DESIGN AND IMPLEMENTATION OF ROUTING PROTOCOL FOR DETECTION OF SYBIL ATTACK IN MANET

Mohd Amir Siddiqui[1], Roshan Jahan[2], Ijtaba Saleem Khan[3]

[1]Research Scholar, [2,3]Assistant Professor, CSE Dept., Integral University, Lucknow, U.P., (India)

ABSTRACT

Network and information security is a major concern of researchers. Important information can be easily hacked these days. Although there are various security algorithms available, but still internet world is not secure. Most of the time intruder attacks on a network by creating malicious node. These malicious nodes destroy the network communication or send information to the other server. Sybil attack is one of the major attacks. This paper presents a technique to detect and prevent mobile Ad-hoc Network from Sybil attack. The proposed technique is implemented on QualNet5.0. The results and graphs are described to evaluate the efficiency of new technique.

Keywords: ZRP, DSR, AODV, Wireless Network, Wormhole Attack.

I. INTRODUCTION

The growth in the use of wireless communications over the last few years is quite substantial and as compared to other technologies, it's huge. The primary advantage of a wireless network is the ability of the wireless node to communicate with the rest of the world while being mobile. For Ad Hoc routing protocols, there are certain specific requirements specific requirements. First of all, such protocols must be distributed, because depending on a central host to make the routing decisions introduces a bottle neck or even to a single point of failure considering the limited resources of the mobile nodes. Secondly, they must be adaptive to the continuously changing topology due to mobility. Thirdly, they must compute the routes in a fast, loop free, optimal resource usage and up to date fashion. Additionally, they must keep the process of route maintenance as local as possible. Finally, they should provide some degree of quality of service (QoS) and keep as much helpful information as possible about only the local and stable network topology.

Mobile ad hoc networks (MANETs)**[1]** are collections of mobile nodes, dynamically forming a temporary network without pre-existing network infrastructure or centralized administration. These nodes can be arbitrarily located and are free to move randomly at any given time, thus allowing network topology and interconnections between nodes to change rapidly and unpredictably. Node mobility can vary from almost stationary to constantly moving nodes, depending on the particular network's structure and purpose. As a general rule, high mobility usually results in low link capacity, whereas low mobility leads to high capacity links. The very dynamic nature of mobile ad-hoc networks creates great challenges for routing protocols. As MANET networks are infrastructure less there exist no dedicated routers. Instead, every mobile node acts itself as a router and is responsible for discovering and maintaining routes. Furthermore, without centralized administration, MANETs can be called autonomous. To support this kind of autonomy, the routing protocol is required to automatically adjust to frequent environment changes. The primary goal of the routing protocol is correct and efficient route establishment to facilitate communication within the network between arbitrary nodes. To successfully fulfill this task, the routing protocol must take the unique characteristics of MANET networks into account.

There are generally purely proactive and purely reactive approaches to implement a routing protocol **[2]** for a MANET but they have their disadvantage. To overcome this a new approach hybrid routing protocols came into existence by taking the advantage of both proactive and reactive in hybrid schema, taking advantage of proactive discovery within a nodes local neighborhood, and using reactive protocol for communication between these neighborhoods.

There are few malicious nodes**[3]** which generates attack on network. This paper is concentrated on identification of such activity and makes communication reliable.

The present work is organised into 4 chapters. In section 1 of present paper, introduces and explains the nature of the problemand the problem itself. Later, the sectionalso reviews previous works and description of various techniques regarding the subject present such as DSR, AODV etc. Sections 2 will discuss the proposed routing technique. Section 3 describes the simulation environment and enlists the results of comparing AODV, DSR and proposed techniques. Its effectiveness is also demonstrated with the help of suitable plots. Section 4 willfinally provides a concluding remark on this work

1.1 Attacks in Network

- **Black hole[4]:** In this attack, a misbehaving node uses the routing protocol to advertise itself as having the shortest path to the node whose packets it wants to intercept. We provide a detailed description here in.
- **Denial of service[5]:** The DoS attack results when the network bandwidth is hijacked by a misbehaving node. It has many forms: the classic way is to flood any centralized resource so that the network no longer operates correctly or crashes. For instance, a route request is generated whenever a node has to send data to a particular destination. A misbehaving node might generate frequent unnecessary route requests to make the network resources unavailable to other nodes.
- **Routing table overflow[6, 7]:** The attacker attempts to create routes to nonexistent nodes. The goal is to have enough routes so that creation of new routes is prevented or the implementation of routing protocol is overwhelmed.
- **Impersonation[8]:** A misbehaving node may impersonate another node while sending the control packets to create an anomaly update in the routing table.
- **Energy consumption[9]:** Energy is a critical parameter in the MANET. Battery-powered devices try to conserve energy by transmitting only when absolutely necessary. An attacker can attempt to consume batteries by requesting routes or forwarding unnecessary packets to a node.
- **Information disclosure[10]:** The misbehaving node may leak confidential informationto unauthorized users in the network, such as routing or location information. In the end, the attacker knows which nodes are situated on the target route.

- **Wormhole Attack[11]:** The attacker receives packets at one point in the network, “tunnels” them to another point in the network, and then replays them into the network from that point. For tunneled distances longer than the normal wireless transmission range of a single hop, it is simple for the attacker to make the tunneled packet arrive with better metric than a normal multi-hop route, for example, through use of a single long-range directional wireless link or through a direct wired link to a colluding attacker.
- **Sybil attack [12]:** In this attack, a mobile node forges the identities of multiple mobile nodes. These identities can be used to play any type of attack in the system. These false identities also create an illusion that there are additional vehicles on the road. Consequence of this attack is that every type of attack can be played after spoofing the positions or identities of other nodes in the network.

1.2 ZRP [2]

ZRP protocol divides the whole network in to non-overlapping zone and runs independent protocols that study within and between the zones. Intra-Zone Protocol operates within the zone and Intra-zone protocol (IARP) operates within a zone and learns all the possible routes, proactively. So, all nodes within a zone know about its zone topology very well. Inter-zone protocol (IERP) is reactive and a source node finds a destination node which is not located within the same zone, by sending RREQ messages to all border nodes. This continues until destination is found.

1.3 DSR [2]

DSR is a fairly simple algorithm based on the concept of *source routing*,in which a sending node must provide the sequence of all nodes through which a packet will travel. Each node maintains its own *route cache*, essentially a routing table, of these addresses. Source nodes determine routes dynamically and only as needed; there are no periodic broadcasts from routers. DSR algorithm is based on route discovery/ route reply cycle and route maintenance. A source node that wants to send a packet first checks its route cache. If there is a valid entry for the destination, the node sends the packet using that route; if no valid route is available in the route cache,

The source node initiates the route discovery process by sending a special route request (RREQ) packet to all neighboring nodes. The RREQ propagates through the network, collecting the addresses of all nodes visited, until it reaches the destination node or an intermediate node with a valid route to the destination node. This node in turn initiates the route reply process by sending a special route reply (RREP) packet to the originating node announcing the newly discovered route. The destination node can accomplish this using inverse routing or by initiating the route discovery process backwards. The DSR algorithm also includes a route maintenance feature implemented via a hop-to-hop or end-to-end acknowledgment mechanism; the former includes error checking at each hop, while the latter checks for errors only on the sending and receiving sides. When the host encounters a broken link, it sends a route error (RERR) packet. Dynamic source routing is easy to implement, can work with asymmetric links, and involves no overhead when there are no changes in the network. The protocol can also easily be improved to support multiple routes to the same destination. DSR’s main drawback is the large bandwidth overhead inherent in source routing. Because each route cache collects the addresses of all visited nodes, RREQ packets can become huge as they propagate through the network. Routing information can also increase enough to exceed the accompanying messages usefulness. These problems limit the network’s acceptable diameter and therefore its scalability.

1.4 Ad Hoc On-Demand Distance Vector Routing (AODV)[2]

AODV routing protocol is based on DSDV and DSR algorithm. It uses the periodic beaconing and sequence numbering procedure of DSDV and a similar route discovery procedure as in DSR. However, there are two major differences between DSR and AODV. The most distinguishing difference is that in DSR each packet carries full routing information, whereas in AODV the packets carry the destination address. This means that AODV has potentially less routing overheads than DSR. The other difference is that the route replies in DSR carry the address of every node along the route, whereas in AODV the route replies only carry the destination IP address and the sequence number.

The Ad hoc On-Demand Distance Vector (AODV) routing protocol is intended for use by mobile nodes in an ad hoc network. It offers quick adaptation to dynamic link conditions, low processing and memory overhead, low network utilization, and unicast route determination to destinations within the ad hoc network. It uses destination sequence numbers to ensure loop freedom at all times (even in the face of anomalous delivery of routing control messages), avoiding problems (such as “counting to infinity”) associated with classical distance vector protocols.

The primary objectives of AODV protocol are:

1. To broadcast discovery packets only when necessary,
2. To distinguishes between local connectivity management (neighborhood detection) and general topology maintenance and
3. To disseminate information about changes in local connectivity to those neighboring mobile nodes those are likely to need the information. AODV decreases the control overhead by minimizing the number of broadcasts using a pure on-demand route acquisition method. AODV uses only symmetric links between neighboring nodes.

II. PROPOSED TECHNIQUE

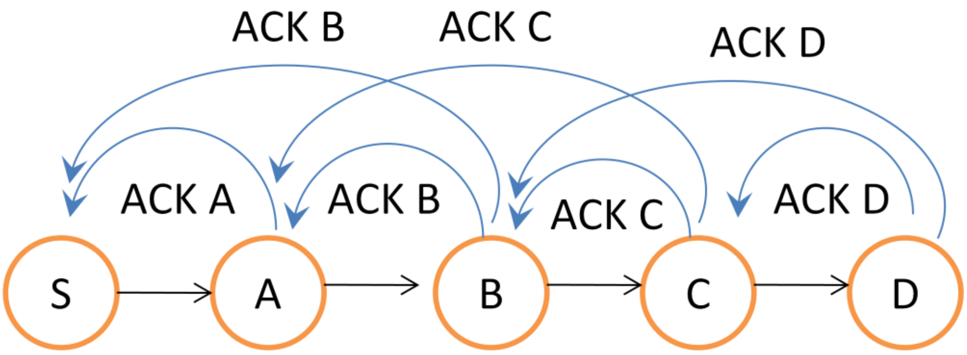

Figure 1: Flow chart of proposed model

Fig. 1 is representing flow chart of proposed model. Here S is source and D is destination. In this model every node will send two acknowledgements. First acknowledgement is for previous node and second acknowledgement is for previous to previous node.

This acknowledgement will contain message size and destination address. If previous nodes get a different destination address, in that case sender will send message through other node and stop communication to malicious node.

If destination address will be changed by any node then network denote that node as malicious node of network and stop communication with that node.

III. SIMULATION RESULTS

The simulation of network is carried out on Qualnet 5.0[13]. The simulation environment is as under:

- **Mobility model Random Way Point**
  - Minimum speed: 0 mps
  - Maximum speed: 5mps, 10 mps, 15 mps, 20mps, 25 mps, and 30 mps
  - Pause time: 5s, 10s, 15s, 20s, 25s, 30s.
  - Simulation Time: 200s
- **Terrain**
  - Coordination 1500 * 1500 m
- **Connection**
  - FTP (File transfer protocol): 41 (client) to 1 (server)
  - Item size 512(byte)
- **Radio/physical layer parameters:**
  - Radio type: 802.11b Radio
  - Data rate: 2Mbps
  - Packet reception model: Bit error rate (bpsk.ber)
- **MAC Protocol**: 802.11
- **Routing Protocol**: AODV,DSR
- **Transport Protocol**: TCP
- **Node**: 50
- **Node Placement**: Random
- **Seed**: 1

Performance metrics used for this works are as follows:

- Throughput [1] is the measure of the number of packets successfully transmitted to their final destination per unit time. It is the ratio between the numbers of sent packets vs. received packets.
- Average End to End Delay [1] signifies the average time taken by packets to reach one end to another end (Source to Destination).
- Avg. Jitter Effect [1] signifies the Packets from the source will reach the destination with different delays. A packet's delay varies with its position in the queues of the routers along the path between source and destination and this position can vary unpredictably.
- Packet Loss,[1] is the Ratio of transmitted packets that may have been discarded or lost in the network to the total number of packet sent.

IV. RESULTS

The results of simulations are as follows:

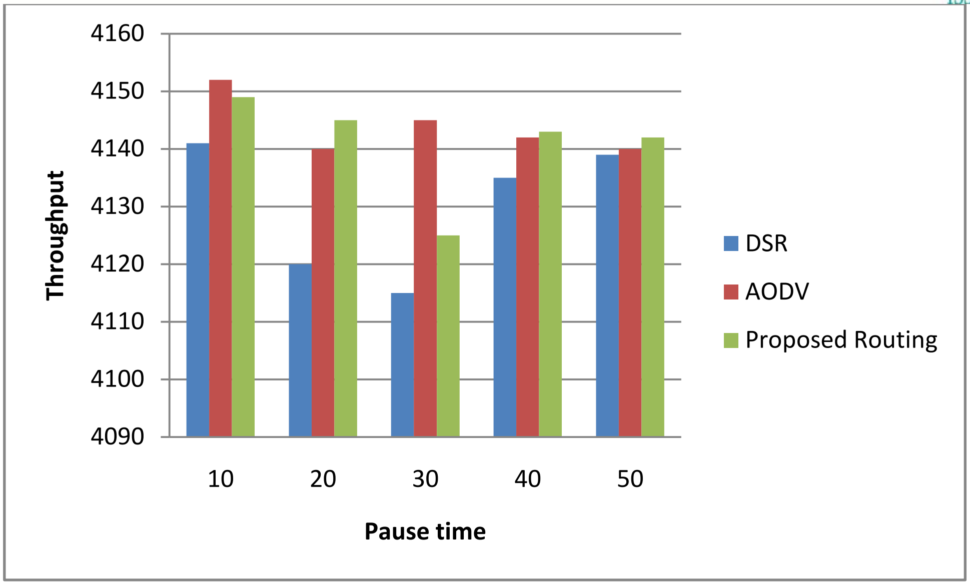

Figure 2: Plot of throughput

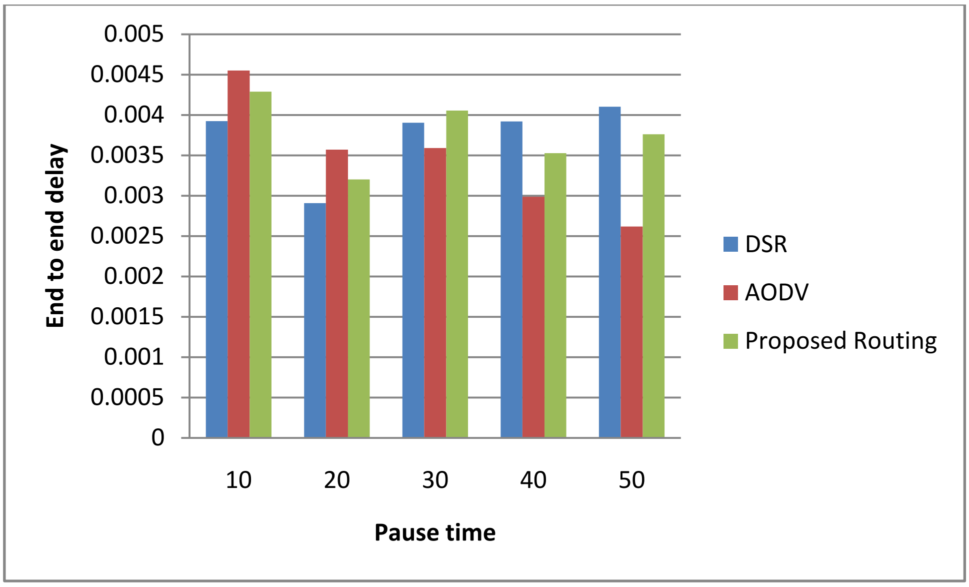

Figure 3: Plot of end to end delay

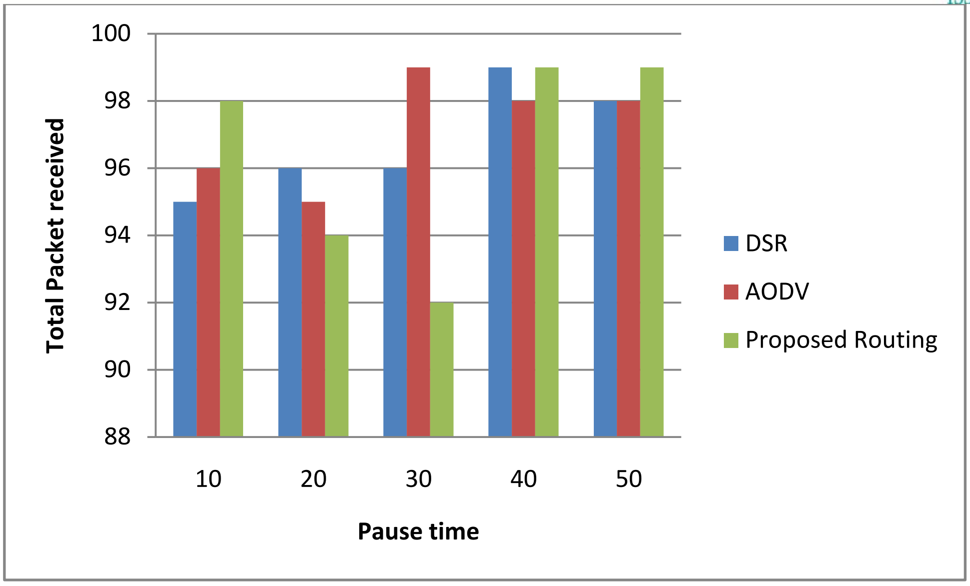

Figure 4: Plot of total packet received

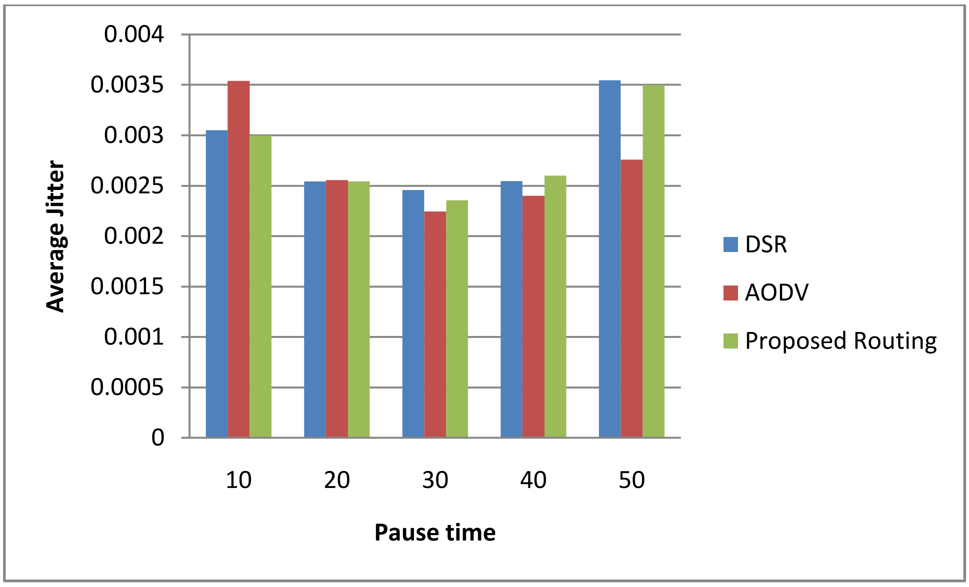

Figure 5: Plot of average jitter

It can be observed that in most of the cases proposed protocol is performing better than AODV and DSR. So, to avoid malicious activity in network proposed routing technique can be used. It can improve efficiency of communication in MANET.

V. CONCLUSION

Identification of malicious in network is like detection of virus in human body. Malicious nodes can destroy complete network, if it is in network. So it should be removed from network. This paper presents a routing protocol which is able to detect and remove malicious node which are creating Sybil attack. This technique can identify the node without affecting the communication. Whenever network finds any malicious node, it changes routing strategy and remove the infected nodes. As it can be observed the result of communication with new technique is better than AODV and DSR. So that, in the case of attack on the network proposed technique can be used.

REFERENCES

[1] Stefano Basagni, Marco Conti, Silvia Giordano, Ivan Stojmenovic, “Mobile Ad Hoc Networking” John Wiley & Sons, 2004.

[2] Jonathan Loo, Jaime LloretMauri, Jesús Hamilton Ortiz, “Mobile Ad Hoc Networks: Current Status and Future Trends”CRC Press, 2012

[3] Joseph MiggaKizza, “Computer Network Security” Springer Science & Business Media, 2005

[4] Aware, A.A.; Bhandari, K., "Prevention of black hole attack on AODV in MANET using hash function," Reliability, Infocom Technologies and Optimization (ICRITO) (Trends and Future Directions), 2014 3rd International Conference on , vol., no., pp.1,6, 8-10 Oct. 2014

[5] Xiuzhen Chen; Shenghong Li; Jin Ma; Jianhua Li, "Quantitative threat assessment of denial of service attacks on service availability," Computer Science and Automation Engineering (CSAE), 2011 IEEE International Conference on , vol.1, no., pp.220,224, 10-12 June 2011

[6] Desai, V.; Shekokar, N., "Performance evaluation of OLSR protocol in MANET under the influence of routing attack," Wireless Computing and Networking (GCWCN), 2014 IEEE Global Conference on , vol., no., pp.138,143, 22-24 Dec. 2014

[7] Long Xiao; ShaoqingMeng; Kaining Lu, "Based on RSAODV the solution to routing table overflow problem," Multimedia Technology (ICMT), 2011 International Conference on , vol., no., pp.246,248, 26-28 July 2011

[8] Bustard, J.D.; Carter, J.N.; Nixon, M.S.; Hadid, A., "Measuring and mitigating targeted biometric impersonation," Biometrics, IET , vol.3, no.2, pp.55,61, June 2014

[9] Dharma Agrawal, Qing-An Zeng, “Introduction to Wireless and Mobile Systems” Cengage Learning, 2010

[10] Nova Southeastern University. Information Systems (DISS),” A Systems Analysis of Information Technology and the Use of WLANs Implemented by an FBI Field Office for Crisis Response Incidents: The Columbia Field Office Case Study” ProQuest, 2007

[11] Yih-Chun Hu; Perrig, A.; Johnson, D.B., "Wormhole attacks in wireless networks," Selected Areas in Communications, IEEE Journal on , vol.24, no.2, pp.370,380, Feb. 2006

[12] Mina Rahbari, Mohammad Ali Jabreil Jamali "Efficient detection of sybil attack based on cryptography in vanet" International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.6, November 2011.

[13] QualNet 5.0 URL: “web.scalable-networks.com/content/**qualnet**”, Last Accessed on 12 Aug’ 2015