ISSN: 2278 – 7798
International Journal of Science, Engineering and Technology Research (IJSETR)
Volume 2, Issue 2, February 2013

A Survey on: Resource Consumption Index of Denial of Service Attack in MANET

Pranita Joshi
Sri Satya Sai Institute of Science & Technology, Sehore

Gajendra Singh Chandel
Sri Satya Sai Institute of Science & Technology, Sehore

Shubham Joshi
Sri Aurobindo Institute of Technology, Indore

Abstract: Resource consumption is the biggest issue while working with wireless networks. Especially when we are in public networks and need to share our infrastructure with others unauthorized and unidentified network components. The problem occurs from connection establishment to communication with these networks. The rate of resource consumption may degrade the performance of existing infrastructure and aligned infrastructure when vulnerabilities comes into effect. This paper has a brief review and proposed a novel concept of Resource Consumption Index of DOS attacks, causes, vulnerabilities and their countermeasures in Mobile Ad Hoc Networks. The work emphasized with the keen consideration of all active and inactive mobile terminals which can either invite attackers by misconception or may become route cause of attacks by their related and surrounded mobile nodes.

Keywords: Denial of Service, mobile terminals misconception, attacks.

I. Introduction:

Denial of service attacks are the collection of fake messages that attacks on resources by misleading services and error prone methods to degrades the performance of networks by overfilling a unit using big number of fake information. The Mobile ad hoc network (MANET) is a dynamic, autonomous multi-hop network. Mobile Networks are not addicted to dedicated infrastructure and can be assembled with dynamism. The Communication between source and destination node in such networks is dependent on participating communicative nodes.

Wireless networks are capacitive in terms of many applications run over it, viz. unrestrained conversations, in military battlefields, academics, hospital and tourism etc. In all such applications a dynamic communication is mandatory. Fei Xing et al [1] described, all these applications require mobile, autonomous and dynamic formation of networks in mobile scenario. There may be two flavors of MANET: closed and open network. Liu et al [2] incepted, In case of closed MANET such as military application, all communicating nodes co-operate towards a common desired goal. Next node entry can be done by the authorized nodes. In open MANET, nodes are free to join the application network and leave the network. Their operational goals may be different.

This scene can be compared with the online video conferencing system where one can interact directly with means of conferencing and shared camera. Both the ends the user can communicate and experience a sole user. But this infrastructure also may have many number of weaknesses in terms of connection, authentication, information distribution and open end mechanism. The open end mechanism is the phenomenon by which no one can filter the upcoming request or node while communicating with video conferencing. As compared to dedicated wired network there are various vulnerabilities exists and this represents due to node's multi-hop nature. These networks are liable to have many attacks at a time and cause distributed denial of service

attack. Privacy, Reliability, consistency and ease of use can be essential requirements for a MANET to be secure and error free. In order to achieve Privacy and Reliability, there are many cryptographic solutions like symmetric and asymmetric cryptography algorithm. The ultimate goal for security solutions under MANET is to cover all security services, which also include accessibility of resources.

While in wireless scenario as the infrastructure is unavailable, the hope of formation of communication hierarchy based on traversed hop-to-hop. So, the nature and type of attacks will be different as of wired network. However the solutions for availability of wired networks are not applicable to MANETs because of different nature of attacks. Security solutions in MANET is challenging because of characteristics of MANETs such as its autonomous and mobile nature.

II. Literature Survey:

There are number of vulnerabilities exist in MANETs as compared to the wired network due to their multi-hop nature. These networks are susceptible to much new kind of attacks such as Black hole, wormhole and jellyfish attacks. Secrecy, integrity and availability are considered to be essential security requirements for MANETs. In order to achieve secrecy and integrity, there are cryptographic solutions like symmetric and asymmetric cryptography algorithm exist, which were initially available to the wired network. The ultimate goal for security solutions under MANET is to cover all security services, which also include availability. In case of MANET, as the infrastructure is unavailable, communication has to hop-by-hop. So, the nature and type of attacks will be different as of wired network. However the solutions for availability of wired networks are not applicable to MANETs because of different nature of attacks.

Security solutions in MANET is challenging because of characteristics of MANETs such as its autonomous and mobile nature. Denial of Service attack makes network connectivity unavailable to the intended user of the network. DOS attacks impact connectivity of the network severely. DOS attacks in wired network exist because of vulnerabilities of communication protocols of the network. For example SYN flood attack, where DOS attacks use 3-way handshake protocol of TCP. DOS attacks in case of MANET become multifold as compared to that of wired network. As the communication in MANET is hop by hop through intermediate nodes; internal nodes of network may intern attacks other neighboring nodes within the network.

W. Stalling et al. [3] described, that basically Denial of Service attack has two categories of attacks in MANET viz. Passive and Active attacks. Passive attacks do not affect the rate of consumption of resources, as the approach of this attack in table driven. While an active attack can badly affect rate of resource consumption. The cause of this affect is just because of the approach which is on demand, that means occurrence of node and their relevance cannot be predefined. Other than this DOS attacks there are various attacks related to type of DOS attack viz. black-hole, flooding attacks, wormhole attack, detour attack etc.

J. Cai et al [4] discussed. A particular DOS attack may fall in many categories. For example black hole attacks may be considered as active and passive both as well as co-operative and single node attack. Sleep deprivation torture attack is categorized as a type of flooding attack as well as a routing disruption attack. M K. Denko et al [5] discussed the potential of DOS attack is the most disastrous and tedious to solve in public networks. It's a commonly characterized as an event in which a large number of unwitting hosts are used as an attack forces against the victim to exhaust either their computational or

communication resources. As a result, legitimate users are denied from the services that they normally expect to perusal. Therefore, DOS attacks attempt show numerous characteristics:

a. To inhibit legitimate network traffic by flooding the network with useless traffic.
b. To deny access to a service by disrupting connections between two parties.
c. To block the access of a particular individual to a service.
d. To disrupt the specific system or service itself.

Denial of service attack can be done with means of other routing attacks like, route disruption attack, wormhole attack, black-hole attack, colluding mis-relay attack etc. each attack shown a great relevance in terms of denial of service from legitimate nodes. All these attack collectively shown their impacts in routing misbehavior and the node or communicating component get revealed. Various intrusion detection systems also explained the root cause of their intrusions and malwares are due to lack of expected service from node and surrounding components.

III. Classification of DOS Attack:

The classification specifies the type of attack relevant to the anomalies and misconception occurred in MANET hierarchy. The effect of Denial of service attack comes into consideration when all participating nodes and network components shown a volatile nature in routing strategies. Following are the classification based on various aspects

- **General Classification of DOS attack:**
  - Passive DOS Attack
  - Active DOS Attack

- **Classification based on purpose of DOS attacks:**
  - DOS attacks target bandwidth
  - DOS attacks target energy resource
  - DOS attacks target storage processing resources

- **Based on target of attack:**
  - DOS attacks targeting single node
  - DOS attacks targeting whole network

- **Based on number of attacking nodes**
  - Single node attack
  - Cooperative DOS Attack

Malicious nodes may also target the bandwidth of the network. Node may use IP spoofing and send forged packets, which appears to come from another source in order to degrade the bandwidth of the network.

IV. Layer Wise DOS attacks:

In terms of Mobile Ad hoc networks, the Denial of service attack, works on physical, data-link and network layer of OSI reference model. Lower layer attacks can be triggered with the common anomalies done at physical layer at the time of raw data and information gatherings. These anomalies moved further with the inception of framing and integration of data with other information string at data link layer. Further after address resolution and packet generation these anomalies become hazards and routing strategy can be tampered. This way the attackers launch any denial of service attack which further impacts on route disruption

- **Lower Layer Attacks (On Physical and Data link Layers)**
  a. Jamming Attacks
  b. Binary Exponential Back Off Attacks
  c. Wireless interference Attacks

- **Network Layer Attacks:**

1. **Routing Disruption Attack**
   a. Black hole attack
   b. Wormhole attack
   c. Rushing attack
   d. Sleep Deprivation Torque Attack

2. **Forwarding Disruption Attack**

   a. Jelly fish Attacks
   b. Directional Antenna Abusing Attacks
   c. Dynamic Power Transmission (Range Attack)

3. **Resource Consumption Attack**

   a. Flooding Attacks
   b. RREQ Flooding Attacks
   c. Data Flooding Attacks
   d. Routing Table Overflow Attacks
   e. Sleep Deprivation Torque Attacks

V. Other DOS Attacks

Colluding Misrelay Attack:

In colluding misrelay attack, multiple attackers work in collusion to modify or drop routing packets to disrupt routing operation in a MANET. By this way packet transmission, packet delivery time and end to end delay disturbed hence the packet drop and node disruption attack occurred concurrently. This attack is difficult to detect by using the conventional methods such as watchdog and pathrater [6].

VI. Proposed Work:

Based on our literature survey we analyzed the clear line defense of Denial of service attack in mobile scenario. The classification of DOS attacks and their study schematized the formulation of an index of resource consumption. This can be reduced by applying front line defense to all DOS attacks by mitigating the effects of denial of service attack in MANET. Our emphasis is to define new routing strategies for the complete elimination of service quality errors by improving the quality of service issues in denial of service paradigm. The colluding approach to develop and propose new protocol architecture for denial of service attack is the ultimate virtue of our study on resource rate consumption index and attack parameters of DOS and cooperative attacks. The present schemes of denial of service attack prevention are not so fruitful to complete mitigation of flaws. Due to cooperative DOS and relative attacks the node improvising is difficult to apply. So, to develop an algorithm and architecture of resource rate consumption index along with cooperative DOS attacks and may solve all these issues. The architecture and simulation of this work can give a novel paradigm to form a novel protocol on cooperative DOS attack.

VII. Conclusion:

The next generation protocols of security will show plethora of novel architectures in wireless scenario. To improvise these emergent issues and challenges in security architecture of MANET we need to develop a common protocol which can cover all strokes of DOS flavors into one. Our current study showed the rigorous work done by researchers on classification of Denial of service attack and related Cooperative DOS attacks in MANET. However, simulation study of DOS patterns may exhibit various findings which can help

research community to update routing strategies for next generation mobile networks.

REFERENCES:

[1] Fei Xing, Wenye Wang, "Understanding Dynamic Denial of Service Attacks in Mobile Ad Hoc Networks" in proc. of IEEE MILCOM'06 conference on Military communications.

[2] Kejun Liu, Jing Deng, Pramod K. Varshney, Kashyap Balakrishnan, "An Acknowledgment-Based Approach for the Detection of Routing Misbehavior in MANETs", in IEEE Transactions On Mobile Computing, Vol. 6, No. 5, May 2007.

[3] William Stallings, "Cryptography and Network Security", Pearson Education, IV edition, 2005

[4] Jiwen CAI, Ping Yi, Ye Tian, Yongkai Zhou, Ning Liu, "The Simulation and Comparison of Routing Attacks on DSR Protocol" in Proceedings of the 5th International Conference on Wireless communications, networking and mobile computing (WiCOM'09)

[5] Mieso K. Denko, ''Detection and Prevention of Denial of Service Attacks in Mobile Ad hoc
Networks using Reputation based Incentive Scheme'' Systemics, Cybernetics and Informatics Vol. 3.

[6] S. Marti et al., "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks," 6th MobiCom, Boston, MA,Aug.2000.