Research Paper

Computer Science

Network Security Parameter Analysis Using Simulation Approach

A. S. Mulla Dept. of Computer Applications, Bharati Vidyapeeth Deemed University, I.M.R.D.A., Sangli.(MS)

Dr. B. T. Jadhav Research Guide and Associate Professor, Dept. Of Electronics and Computer Science, Yashwantrao Chavan Institute of Science, Satara.(MS)

ABSTRACT

In wireless network, an ad-hoc network is a network without infrastructure. In mobile ad-hoc network, nodes are free to move and organize themselves in any fashion. This network provides services of type "anytime anywhere" through which information can be available at all time and everywhere. But before looking for it, one should think about security of network which is playing a crucial role in data transmission. This paper discussed few focused parameters of network security and an experimental approach for the same.

KEYWORDS : ad-hoc, infrastructure, mobile, security.

Introduction

In mobile ad-hoc network, nodes are free to move or can be static inside the network. Due to dynamic nature of nodes in ad-hoc network, no specific boundary for protection can be defined. As node can join or leave the network at any instance of time, give rise to the problem of vulnerability. So nodes may perform malicious activity like packet dropping, storing energy, utilizing less bandwidth etc. Such problem creates threats for security of network which in turn affects network performance in terms of throughput, packet delivery ratio, end to end delay etc. Regarding this we have to focus on some important parameters of a mobile node like -

- Packet dropping ratio
- Mobility
- Speed
- Energy
- Bandwidth utilization
- Time

By considering these parameters, we can focus on security of network by its categorization and its simulation showing the result of same.

ROLE OF NETWORK ATTACKER PARAMETERS

As mentioned above, we can see one by one parameter and its role in network security. As we know a misbehaving node may creates some type of vulnerabilities in the network. Misbehaving nodes can be categorized as either a malicious node or selfish node. Selfish nodes are nodes that participate in the network to maximize their own benefit by using network resources while saving their own resources. Whereas Malicious nodes directly attack a network by disrupting its normal operation.

Packet dropping is a passive attack which can result in repeated retransmissions, which in turn may cause network congestions. As a wireless link does not provide the same protection for data transmissions as does its wired link counterpart. Hence, any user or receiver within the transmissions range can eavesdrop or interfere with data packets or routing information.

Energy is also one of important resource, specifically the battery power of the service provider. Since mobile devices operate by battery power, energy plays crucial role in MANETs. A node consuming less energy is considered as a malicious node which may continuously send a bogus packet to a node with the intention of consuming the victim's battery energy and preventing other nodes from communicating with the node. The use of localized monitoring can help in detecting such nodes and preventing their consequences.

For bandwidth utilization, consider the case where an attacker located between multiple communicating nodes

wants to waste the network bandwidth and disrupt connectivity. The malicious node can send packet with bogus source IP addresses of other nodes, thereby overloading the network. This consumes the resources of all

neighbors that communicate, overloads the network, and results in performance degradations. Such attacks can be

prevented based on the reputation information exchanged among the involved nodes or the cluster head.

Since all nodes can be mobile, changes in network connectivity and resource availability also expose a network to various attacks. This calls for detection and prevention of attacks in the network.

PROPOSED SCHEME

When a malicious node receives an application packet from a node destined for some other node then instead of forwarding that packet, it simply drops that packet. This data loss may become severe when number of malicious nodes present in network is high. For the same, we can create a scenario for any number of nodes with following combinations

- Only one Source, One mediator and Only one Destination
- Two sources, One mediator and Two Destinations.
- Any number of Sources, Any number of Mediators and any number of Destinations.

From such scenario, one can analyze packet dropping ratio for each and every path in every scenario which will be helpful for us to suggest secure path or route (considering mediators role) in each scenario.

For energy parameter also we can create scenario with and without mobility starting from low to any number of nodes with varying number of sources, mediators and destinations giving variable huge database of energy for various nodes which can be used to find a mediator utilizing more energy and consuming less energy which will be useful for us to find malicious activity of nodes.

If we go for speed and mobility parameters, one can say that a speedy and mobile node may affect network performance affecting network security. For analysing the same we can create scenario using ns-2 to simulate the effect of same.

A transmission or retransmission showing delay for data transmission also shows misbehaviour of a node.

After analysing this whole database one can suggest proper solution for security of network and also to depict correct result, we can use fuzzy logic approach. Fuzzy logic approach will be helpful for us to design a decision making system for network security and this designed DSS will be very useful for a third party to take proper decision while moving towards network security.

PERFORMANCE EVALUATION

To analyze the performance of our solution, various contexts will be created by varying the number of nodes in terms of number of sources, number of destinations and number of mediators. By using such scenarios we can get several databases for above mentioned parameters using NS2. From it we can analyze following evaluation metrics:

Average Packet delivery ratio (PDR):

It is defined as the ratio of the total number of data packets received by destinations and the total number of packets sent by a source. This metric shows the reliability of data packet delivery.

Packet Loss:

This metric informs us about the amount of control packets fails to reach its destination in a timely manner.

Depending on which one can determine the performance and fairness of network the considering its Throughput, Delay etc parameters to carry out its work safely and efficiently.

CONCLUSION

Our proposed work will be helpful for ad-hoc network as one of decision making system to detect malicious node and its behavior in existing scenario. From which it is possible to consider parameters affecting on network security and we can go for providing better security for our network which will improve network performance and its fairness. For simulation we may use ns2 (Network Simulator-2) as a simulator.

REFERENCES

[1] Ajay Sharma, “Performance Evaluation of AODV under Blackhole attack in MANET using NS2 simulator”, International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), Volume 1, Issue 8, October 2012 ISSN: 2278 – 1323 | [2] Alper T. M_zrak, “Detecting Malicious Packet Losses”, IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 20, NO. 2, FEBRUARY 2009 191 | [3] Anil Kumar Gupta, “Detecting and Dealing with Malicious Nodes Problem in MANET”, International Journal of Scientific & Engineering Research, Volume 4, Issue 7, July-2013 161 ISSN 2229-5518 IJSER © 2013 | [4] Ankur Ratmele “Performance Analysis of AODV under Worm Hole Attack through Use of NS2 Simulator”, International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com Vol. 3, Issue 3, May-Jun 2013, pp.201-205 | [5] Jose Anand, K. Sivachandar “Vampire Attack Detection in Wireless Sensor Network”, International Journal of | Engineering Science and Innovative Technology (IJESIT) Volume 3, Issue 4, July 2014. | [6] Ranjeet Suryawanshi, Sunil Tamhankar, “Performance Analysis And Minimization Of Black Hole Attack In MANET”, International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com Vol. 2, Issue4, July-August 2012, pp.1430-1437 | [7] Rooshabh Kothari, “Implementation of Black Hole Security Attack using Malicious Node for Enhanced - DSR Routing Protocol of MANET”, International Journal of Computer Applications (0975 – 8887) Volume 64– No.18, February 2013 | [8] S.Gopinath1& M.Vetriselvan, “A New Mechanism for Malicious Detection in MANET”, International Journal of Advanced Information Science and Technology, Vol.5, Iss.5, 2012 ISSN: 2319-2682 | [9] Syed S. Rizvi and Khaled M. Elleithy, “A New Scheme for Minimizing Malicious Behavior of Mobile Nodes in Mobile Ad Hoc Networks”, (IJCSIS) International Journal of Computer Science and Information Security Vol. 3, No.1, 2009 | [10] Vinod Kumar, “A Fuzzy Based Control over Malicious Nodes in Manet”, International Journal of Latest Trends in | Engineering and Technology (IJLTET) |