other, that nodes **B** and **C** cannot hear each other, and that **M** is a malicious node attempting a denial of service attack. Suppose **S** wishes to communicate with **X** and that **S** has an unexpired route to **X** in its route cache. **S** transmits a data packet toward **X** with the source route **S --> A --> B --> M --> C --> D --> X** contained in the packet's header.

2.2 ROUTING ATTACKS ON AODV PROTOCOL

We can classify routing attacks on AODV into four classes:

1) Route Disruption: A malicious node either destroys an existing route or prevents a new route from begin established.

2) Route Invasion: A malicious node adds itself into a route between source and destination nodes.

3) Node Isolation: A given node is prevented from communicating with any other nodes. It differs from route disruption in that route disruption is targeting at a route with two given nodes, while node isolation is targeting at all possible routes to or from a given node.

4) Resource Consumption: The communication bandwidth in the network or storage space at individual nodes is consumed.

B. Typical Attacks

In the following, we give a short description of some typical routing attacks on AODV.

1) Neighbour Attack: When an intermediate node receives a RREQ/RREP packet, it adds its own ID in the packet before forwarding it to the next node. A malicious node simply forwards the packet without adding its ID in the packet. This causes two nodes that are not within the communication range of each other believe that they are neighbours, resulting in a disrupted route. The Neighbour and Black hole attacks prevent the data from being delivered to the destination node. But in the Neighbour attack, the malicious node does not catch and capture the data packets from the source node.

2) Black hole Attack: In the first type of the attack, a malicious node waits for its neighbours to initiate a route discovery process. Once the malicious node receives a broadcasted RREQ packet, it immediately sends a false RREP packet with a greater sequence number. So, the source node assumes that the malicious node is having a fresh route towards the destination node and ignores RREP packets received from other nodes. The malicious node takes all the routes towards itself and does not allow forwarding any packet anywhere. In the second type, once a malicious node receives a broadcasted RREQ packet, it intentionally increases the broadcast ID and source sequence number, and rebroadcast the modified packet with a spoofed source IP address.

3) Rushing Attack: Each intermediate node typically forwards only one RREQ packet originating from each route discovery. A malicious node simply exploits this property of the operation of route discovery by quickly forwarding RREQ packets. As a result, the source node will not be able to discover any valid routes that do not include the malicious node. On-demand routing protocols (e.g., AODV) introduce a delay between receiving a RREQ packet and forwarding it, in order to avoid collisions of RREQ packets. A malicious node ignoring this delay will generally be preferred to similarly situated being nodes.

4) RREQ Flooding Attack: A malicious node sends a huge number of RREQ packets in an attempt to consume the network resources. The source IP address is forged to a 68 randomly selected node and the broadcast ID is intentionally increased.

3. PROPOSED METHOD AND OBJECTIVE:-Our proposed method primarily based on detection of DOS attacks and isolating these malicious nodes from the network, so that rest of the genuine nodes can work peacefully. Proposed mechanism works using AODV protocol for routing of nodes. We have designed a trust based packet forwarding scheme for detecting and isolating the malicious nodes using the routing layer information.

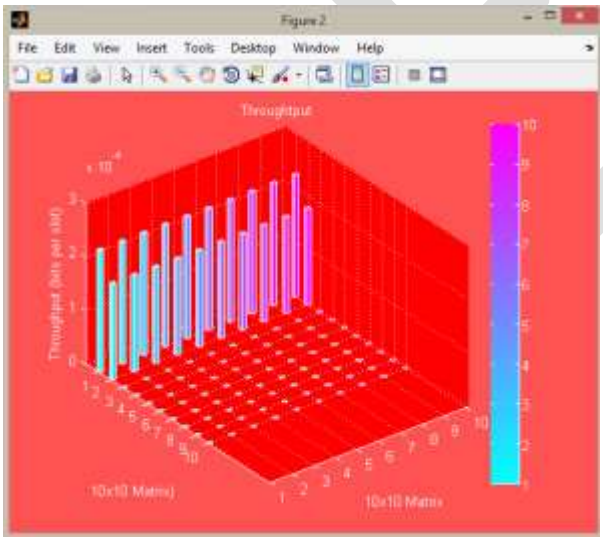
It uses trust values to favour packet forwarding by maintaining a trust counter for each node. A node is punished or rewarded by decreasing or increasing the trust counter. If the trust counter value falls below a trust threshold, the corresponding intermediate node is marked as malicious. We propose a Trust based packet forwarding scheme in MANETs without using any centralized infrastructure. Each intermediate node marks the packets by adding its hash value. And forward the packet towards the destination node. The destination node verifies the hash value and check the trust counter value. If the hash value is verified, the trust counter is incremented, otherwise it is decremented. If the trust counter value falls below a trust threshold, the corresponding the intermediate node is marked as malicious. This scheme presents a solution to node selfishness without requiring any pre-deployed infrastructure. It is independent of any underlying routing protocol.

4. PERFORMANCE EVALUVATION:-

Quality of Service based performance metrics are designed for detection of malicious nodes under simulation environment. These parameters are as follow:-

4.1 *Throughput*

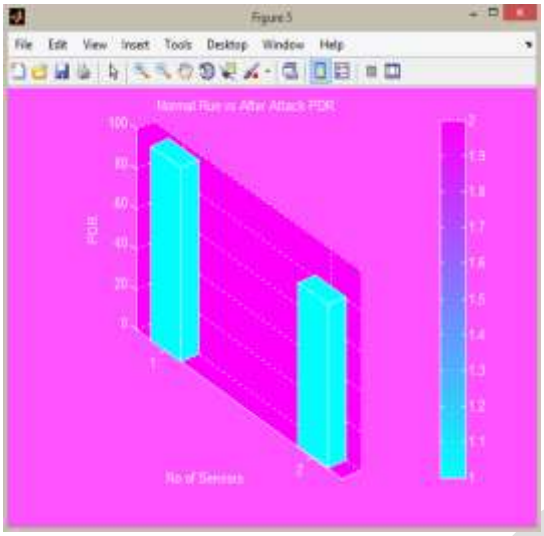
Throughput or network throughput is the average rate of successful message delivery over a communication channel. This data may be delivered over a physical or logical link, or pass through a certain network node. The throughput is usually measured in bits per second (bit/s or bps), and sometimes in data packets per second or data packets per time slot. Throughput is essentially synonymous to digital bandwidth consumption.



4.2 *PDR*

It the ratio of number of packet actually delivered without duplication to destination verses the number of packet supposed to be received. This number represents the effectiveness and throughput of a protocol in delivering data to the intended receiver within the network.

PDR = TOTAL NO. OF PACKET RECEIVED /TOTAL NO. OF PACKET SEND



4.3 *ENERGY CONSUMPTION*

The total energy consumed in the network is energy consumption. It is measured in whr.

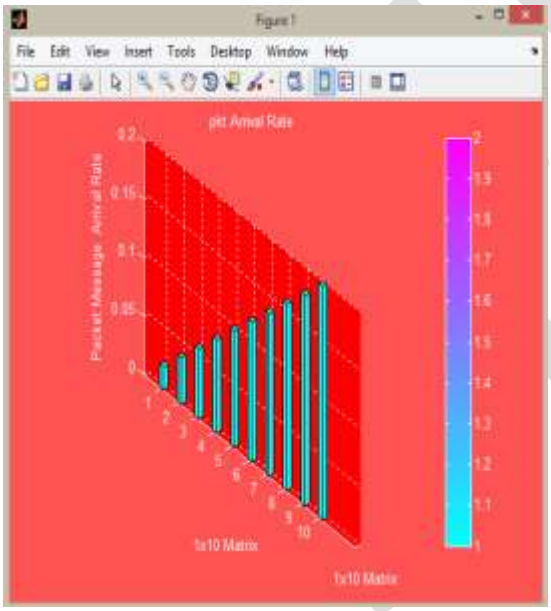


Figure 1 is also a reflection of how no. of message packets are affected when there is an attack being introduced this graph shows how many packets have been lost (control message) when there was no. of attacks.

4.4 *NUMBER OF COLLISIONS*

In a network, when two or more nodes wants to transmit data at the same time network collision occurs. When a packet collision occurs the packet is either discarded or sent back to their originating stations and again

retransmitted in a times based sequence to avoid collisions. Collisions can result in loss of packet integrity or can impede the performance of a network. This metric is used to measure such collision in the network.

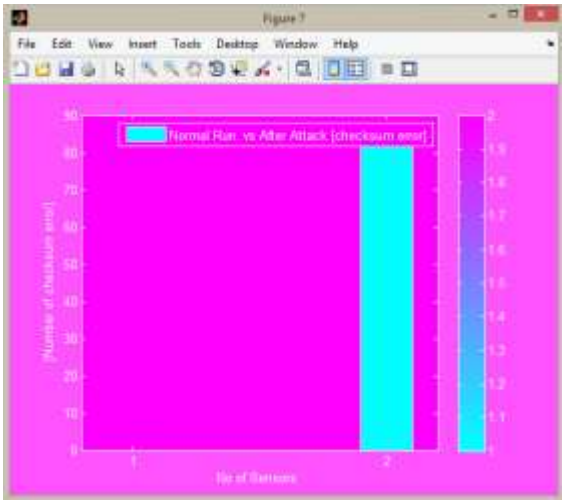
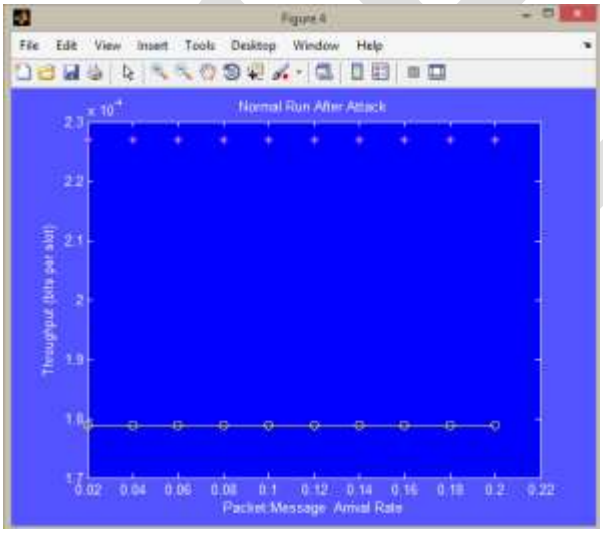


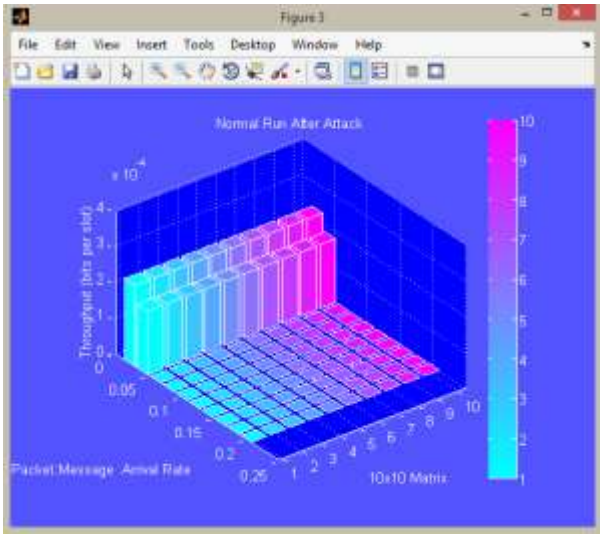
Figure 7 shows that there are less checksum errors before attack and after attack there are increase in checksum errors.

4.5 *PLR*

Packet loss ratio = Number of lost packet / (Number of lost packet + Number of packets received successfully)

Knowing your packet loss ratio will help you determine if the slowness issue is based on your connection to the nodes, or it stems from a different problem. Poor communication connections can be caused by a number of reasons, so using a packet loss ratio formula is a part of the detection process.

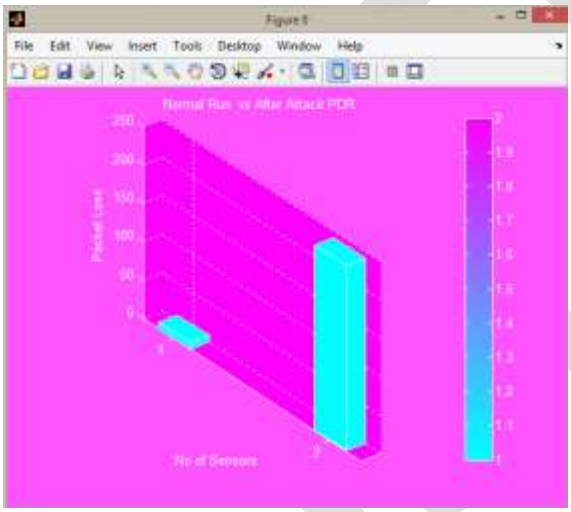




Simulation results showed that, it is clear from the figure 3 that in attacks there is reduction in throughput of system with respect to message arrival time

4.6 Routing overhead (RO)

Routing Overhead defines the ratio of the amount of routing related transmissions [Route REQuest (RREQ), Route REPly (RREP), Route ERRor (RERR), ACK, S-ACK, and MRA].During the simulation, the source route makes unicast and multicast an RREQ message to all the neighbours within its communication range.



The figure 6 shows that when the network is running smooth and fine without any introduction of any attack there is normal communication of packet being send and receive which leads to packet delivery ratio above 90% which can be seen in the session of IDS but when there is an attack occurring there is a sudden dip in throughput as well as PDR about 10% less than normal.

5. CONCLUSION AND FUTURE SCOPE

Simulation results have shown that the problem of DOS attacks in MANETS and proposed our simulated approach for analysis of security in MANETS. Our results confirm that DOS attacks can be detected easily and efficiently using the AODV based reputation protocol. In future scope of this research work we can be designed for Fuzzy Logic system for multi-node optimization, enhanced reliability and accuracy. This research work can be developed for mathematical model for detection of many types of attacks.

REFERENCES:

[1] Ashish K Maurya and Dinesh Singla "Simulation based performance comparison of AODV,FSR,ZRP routing protocols in MANET", International Journal of computer applications. Foundation of computer science 12(2), December 2014, pp 23-18.

[2] T Ravi Nayak et al. "Implementation of Adaptive Zone Routing protocol for wireless network", International Journal of engineering Science and Technology Vol.2 (12), 2013 pp 7273-7288.

[3] Rajneesh Kumar Gujral, Manpreet Singh "Analyzing the Impact of Scalability on QoS Aware Routing for MANETs "International Journal of Computer Science MANETs vol. 8(3), pp no. 487-495, May 2013,Issue ISSN (online): 1694-0814.

[4] Preeti Arora and GN Purohit "Comaparative Analysis of Adhoc Routing Unicast Protocols(using WiMAX Environment", IJCSI International Journal of computer science issues ,Vol-8 Issue2,March 2011.

[5] Sree Ranga Raju and Jitendranath Mungara " Performance Evaluation of ZRP over AODV and DSR in Manet using Qualnet", European Journal of Scientific Research ISSN 1450-216X Vol. 45 No 4(2010) pp 651-667.

[6] Md. Saiful Azad, Mohammad Moshee Uddin, Farhat Anwar and Md. Arafatur Rahman "Performance Evaluation of Wireless Routing protocols in Mobile Wimax Environment", Proceedings of the international multiconference of engineers and computer scientists 2008, vol. 2 IMECS 2008, 19-21 March,2008 Hong Kong.

[7] Brijesh Patel and Sanjay Srivastava, "Performance Analysis of Zone Routing Protocols in Mobile Ad hoc Networks" Dhirubhai Ambani Institute of Information and Communication Technology Gandhinagar 382 007, India, 2006.

[8] Charles E.Perkins and Elizabeth M. Royer, "Ad hoc on demand distance vector (AODV) routing (Internet-Draft)", Aug- 2013.

[9] H. Yang, et al, "SCAN: Self-Organized Network-Layer Security in Mobile Ad Hoc Networks," IEEE Network, vol. 24, 2012, pp. 1-13.

[10] Hoang Lan Nguyen, Uyen Trang Nguyen. "*A study of different types of attacks on multicast in mobile ad hoc networks".* Ad Hoc Networks, Volume 6, Issue 1, Pages 32-46, January 2012