PERFORMANCE ANALYSIS OF AODV ROUTING PROTOCOL IN MOBILE ADHOC PROTOCOL

Usha Dagar

Research Scholar, School of Engineering & Technology
Poornima University, Jaipur, Rajasthan (India)

ABSTRACT

Wireless communication is the transfer of information between two or more points that are not connected by an electrical conductor. In order to communicate each other, the nodes cooperatively forward data packets to other nodes in the network by using the routing protocol, they are vulnerable to many severe attacks. we address so many attacks as wormhole attack , Sybil attacks, man-in-middle attacks, sinkhole attacks , jamming attacks and flooding attacks e.t. Routing is a crucial factor of security in MANET and hence the focus of this thesis along with the performance analysis of routing protocols. The comparison analysis will be carrying out about these protocols using Simulator NS 3. In this paper we find the solution approaches which are Result Verification Mechanism for AODV Routing Protocol in MANETs. Mobile Ad hoc Network is based on demand routing protocol to improve the performance and provide secure communication between two devices.

Key words: MANET, AODV, MAODV, Wormhole Attack, Sybil Attack, Simulator NS 3

I INTRODUCTION

A Mobile ad hoc network is a group of wireless mobile computers (or nodes) in which nodes collaborate by forwarding packets for each other to allow them to communicate outside range of direct wireless transmission. Ad hoc networks require no centralized administration or fixed network infrastructure such as base stations or access points, and can be quickly and inexpensively set up as needed. A MANET is an autonomous group of mobile users that communicate over reasonably slow wireless links. The network topology may vary rapidly and unpredictably over time, because the nodes are mobile. The network is decentralized, where all network activity, including discovering the topology and delivering messages must be executed by the nodes themselves [17]. A mobile ad hoc network is collection of self-configuring and adaption of wireless link between communicating devices (mobile devices) to form an arbitrary topology without the use of existing infrastructure. In wireless network technology, simulative analysis is a significant method to understand the performance of routing protocol. In this paper an attempt has been made to compare the performance of two prominent on-demand reactive routing protocols for mobile ad hoc networks: The On-demand protocols, AODV perform better under high mobility simulations than the table-driven protocol. Although AODV perform well with respect to all included performance matrices in the paper if it has no constraints of bandwidth. The performance differentials are analyzed using varying network load, mobility, and network size [8].

1.1 Performance Issues in MANET

Performance in Mobile Ad-Hoc Network (MANET) is the most important concern for the basic functionality of network. To judge the quality of a protocol one needs to test them on the basis of metrics i.e. both qualitative and quantitative. These metrics are used to measure the suitability and performance of the different protocols. The metrics should be chosen carefully and should be independent of any routing protocol. The following is a list of all desirable qualitative properties of MANET as follows:-

- **Security:** - A MANET routing protocol is vulnerable to many forms of attack. They are more prone to security replay transmission, do spoofing threats than other general wired networks because the network structure is not strictly defined. Also a number of nodes keep on getting added as well as deleted from the network making it very easy for a malicious node to enter a network. Then it will be relatively easy for that node to snoop on network traffic, redirect traffic and flood the entire network. Security is very important to stop any kind of disruption of the network. There are three Attacks in security as follows:
- Wormhole Attack Detection in MANET
- Sybil Attack Detection in MANET
- DOS and blackhole Attack Detection in MANET

II. PERFORMANCE EVALUATION MATRICE

Throughput-Throughput is the average rate of successful message delivery over a communication channel. Throughput is usually measured in bits per second (bits/sec), and sometimes in data packets per second or data packets per time slot. High throughput is always desirable in a communication system.

Packet Delivery Ratio: The ratio between the numbers of packets received by the TCP sink at the final destination and the number of packets originated by the "application layer" sources. It is a measure of efficiency of the protocol.

End to End Delay- End-to-end delay refers to the time taken for a packet to be transmitted across a network from source to destination. A data packet may take longer time to reach to the destination due to queuing and different routing paths.

Average Jitter- Jitter is the variation in delay by different data packets that reached the destination and can seriously affect the quality of audio/video and thus an unwanted parameter.

Average Queue Length- It is FIFO Queue Size (bytes) in MAC layers. The length of Queue depends on congestion and route discovery
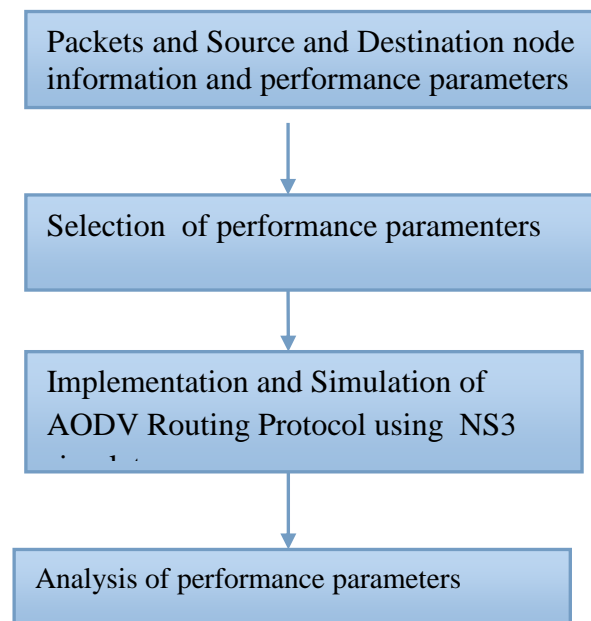
III COMMON FINDINGS

- Ranging method has costs less, no use for high accurate range, but it has extremely precise. It is particularly suitable for the low-cost, lacking resources of wireless sensor network.
- The IDS system is used for wireless *A*dhoc networks which provides with capability of detecting attacks inside and outside of system.

- A cross layer hierarchy design improves Quality of service by high communication of the layers.
- Advantage of the analytical model is presented in this paper which results offer great insights for new worm detection techniques.
- FIS system successfully detects the wormhole present in the MANET using network and physical layer parameters.
- FMS (Feature monitoring system) approach has no need to maintain any hardware requirements like directional antennas, time synchronization, and any unwanted assumptions.
- Wormhole detection technique detects the wormhole, and will serve as improved form of existing AODV protocol.
- Cross layer detection techniques achieves a high accuracy in predicting and defending the network against all Denial of Service attack.
- AODV protocol detects the legitimate path and wormhole path in the network efficiently.
- The sending Route Request (RREQ) processes with RTT method has lowest packet dropped and cannot interrupt the transmission processes thus reduces the traffic loads and increase the performance.
- There are no requirement of any special hardware like directional antennas, time synchronization, and any unwanted assumptions and any complex calculation in the AODV routing protocol.

3.1 Objectives can be outlined as follows

- To Design Network scenario for implementing existing AODV Routing Protocol.
- To make certain   modifications in AODV Routing Protocol.
- To decide input/output parameters.
- To carry out Performance Analysis of Existing and modified routing protocol.

Functional Diagram

Packets and Source and Destination node information and performance parameters

↓

Selection of performance paramenters

↓

Implementation and Simulation of AODV Routing Protocol using NS3

↓

Analysis of performance parameters

VI. CONCLUSION

The review of 20 research papers has been carried out in the area of Simulation Based Performance Analysis of Routing Protocols in Mobile ad hoc Network and find out current challenges and scope of work in the area. After the review, one issue was found which should be given proper concern, during the designing and implementation of performance analysis mechanism of routing protocols. The solution approaches under particular issues were studied in depth and were analyzed on the basis of various findings, which helped to understand the strengths and weaknesses of the solution approaches. A routing protocol plays a key role to measure the performance of a MANET. Routing protocols are classified under two categories; proactive protocols and reactive protocols.

As initial objectives, some more specific research papers related to Comparative analysis of routing protocols were reviewed. We analyzed the performance investigation of performance of routers in wireless network on the basis of AODV, DSR, and another protocols and parameters such as throughput, end to end delay and PDR. After that we proposed a Mixed Routing Protocol framework which improves performance.

Further on, we can evaluate the performance of proposed model of simulation enabled on-demand protocols. Beside this, in Future, we will incorporate route break prediction in our proposed different-different routing protocols.

REFERENCES

[1] Larry Korba ,1998," Security System for Wireless Local Area Networks ", In IEEE, National Research Council of Canada, Issue on security of WLAN ,pp1550-1554,1998.

[2] Upkar Varshney, 1998, "Design and Performance Evaluation of Connection Routing Schemes for Wireless ATM Environment", In IEEE, International Conference on Universal Personal Communications (ICUPC), pp. 409-415, 1998.

[3] Upkar Varshney, 1999," Connection Routing Schemes for Wireless ATM", In IEEE, Proceedings of the 32nd Hawaii International Conference on System Sciences, 1999.

[4] Jun-Zhao,2001,"Mobile Ad Hoc Networking :An Essential Technology for Pervasive Computing", In IEEE, IEEE Journal on Selected Areas in Communications, Issue on routing in MANET,pp 316-321,2001.

[5] Harish Sitaraman, Jesse M. Davis,Joseph B. Evans, 2001,"Broadband Wireless Local Loop Evaluation Via an Active TCP Connection Monitoring Methodology", In IEEE, IEEE Communications Magazine, Issue on Monitoring in Wireless network, pp 594-603, 2001.

[6] Prashant Krishnamurthy, Joseph Kabara, Tanapat Anusas-amornkul, 2002, "Security in Wireless Residential Networks", In IEEE, IEEE Transactions on Consumer Electronics, Vol. 48, pp.157-166, 2002.

[7] Ha Cheol Lee, 2003, "The Relation of Cell and Call Connection Level GoS for the Random Traffic in the Wireless ATM Access Transport", In IEEE, Proceedings of ICCT, pp. 886-890, 2003.

[8] Debao Xiao , Chao Chen, Gaolin Chen, 2005, "Intrusion Detection based Security Architecture for Wireless Sensor Networks", In IEEE, Proceedings of ISCIT, 2005.

[9] Shi Zhong, Taghi M. Khoshgoftaar and Shyarn V. Nath , 2005, "A Clustering Approach to Wireless Network Intrusion Detection", In IEEE, Issue on security of wireless networks, Vol.2, No.3, 2005.

[10] Wider D. YU, Vijaylaxmi Jothiram, 2007, "Security in Wireless mobile Technology for Health care System",In IEEE, Issue on security of wireless mobile technology, 2007, pp,308-311, 2005.

[11] Hany Samul, Weihua Zhuang,Bruno Presis, 2008, "Routing over Interconnected Heterogeneous Wireless Network with Intermittent Connections ", In IEEE, IEEE Communication Society, Volume 56, routing in Wireless network, pp 2282-2286, 2008.

[12] Qian Zhang, Ya-Qin Zhang, 2008, " Cross-Layer Design for QoS Support in Multihop Wireless Networks", IEEE, Volume 96, No. 1, Issue on Quality of service in Multihop networks, 2008.

[13] Hassen Redwan and Ki-Hyung Kim, 2008, "Survey of Security Requirements, Attacks and Network Integration in Wireless Mesh Networks", In IEEE, Issue on security on Wireless Mesh Networks,Japan-China Joint Workshop on Frontier of Computer Science and Technology, pp. 3-9, 2008.

[14] Nilesh Ananthanarayanan, 2008,"Vehicle Monitoring System in Wireless Networks", In IEEE,Issue on Monitoring of Wireless Networks,Vol. 26 ,no.5,pp. 141 -146, 2008.

[15] Okoli. Adaobi, Ejiro Igbesoko, Mona Ghassemain,"Evaluation of Security Problems and Instruction Detection System for Routing Attacks in Wireless Self-Oragnised Wireless Network", In IEEE, International Journal of Communications and Information Technology,Volume1,Issue on Security in Wireless Network, pp 16-20, 2012.

[16] Rashween Kaur Saluja, Rajesh Shrivastava, 2012, "A Scenario Based Approach for Gateway Discovery using Manet Routing Protocol", In IEEE, International Conference on Computer Communication and Informatics(ICCI-2012),issue on Routing in Mobile Ad Hoc Network, 2012.

[17] Yan Yu, Yubao Yao," Improved AODV Routing Protocol for Wireless Sensor Network and Implemenation using OPNET", In IEEE, Third International Conference on Intelligent Control and Information Processing july 15-17,2012-Dailan China, Issue on Routing in Wireless Sensor Network, pp 709-713, 2012.

[18] Shi-Zong, Shyarn V. Nath, 2012 "A Clustering Approach based to Wireless network intrusion detection system", Issue on security on wireless networks, IEEE, vol. 35, pp.99-101, 2012.

[19] Woosik Lee,Namgi Kim, 2013, "A study of Transmission Power Control Algorithms in wireless body sensor networks", In IEEE, Soft tech 2013 ,ASTL, Vol. 19,pp. 31-34, 2013.

[20] Lititng Cao, Shriu Zhou ,2013"Intelligent Security system based on Wireless Sensor Networks", In IEEE, First international Conference on Intelligent Networks and Intelligent Sytems,PP,143-146, 2013.