Quest Journals
Journal of Electronics and Communication Engineering Research
Volume 2 ~ Issue 6(2014) pp: 01-06
ISSN(Online) : 2321-5941
www.questjournals.org

Research Paper

Detection Approach for Denial of Service Attack in Dynamic Wireless Networks

Deepesh Namdev[1], Monika Mehra[2]
[1]*HOD cum Associate Professor (E&C, EE), Gurukul Institute of Engg. & Technology, Kota(Raj), India*
[2]*Student of Gurukul Institute of Engg. & Technology, Kota (Raj), India*

Received 17 June, 2014; **A**ccepted 07 July, 2014 © The author(s) 2014. Published with open access at **www.questjournals.org**

***ABSTRACT*:-** *Mobile ad hoc networks are dynamic mobile networks that can be formed in the absence of any pre-existing communication infrastructure. In addition to node mobility, a MANET is characterized by limited resources such as bandwidth, battery power, and storage space. The underlying assumption in MANETs is that the intermediate nodes cooperate in forwarding packets. However, this assumption does not hold in commercial and emerging civilian applications. MANET is quickly spreading for the property of its capability in forming rapidly changing topologies network without the aid of any established infrastructure or centralized administration. The security challenges in MANET have become a primary concern to provide secure communication. The Attacks on MANET disrupts network performance and reliability. The DOS (denial-of-service), Distributed denial-of-service (DDoS) attacks are a rapidly growing problem. The multitude and variety of both the attacks and the defence approaches is overwhelming. These attacks lead toward the degradation or prevention of legitimate use of network resources. In this paper kind of attacks are presented which are attacked on ad-hoc network. The motive of the study is aware about different service availability attacks and its effects on network operation.*

***KEYWORDS*:-** *Attacks, DOS, Distributed DOS, MANETs, TTL.*

I. INTRODUCTION

Wireless networks are inherently susceptible to security problems. The intrusion on the transmission medium is easier than for wired networks and it is possible to conduct denial of service attacks by scrambling the used frequency bands. The ad hoc context increases the number of potential security vulnerabilities. Ad hoc networks can not benefit from the security services offered by dedicated equipment such as firewalls, authentication servers and so on. The security services must be distributed, cooperative and consistent with the available bandwidth.

One of the serious attacks to be considered in ad hoc network is DDoS attack. A DDoS attack is a large-scale, coordinated attack on the availability of services at a victim system or network resource. The DDoS attack is launched by sending an extremely large volume of packets to a target machine through the simultaneous cooperation of a large number of hosts that are distributed throughout the network. The attack traffic consumes the bandwidth resources of the network or the computing resource at the target host, so that legitimate requests will be discarded [1]. A bandwidth depletion attack is designed to flood the victim network with unwanted traffic that prevents legitimate traffic from reaching the victim system. A resource depletion attack is an attack that is designed to tie up the resources of a victim system. This type of attack targets a server or process at the victim making it unable to legitimate requests for service. Any amount of resources can be exhausted with a sufficiently strong attack. The only viable approach is to design defence mechanism that will detect the attack and respond to it by dropping the excess traffic. The effect of these attacks varies from temporarily blocking service availability to permanently distorting information in the network.

DoS attacks can target a client computer or a server computer. For example, an attack may target a system by exhausting limited wireless resources such as bandwidth, storage space, battery power, CPU, or system memory. Networks and applications can be attacked by modifying routing information or changing

system configuration, thereby directly attacking data integrity [2].

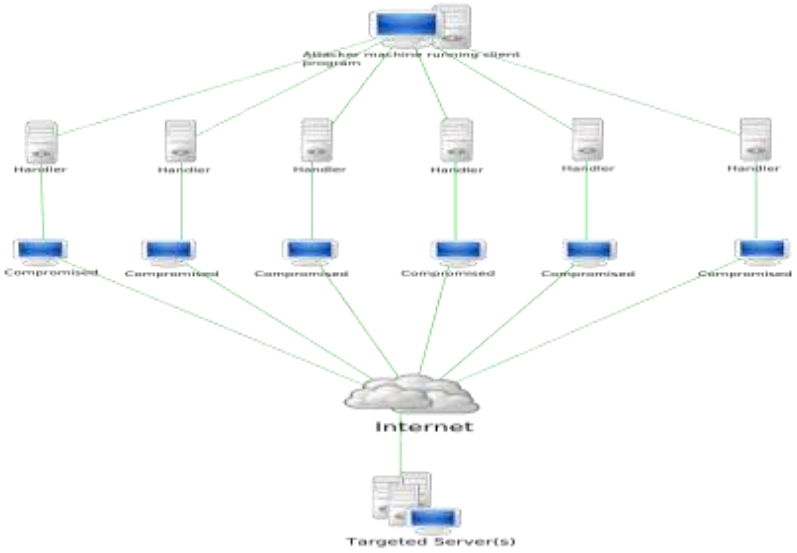

Fig.1: Dos attack on network

II. ATTACKS

Attacks for MANET's. can be identified into two categories either active or passive, according to the attack means. Active attacks can modify data, disrupt network operation, or disable services [3]: Active attacks on network routing include flooding, modifying routing information, providing false route requests and replies, attracting unexpected traffic, hiding error messages, and fabricating false error messages.

Passive attacks do not alter data but fail to cooperate in providing services such as routing and packet forwarding. Passive attacks include packet dropping to conserve resources. These abnormal node behaviours result in performance degradation and cause denial of service attacks, packet losses, longer delays, and low throughput.

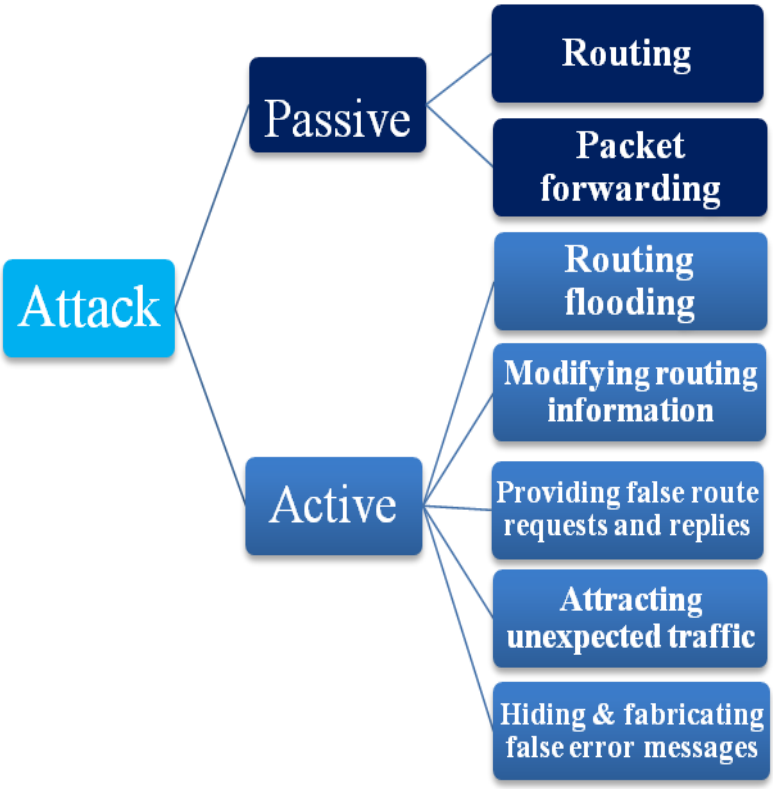

Fig.2: Types of attack

The Security Attacks on each layer in MANET can be identified as:-
Distributed denial-of-service attack is characterized by an explicit attempt by attackers to prevent the legitimate use of a service. Denial of Service (DoS) is the degradation or prevention of legitimate use of network resources The MANETs are vulnerable to Denial of Service (DoS) due to their salient characteristics.
DoS attacks that target resources can be grouped into three broad scenarios namely as:

- Those attack scenario targets Energy resources, specifically the battery power of the service provider(In such these attacks a malicious node may be 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.

- Those attacks aimed at targeting Storage and Processing resources (these attacks are carried out mainly to target memory, storage space, or CPU of the service provider).

- The third attack scenario targets bandwidth, where an attacker located between multiple Distributed denial of service attack is an attempt to prevent or degrade availability of any resources. For this multiple source hosts at the same time to send attack traffic. Since DoS attack the attacker uses a single source host to send attack traffic to a victim. A distributed DoS (DDoS) attack involves more than one sources of attack traffic. Distributed denial-of-service attack is one such kind of attack, which poses an immense threat to the availability of a service or resource. These attacks are sometimes referred to as "flooding" attacks.

III. BACKGROUND

The security issues for MANET's [4] can be analyzed on basis of individual layers namely application layer, transport layer, network layer, link layer and physical layer. On the network layer, an adversary could take part in the routing process and exploit the routing protocol to disrupt the normal functioning of the network. Network layer is more vulnerable to attacks than all other layers in MANET. A variety of security threats is imposed in this layer. Both routing and packet forwarding operations are vulnerable to malicious attacks, leading to various types of malfunction in the network layer. Since the main network-layer operations in MANETs are usually ad hoc routing and data packet forwarding, which interact with each other and fulfill the functionality of delivering packets from the source to the destination, The Network layer vulnerabilities for MANET's fall into following two categories

- Routing attacks and
- Packet forwarding attacks

The security approach in MANET requires an accurate analysis and classification of denial of service attacks (more specifically DDoS) specific to the dynamic (ad-hoc) networks environment. A countermeasure against node misbehavior in general and denial of service attacks in particular is our prime source of concern [5]. Service availability must guarantee that all resources of the communications network are always utilizable by authorized parties. A denial-of-service attack is characterized by an explicit attempt by attackers to prevent the legitimate use of a service. A distributed denial-of-service (DDoS) attack deploys multiple machines to attain this goal. DDoS attacks on the Network disrupt the availability of a service or resource. DDoS attack is an example of a bandwidth attack. Consequences of DDoS attacks may even have greater effect if the attempt or location of DDoS attack is Cluster-Head. In this section, an overview of the existing methods & procedures are reviewed to enable MANET's to overcome DDoS attacks. A Reputation-based incentive mechanism for detecting and preventing DoS attacks in MANETs. A clustering architecture was proposed for performing reputation data management in a localized and distributed manner. DoS attacks were detected through collaborative monitoring and information exchange. Reputation rating was carried out using neighbourhood and cluster level information with more weight given to a node's own observation. A load balancing mechanism was used to reduce traffic on heavily used cooperative nodes. The security challenges related to MANET gives information about various security threats an ad-hoc network faces, the security services required to be achieved and the countermeasures for attacks in each layer. As per the contents of this paper, secure routing protocol is still a burning question. There is no general algorithm that suits well against the most commonly known attacks such as wormhole, rushing attack etc. In short, we can say that the complete security solution requires the prevention, detection and reaction mechanisms applied in MANET. The LID Algorithm is the Lowest ID Algorithm. The LID algorithm is used to Determine cluster heads and the nodes that constitute the cluster. Each node is assigned a unique id and a node with the lowest ID is chosen as the Cluster-Head, all the nodes within radius R around that node are its members. The process repeats until every node belongs to a cluster.

SPIRITE, an incentive based system in which selfish nodes are encouraged to cooperate. In this system, a node reports to the Credit Clearance Service, the messages that it has received/forwarded by uploading its

receipts. Intermediate nodes earn credit when they forward message of others' node. In addition to the availability of central authority, sprite assumes source routing, and a public key infrastructure.

IV. RELATED WORK

Recently proposed incentive mechanisms for enforcing cooperation among nodes can be classified into trade-based and trust-based mechanisms. Trade-based mechanisms assume market models for providing virtual currency incentives for motivating cooperation among nodes. In the trust-based models, trust is created and the service provider is stimulated by these trust values. Each scheme can be deployed in different application scenarios. The trade-based models are not applicable in cooperative networks where no financial incentives are needed to run the network. However, trust-based schemes can still be used to improve network performance. In the trade-model proposed in [6], every device has a tamper- resistant security module, PKI to ensure authentication. This security module is used for account management. Two billing models that charge nodes as a function of number of hops messages have travelled were proposed. An ad hoc participation economy (APE) that uses a dedicated banker node to manage accounts was proposed in [7]. Unlike the tamper-resistant mechanism, the APE uses dedicated banker nodes for account management and also has facilities for converting virtual currency into real monetary units. Incentive mechanisms that use a node as a transaction manager are not plausible in dynamic ad hoc networks since location tracking incurs additional overhead. A similar reputation-based mechanism known as a reputation participatory guarantee (RPG) was proposed [8]. This mechanism provides a network layer solution that detects selfish nodes without propagating reputation ratings in the network. A trade-based model that relies on the accessibility of banker nodes was proposed in [9]. This model does not use any tamer- resistant hardware but instead uses credit-clearance services in a wireless overlay network. In [10], a reputation-based model that investigates the effect of misbehaviour on network performance was presented. It uses a watchdog for identifying misbehaving nodes and a pathrater for selecting routes that do not select misbehaving nodes. In [11], CONFIDANT, a reputation-based model that removes misbehaving nodes by propagating bad.

Reputation through the network was proposed. In [12], a reputation based model that only propagates positive reputations among the nodes was proposed. Reputation computation involves the aggregation of three different types of information based on different levels of observations and services. This method of reputation computation incurs greater overhead than other proposed schemes. Existing incentive mechanisms for enforcing cooperation can be classified into trade-based and reputation-based. While the former uses a payment-based incentive, the latter uses mutual ratings based on services provided among the nodes. While extensive work has been carried out on confidentiality, integrity, and privacy attacks, the threat to network availability has received less attention. Availability is an important requirement for improving network performance. Existing studies on DoS attacks concentrate on the analysis of various attack scenarios targeting a specific layer, or propose a probing mechanism to detect misbehaving nodes that target a specific network layer function. While using a probing mechanism can help in detecting DoS attacks, probing packets may introduce communication overhead in the larger network. Reputation rating coupled with localized probing mechanisms can alleviate this problem.
Xiapu Luo et al [13] have presented the important problem of detecting pulsing denial of service (PDoS) attacks which send a sequence of attack pulses to reduce TCP throughput. Wei-Shen Lai et al [14] have proposed a scheme to monitor the traffic pattern in order to alleviate distributed denial of service attacks. Shabana Mehfuz1 et al [15] have proposed a new secure power-aware ant routing algorithm (SPA-ARA) for mobile ad hoc networks that is inspired from ant colony optimization (ACO) algorithms such as swarm intelligent technique.
Xiaoxin Wu et al [16] proposed a DoS mitigation technique that uses digital signatures to verify legitimate packets, and drop packets that do not pass the verification Ping Yi, Zhoulin Dai, Shiyong Zhang and Yiping Zhong [17] have presented a new DOS attack and its defense in ad hoc networks. The new DOS attack, called Ad Hoc Flooding Attack(AHFA), can result in denial of service when used against on-demand routing protocols for mobile ad hoc networks.

V. PROBLEM DEFINITION AND SOLUTION

Distributed Denial of Service (DDoS) is a powerful attack which consumes the network as well as system resources. The attack is usually initiated by an attacker host which paralyses the entire network by flooding heavy network traffic. Thus the sharing process that takes place among the various nodes in the network gets disrupted. Moreover, an attacker compromises a large number of nodes which act as a part of the attack by exploiting the entire network resources. The malicious traffic generated by the nodes will be very high that the victim node cannot afford to it. Also, it is difficult to identify these attacks since most of the IP packets are created in a fake manner. An attacker causes congestion in the network by either generating an excessive amount of traffic by itself, or by having other nodes generate excessive amounts of traffic. In wireless networks, DDoS attacks are difficult to prevent and protect against. They can cause a severe degradation of network

performance in terms of the achieved throughput and latency. DDos attacks can apply individual layer of networks such MAC and Network layer in different forms. At the MAC layer the following DDOS attacks can be attempted:

a) Since we assume that there is a single channel that is reused, keeping the channel busy in the vicinity of a node leads to a denial of service attack at that node.

b) By using a particular node to continually relay spurious data the battery life of that node may be drained.

DDOS attacks at the routing layer could consist of the following:

a) The malicious node participates in a route but simply drops a certain number of the data packets. This causes the quality of the connections to deteriorate and further ramifications on the performance if TCP is the transport layer protocol that is used.

b) The malicious node transmits falsified route updates. The effects could lead to frequent route failures thereby deteriorating performance.

c) The malicious node could potentially replay stale updates. This might again lead to false routes and degradation in performance.

d) Reduce the TTL (time-to-live) field in the IP header so that the packet never reaches the destination.

A lot of works have been done on detection and prevention of DDos attacks at both of layer which have included different form. Rather than this some work require against DDos attack which focuses modifications of TTL value by malicious node. To rectify or reduce the tampering of time to live form of distributed denial of service attack which target the TTL field of routing packets, efforts are putting to advised a mechanism. Advised mechanism basically deals with time to live field of IP packets, which is able to detect TTL value tampered by malicious nodes. A decision is taken on the basis of comparison of TTL value with number of hopes from source to destination. If TTL value is small than number of hope counts means value is tempered by malicious node otherwise packet reached at destination at given TTL value.

VI. CONCLUSION

The evolution in intruder tools is a long- standing trend and it will continue. And, DoS attacks by their very nature are difficult to defend against and will continue to be an attractive and effective form of attack. To investigate the issue of distributed denial of service by means of the proposed architecture and mechanism for detection and control of DDOS attacks over reputation and score based MANET. To studied a novel DoS attack perpetrated by Jel- lyFish: relay nodes that stealthily misorder, delay, or periodically drop packets that they are expected to forward, in a way that leads astray end-to-end congestion control protocols. This attack is proto- col-compliant and yet has a devastating impact on the throughput of closed-loop flows, such as TCP flows and congestion-controlled UDP flows. For completeness, we have also considered a well- known attack, the Black Hole attack, as its impact on open-loop flows is similar to the effect of JellyFish on closed-loop flows. We studied these attacks in a variety of settings and have provided a quantification of the damage they can inflict. We showed that, perhaps surprisingly, such attacks can actually increase the capacity of ad hoc networks as they will starve all multihop flows and provide all resources to one-hop flows that cannot be intercepted by JellyFish or Black Holes. As such a partitioned system is clearly undesirable; we also consider fairness measures and the mean num- ber of hops for a received packet, as critical performance measures for a system under attack.

REFERENCES

[1] S.A.Arunmozhi, Y.Venkataramani, " DDoS Attack and Defense Scheme in Wireless Ad hoc Networks", International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.3, May 2011

[2] Mieso K. Denko, "Detection and Prevention of Denial of Service (DoS) Attacks in Mobile Ad Hoc Networks using Reputation-Based Incentive Scheme", SYSTEMICS, CYBERNETICS AND INFORMATICS VOLUME 3, NUMBER 4

[3] Rizwan Khan, A. K. Vatsa, " Detection and Control of DDOS Attacks over Reputation and Score Based MANET ", Journal of Emerging Trends in Computing and Information Sciences VOL. 2, NO. 11, October 2011

[4] H Yang , H Y. Luo , F Ye , S W. Lu , and L Zhang, " Security in mobile ad hoc networks: Challenges and solutions " (2004). IEEE Wireless Communications. 11 (1) , pp. 38 - 47 Postprint available free at: http://repositories.cdlib.org/postprints/618.

[5] Rizwan Khan, A. K. Vatsa, " Detection and Control of DDOS Attacks over Reputation and Score Based MANET ", Journal of Emerging Trends in Computing and Information Sciences VOL. 2, NO. 11, October 2011

[6] L. Buttyan and J. Hubaux, "Stimulating cooperation in self- organizing mobile ad hoc networks," ACM/Kluwer Mobile Networks and Applications (MONET) 8 (2003).

[7] M. Baker, E. Fratkin, D. Guitierrez, T. Li, Y. Liu and V. Vijayaraghavan, "Participation incentives for ad hoc networks," http://www.stanford.edu/~yl31/adhoc (2001).

[8] D. Barreto, Y. Liu, J. Pan and F. Wang, "Reputation-based participation enforcement for adhoc networks," http://www.stanford.edu/~yl314/adhoc (2002).

[9] S. Zhong, J. Chen and Y.R. Yang, "Sprite: A simple, cheat- proof, credit-based system for mobile ad-hoc networks," Technical Report 1235, Department of Computer Science, Yale University (2002).

[10] S. Marti, T.J. Giuli, K. Lai and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," In: Mobile Computing and Networking. (2000) 255–265.

[11] S. Buchegger and J.Y.L Boudec, "Performance Analysis of the CONFIDANT Protocol: Cooperation Of Noes — Fairness In Distributed Ad-hoc NeTworks," In Proc. Of IEEE/ACM Workshop on Mobile Ad Hoc Networking and Computing (MobiHOC),

Lausanne, CH, IEEE (2002) 226–236.
[12] P. Michiardi and R. Molva, "Making greed work in mobile ad hoc networks," Technical report, Institut Eur´ecom (2002).
[13] Xiapu Luo, Edmond W.W.Chan,Rocky K.C.Chang: Detecting Pulsing Denial-of-Service Attacks with Nondeterministic Attack Intervals, EURASIP Journal on Advances in Signal Processing (2009)
[14] Wei-Shen Lai, Chu-Hsing Lin , Jung-Chun Liu , Hsun-Chi Huang, Tsung-Che Yang: Using Adaptive Bandwidth Allocation Approach to Defend DDoS Attacks, International Journal of Software Engineering and Its Applications, Vol. 2, No. 4, pp. 61-72 (2008)
[15] Shabana Mehfuz, Doja,M.N.: Swarm Intelligent Power-Aware Detection of Unauthorized and Compromised Nodes in MANETs", Journal of Artificial Evolution and Applications (2008)
[16] Xiaoxin Wu, David,K.Y.Yau, Mitigating Denial-of-Service Attacks in MANET by Distributed Packet Filtering: A Game-theoretic Approach, in Proceedings of the 2nd ACM symposium on Information, computer and communication security, pp 365-367 (2006)
[17] Security Scheme for Distributed DoS in Mobile Ad Hoc Networks, ACM, Newyork,USA (2004) Ping Yi, Zhoulin Dai, Shiyong Zhang, Yiping Zhong: A New Routing Attack in Mobile Ad Hoc Networks, International Journal of Information Technology, Vol. 11, No.2 (2005)