Detection Mechanism for Distributed Denial of Service (DDoS) Attack in Mobile Ad-hoc Networks

Deepak Vishwakarma
PG Scholar
Indore Institute of science & Technology, Indore (MP), India

D.S. Rao, PhD
Dean, CSE Department
Indore Institute of science & Technology, Indore (MP), India

ABSTRACT
Mobile ad hoc networks are non-static networks which formed without any central point communication infrastructure. In addition to node mobility, a ad-hoc is defined by bounded resource constraints such as bandwidth, battery power, and storage space. In this network, the intermediate nodes play role of router which routed the packets to the terminal node. The security challenges in the networks 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 influences network resources, denying of service for genuine node and degrades network performance. In this paper kind of attacks are presented which are attacked on ad-hoc network and advised approach to detect DDoS attack.

Keywords
MANETs, Attacks, DoS, Distributed DoS.

1. INTRODUCTION
Wireless networks are inherently susceptible to security problems. The attacks on the wireless are easier than for wired networks because it has lack of physical thing and it is possible to conduct deny of service. Ad hoc networks can not benefit from the security services such as physical firewalls, authentication servers etc. DDoS attack is one of the attacks to be considered in ad hoc network. A DDoS attack is a attack on the availability of services which deny of service for legitimate node by cooperative manner. The DDoS attack is launched floods of packets on target node through the simultaneous cooperation of a several number of other nodes that are distributed throughout the network [1]. A resource consumption attack is an attack that is designed to unnecessary consumption of the resources of network. The only possible method is to design defence mechanism that will identify the attack and respond to it by dropping the excess traffic. The effect of these attacks varies from temporarily blocking the availability of service to permanently distorting information in the network. DoS attacks can target a server computer or a client computer. For example, an attack may target a system by exhausting limited wireless resources like bandwidth, storage space, battery power, CPU, or system memory. The output of these attacks varies from temporarily blocking of services to permanently removing information in the network. Networks can be attacked by changing route table or tampering its configuration by intruders [2].

2. ATTACKS
Attacks in MANET's can be identified into two categories:

- Active attack
- Passive attack

Active attacks can change data, interrupt network operation, or disable services [3], Active attacks on network routing contain flooding, modifying routing information, providing false route requests and replies, attracting unpredicted traffic, hiding error messages, and fabricating false error messages.

Passive attack fails to assist in providing services like routing and packet forwarding. Passive attacks contain packet dropping to protect resources. These abnormal node behaviors result in performance degradation and origin denial of service attacks, longer delays, packet losses and low throughput.

The Security Attacks on each layer in MANET can be identified as:-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:

- The first attack scenario targets Energy resources, particularly the power of battery of the service provider(In such these attacks a infected node may be constantly send a fake packet to a node with the purpose of consuming the victim's battery energy and preventing other nodes from communicating with the node.

- The second attacks intended at targeting Storage and Processing resources (these attacks are carried out generally to target memory, storage space, or CPU of the service provider).

- The third attack scenario targets bandwidth, where an attacker placed between multiple Distributed Denial of service (DDoS) attack is an attempt to prevent or degrade availability of resources. For this multiple source hosts at the same time to send attack traffic. Seeing as Denial of Service 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 (DDoS) attack is attack, which poses a massive threat to the availability of a resource or service. These attacks are sometimes known as "flooding" attacks.

3. BACKGROUND

There are many security issues for MANET's [4] defined on the basis of service layers such as application layer, transport layer, network layer, etc. At the network layer, an intruder take participate in the routing process and affect the routing protocol to disrupt the working of the network. A variety of security threats is imposed in this layer.

The Network layer vulnerabilities for MANET's fall into following two categories:

- Routing attacks and
- Packet forwarding attacks

The security approach requires an accurate detection of denial of service attacks (more specifically DDoS) specific to the dynamic (ad-hoc) networks environment [5]. Service availability must guarantee that all resources of the communications network are always utilizable by authorized parties. DoS attacks were detected through collaborative monitoring and information exchange. Reputation rating was carried out using neighborhood and cluster level information with more weight given to a node's own observation. There is lacking of generalized approach which works efficiently against several attacks such as wormhole, rushing attack etc. 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 wherein selfish nodes are encouraged to cooperate. In this system, a node reports to the Credit Clearance Service, the messages that it has received or forwarded by uploading its receipts. Center nodes earn credit when they forward message of others node. In addition to the availability of central authority, sprite assumes a public key infrastructure and source routing.

4. RELATED WORK

This section presents some recently proposed mechanisms for detection of attacks which can be classified into trade-based and trust-based mechanisms. Trade-based mechanisms consider market models for providing virtual currency incentives for motivating cooperation among nodes. In the trust-based models, trust is created and the node verified by trust values. Each scheme can be adapted in different routing scenarios. The trade-based models are not applicable in cooperative networks. 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 tamper- resistant hardware but instead uses credit-clearance services in a wireless overlay network.

In [10], a reputation-based model that investigates the effect of misbehavior on network performance was presented. It uses a watchdog for identifying misbehaving nodes and a path rater 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] presented the major 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 elimination technique that used digital signatures to verify legitimate data, and drop packets that do not pass the verification.

Ping Yi et al [17] have presented a new DOS attack and its defence approach 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.Gupta et al [18] have analyzed the Denial of Service Attacks at the MAC Layer in Wireless Ad Hoc Networks and focused on the properties of the popular medium access control (MAC) protocol, the IEEE 802.11x MAC protocol, which enable such attacks.

5. PROPOSED MECHANISM

Mobile ad-hoc network has several loop-false due to infrastructure-less environment. These loop-false makes opportunity for attackers to influence smoothness of network operations. Attacker or unauthorized person can put different attacks by identifying loop-false in the network which is violating security policies of network. One of them is Distributed Denial of service (DDoS) attack to infer availability policy of security. Additionally attacks influence different network resources also those are precious for running network process such as Battery Power, Throughput and End to End delay. Distributed Denial of Service (DDoS) attacks can apply individual layer of networks like Media Access Control (MAC) and Network layer in different forms. At the MAC layer the following DDOS attacks can be attempted:

a) Seeing as we assume that there is a single channel that is reused, keeping the channel busy in the vicinity of a node leads to a DoS attack at that node.

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

Distributed Denial of Service (DDoS) attacks at the routing layer could consist of the following:

a) The malicious or infected node participates in a route but normally drops a several number of the data packets. This results the quality of the connections to deteriorate and further effect on the performance if TCP which is the transport layer protocol is used.

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

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

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

Several mechanism and protocol advised on detection of DDoS attack but their also required some work. To provides a solution for identified problem, a mechanism is proposed to prevent data packet loss occurs during the determining the value of TTL value of nodes and detection of malicious attack in the network. The mechanism proposed which use additional packet named as TTL (time-to-live) before of data packet to determine the value of TTL of nodes. The TTL value of node is decremented by malicious one. Each node has route table which contain path for every node. Node check the value of TTL of nodes if it is abnormal then node declared as malicious or compromised by DDoS.

A. Algorithm

Algorithm TTL_Mechanism(node,n)

{

// Initialize TTL value of nodes by network

Set TTL_v:=0;

For i :=1 to n step i:=i+1 do

node[i]:= TTL_v;

//node send RREQ packet to discover route

Send (node[i], node[j], RREQ);

// node receive RREP packet from each neighboring node

node[i]:=Receive(node[j], RREP);

//node check TTL value of each node

If (nod[i] ==TTLv>=0)

Send (node[i], node[j], DATA);

Else

Declared (node[i+1], Malicious Node);

End if

Exit

//end for loop

6. CONCLUSION

The evolution in intruder tools is a long- standing fashion and it will continue. And, DoS attacks by their very nature are complex to defend against and will continue to be an effective type of attack. Distributed Denial of Service attack is protocol compliant and yet has a devastating impact on the throughput of closed-loop flows, like TCP flows and congestion-controlled UDP flows. To investigates the issue of distributed denial of service by means of the proposed mechanism. Proposed mechanism offers detection and control of DDOS attacks over reputation and score based MANET. Mechanism save network resources and enhance network performance.

7. 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 ", IEEE Wireless Communications-2008, pp. 38 – 47.

[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), 2003.

[7] M. Baker, E. Fratkin, D. Guitierrez, T. Li, Y. Liu and V. Vijayaraghavan, "Participation incentives for ad hoc networks", (2001).

[8] D. Barreto, Y. Liu, J. Pan and F. Wang, "Reputation-based participation enforcement for adhoc networks", (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 Nodes — 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] ShabanaMehfuz, 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).

[18] Denial of Service Attacks at the MAC Layer in Wireless Ad Hoc Networks, National Science Foundation under Grant No. 9985195, DARPA award N660001-00-18936 Riverside CA, Vikram Gupta,Srikanth Krishnamurthy and Michalis Faloutsos, MILCOM-Network Security, Anaheim, October 2002.