Detection and Prevention Mechanism for TTL Field Tampering Form of DDoS Attack in MANET's

Deepak Vishwakarma
PG Scholar
CSE Department
IIST, Indore [MP]

Nitin Rathore
Asst. Professor
CSE Department
IIST, Indore [MP]

Anil Khandekar
H.O.D.
CSE Department
IIST, Indore [MP]

Ranjeet Osari
Asst. Professor
CSE Department
IIST, Indore [MP]

ABSTRACT
A mobile ad hoc network (MANET) is a group of nodes or devices without any fixed infrastructure or centralized control. There will be no centralized control (like switch router etc.) or network infrastructure for a MANET to be set up, thus making its deployment very quick and inexpensive. In mobile ad-hoc network, the intermediate nodes or devices play role of router which routed the packets to the terminal node .The nodes ability to changes its location freely ensures a flexible and versatile non-static network topology which is another important function of a mobile ad-hoc network. Some of the ad-hoc applications cover emergency disaster relief, military operations over a battlefield (vulnerable infrastructure), and wilderness expeditions (transient networks), and community networking through health monitoring using medical sensor network (MSN). The security challenges in mobile ad-hoc networks have become a key concern to provide secure and reliable communication. The Attacks on mobile ad-hoc networks minimizes network reliability and performance. The DOS (denial-of-service), Distributed denial-of-service (DDoS) attacks are very quickly growing problem. The variety and multitude of both the attacks and the defence approaches is overwhelming. These attacks affected network resources, denying of service for valid node and degrades performance of network. In this paper, distributed denial of service attacks (DDoS) is presented which are attacked on mobile ad-hoc network and advised approach to detect DDoS attack and provide valid solutions to maximize network performance and resources through comparison of different network parameters.

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 cannot 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 protection mechanism that will identify the attack and respond to it by dropping the excess traffic. 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. ATTACK IN MOBILE AD-HOC NETWORKS
There are two types of attack in MANET active or passive according to the attack means. Active attacks can change data, disrupt network operation, or halt services [3]:

Active attacks on network routing include flooding, tampering in routing information, produces false route requests and replies, attracting unpredicted traffic, hiding and changes error messages, and fabricating false error messages. Passive attack fails to assist in providing services like routing and packet forwarding. Passive attacks include packet dropping to protect resources. These uncharacteristic node behaviors result in performance degradation and cause denial of service attacks, packet losses, longer delays, low throughput and increases battery consumption.

The Security Attacks on every layer in mobile ad-hoc network can be identified as: - DoS attack is characterized by an explicit attempt by attackers to prevent the legitimate use of services. It may also responsible for the degradation and avoidance of legitimate use of network resources. The Mobile ad-hoc networks are vulnerable to Denial of Service 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 the service provider (In such cause these attacks a malicious node may be frequently send a bogus 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 attack scenario intended at targeting memory storage and processing resources (these attacks target

CPU of Service provider, memory, storage space).

The third attack scenario targets bandwidth of the network, where an attacker placed between multiple Distributed Denial of service (DDoS) attack is an attempt to avoid or minimizes availability of resources. For this multiple source hosts at the same time to send attack traffic. Seeing as DoS attack, the attacker uses a single source host to send attack traffic to a victim. A distributed DoS (DDoS) attack includes more than one sources of attack traffic. Distributed denial-of-service attack is a attack, which poses an enormous threat to the availability of a resource or service. These attacks are referred to as "flooding" attacks.

3. RELATED WORK

This part of paper presents a few 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 essential currency incentives for motivating co-operation among nodes. In the trust-based mechanisms, trust is created and the node confirmed 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 the performance of network.

In the trade-model, proposed in [4], every device has a tamper- resistant security module, PKI (public key infrastructure) to ensure authentication, so it is used for account management. There are two billing mechanisms were proposed that charge nodes as a function of number of hops messages have travelled.

An ad-hoc participation economy (APE) that uses a dedicated banker node to manage accounts was proposed in [5]. Unlike the tamper-resistant scheme, the ad-hoc participation economy uses dedicated banker nodes for account management and it also has facilities for converting virtual currency into real monetary units. Improved mechanisms that use a node as a transaction manager are not plausible in dynamic ad-hoc networks since location tracking incurs additional overhead.

A related reputation-based mechanism known as a reputation participatory guarantee (RPG) was proposed [6]. 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 [7]. This model does not use any tamper- resistant hardware but instead uses credit-clearance services in a wireless overlay network.

In [8], a reputation-based model that investigates the effect of misbehavior on network performance was presented. It uses a watchdog mechanism for identifying misbehaving nodes and a path rater for selecting routes that do not select misbehaving nodes.

In [9], CONFIDANT, a reputation-based model that removes misbehaving nodes by propagating bad Reputation through the network was proposed.

In [10], a reputation based mechanism that only propagates positive reputations among the nodes was proposed. Reputation computation mechanism involves the aggregation of three different types of information, based on different levels of services and observations. This method of reputation computation incurs greater overhead than other proposed mechanism. Presented incentive mechanisms for enforcing cooperation can be categorized 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 and integrity attacks, the threat to availability of network has received less attention. Availability is a key requirement for improving the performance of network. Existing studies on Denial of Service attacks concentrate on the analysis of various attack scenarios targeting a particular layer, or propose a probing mechanism to detect misbehaving nodes that target a particular network layer function. While using a probing scheme can help in detecting Denial of Service (DoS) attacks, probing packets may initiate communication overhead in the bigger network. Reputation rating tied with localized probing scheme can alleviate this problem.

Xiapu Luo et al [11] presented the major problem of indentifying pulsing denial of service (PDoS) attacks which send a sequence of attack pulses to reduce TCP (Transmission control protocol) throughput.

Wei-Shen Lai et al [12] have proposed a mechanism to monitor the pattern of traffic in order to alleviate distributed denial of service attacks (DDoS).

Xiaoxin Wu et al [13] have proposed a Denial of Service (DoS) elimination technique that used digital signatures (DS) to verify legitimate data and drop packets that do not pass the authentication.

Ping Yi et al [14] have presented a new DOS attack and its defence approach in ad-hoc networks. The new denial of service (DOS) attack, called Ad-hoc Flooding Attack (AHFA), can result in denial of service (DoS) when used against ad-hoc on demand routing protocol for mobile ad-hoc networks [15].

V.Gupta et al [16] have analyzed the Denial of Service (DoS) Attacks at the MAC Layer in Wireless Ad-hoc Networks and concentrate on the properties of the popular medium access control (MAC) protocol, the IEEE 802.11x MAC protocol, which allow such type of attacks.

4. AODV ROUTING PROTOCOL

The ad-hoc on demand distance vector (AODV) [17] is a distance vector routing algorithm. However it is a reactive protocol i.e. it requests the route when needed. It does not need nodes that maintain routes for destinations, which are not actively used in communication. The main features of AODV routing protocol are loop-free routing and immediate

notification is to be sent to the affected nodes on link breakage. The algorithm uses various messages such as route request (RREQ), route reply (RREP), and route error (RERR) to maintain and discover links.

5. PROBLEM DEFINITION

Multi-Hop wireless network has several loop-false due to infrastructure-less environment. These loop-false makes opportunity for attackers to influence the 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 the network. One of them is a DoS attack to infer such Availability, Confidentiality or Authenticity policies. Additionally, attacks influence different network resources also those are precious for running network process. Some of them defined below.

- Battery Power
- Lifetime
- Throughput
- Packets delay
- Routing overhead

Several mechanisms and protocol advised on individual black hole attack, but required to more work on DoS attack on which few work approached by researches. In already existing advised approach, certain problem found. Firstly node sent data packet to determine the value of reliability level of nodes in the network. When nodes play role as malicious then it do not acknowledgement of data packet because these watch data packets only, in this scenario data packet of the sender or it read by malicious node. Secondly, is too difficult to detect node as malicious when its reliability level value zero initially when the network is deployed. Thus we required approach to prevent data packet, and perfect detection of malicious nodes in the network.

6. PROPOSED MECHANISM

Mobile ad-hoc network has several loop-false due to infrastructure-less environment. These loop-false makes opportunity for attackers to influence the 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 the network. One of them is a DDoS attack to infer availability policy of security. Additionally, attacks influence different network resources also those are precious for running network process such as Throughput, Battery Power, Routing overhead and End to End delay. Several mechanism and protocol advised on detection for TTL field form 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 TTL value of nodes and detection of malicious attack in the network. The mechanism proposed which use additional packet named as reliability packet (RL packet) before of data packet to determine the TTL value of nodes. The RL value of node is decremented by malicious one. Each node has route table which contain path for every node. Node check the RL value of nodes, if it is abnormal then node declared as malicious or compromised by DDoS. In this approach at the initial level every node has zero reliability value and transmission start with a packet termed as reliability packet, node who responded properly in specific time slice then increases its reliability and those nodes who does not responded in time slice than decrease their reliability value or it remain zero and if it goes to less than zero or remain zero then announced that it's a malicious node. Reliability approach make service availability and retransmission time.

A. Algorithm

Algorithm RL_Mechanism(node,n)

{ // Initialize RL value of nodes by network

Set RL $_v$:=0;

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

node[i]:= RL $_v$;

//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 RL value of each node

RLv=RLv+1;

If (node[i]==RLv>0)

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

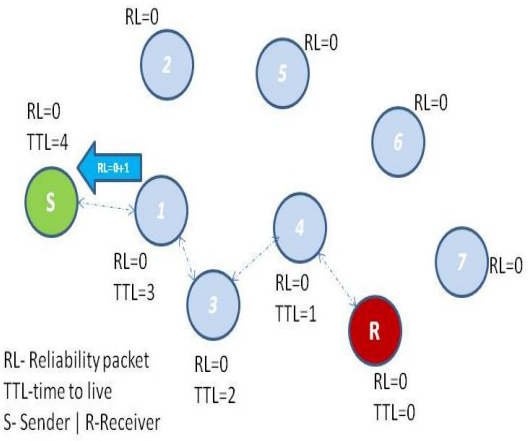
Else

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

End if

Exit

}



Operation

- At node-S: RL=0 and TTL=4. node-S send RREQ to its neighbors.
  if node-S got response from neighbor node then the responded node RL value=0+1 (incremented). if not got response then the neighbor RL value=0-1= -1 (decremented).
- And the process continue until the TTL value will become zero.
- Response include: RREP and RERR.

Figure 1: Communication using RL and TTL Field

7. SIMULATION RESULT AND DISCUSSION

The entire simulations were carried out using ns-2.35 network simulator [18] which is a discrete event driven simulator developed at UC Berkeley as a part of the VINT project. The goal of NS2 is to support research and education in networking or MANET. It is suitable for designing new protocols, comparing different protocols and traffic evaluations.

Simulation Parameters

We get simulator parameter like number of nodes, dimension, routing protocol, traffic, etc. According to below table 4.1 we simulate our network.

Table 4.1 Simulation parameter

Number of nodes	40
Dimension of simulated area	800×600
Simulation time (seconds)	45
Radio range	300m
Traffic type	CBR, 3pkts/s
Packet size (bytes)	512
Routing Protocol	AODV
Connection Type	TCP

Simulation Scenario

There are three scenarios considered and simulated named as normal, DDoS and proposed. To simulate each scenario TCL (Tool Command Language) script is created in which 40 nodes are created with specified range and traffic type. Further components are also defined in script file such as packet size, connection type, antenna type and routing protocol. Proposed approach plays precious role in ad-hoc network security to find groups of anonymous node with minimization of packet drop ratio. Reliability and throughput occurred as a result of the approach. The results of the proposed approach are analyzed on the basis of various network parameters. Result analysis deals with obtaining the results of each scenario which created in this work such as normal, attack, proposed etc. At the end they are compared and analyzed them with each other considering some network parameters such as a packet delivery ratio (PDR), throughput, routing overhead etc.

Result Parameter- The proposed approach result considers following key network parameters with comparison between Proposed (TTL), Normal and DDoS:

1. *Packet Delivery Ratio (PDR)* - Packet delivery ratio calculated by total number of received packet divided by total number of sent packet.

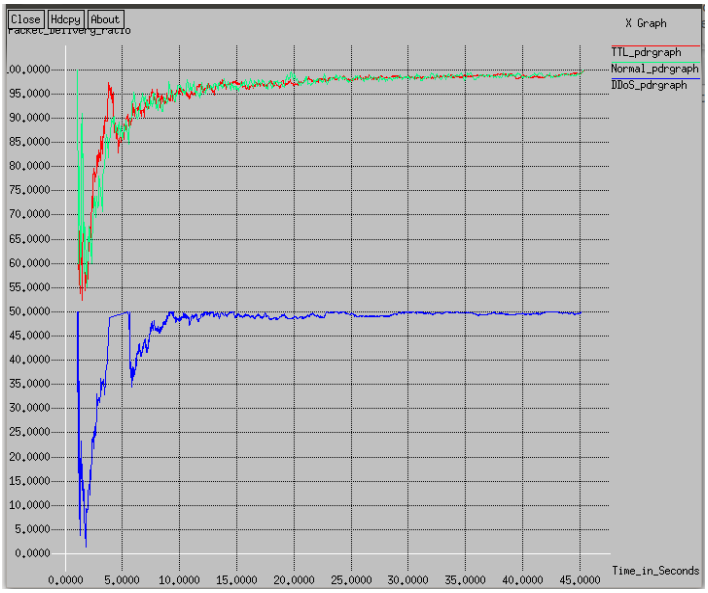


Figure 2: PDR Comparison

2. Throughput- The throughput is determined by the successful received packet at per unit time. It is measured in bits, bytes or packets per seconds.

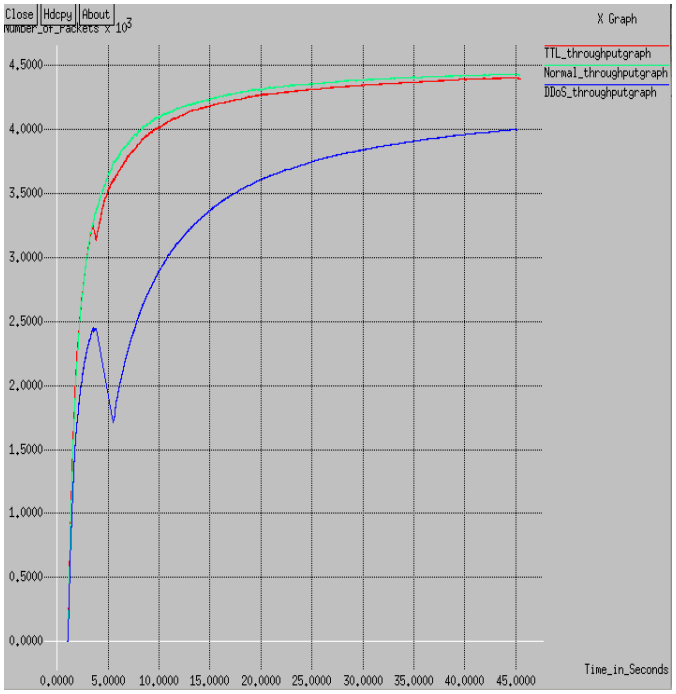


Figure 3: Throughput Comparison

3. Routing Overhead (RO) - Routing overhead is determined by counting the total number of routing packets traversed in the network with respect to time.

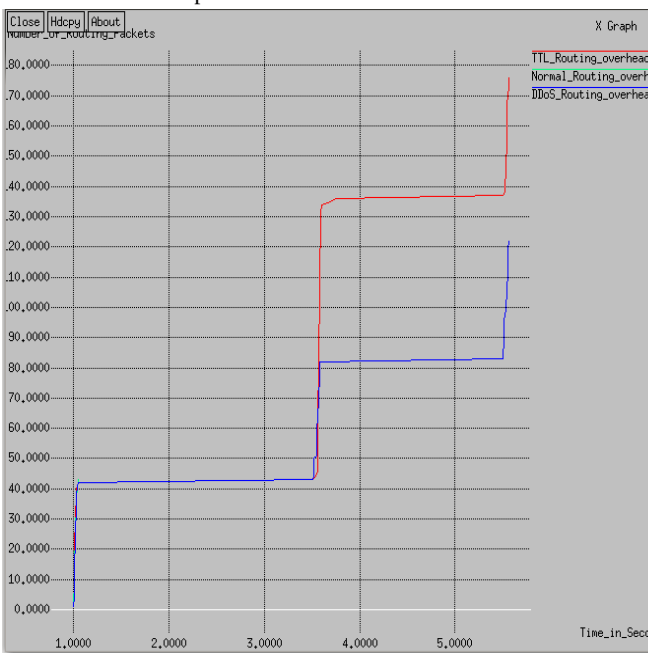


Figure 4: Routing Overhead Comparison

4. End to end packet delay (E2EPD) - It is the difference between the packets received time and packet sent time.

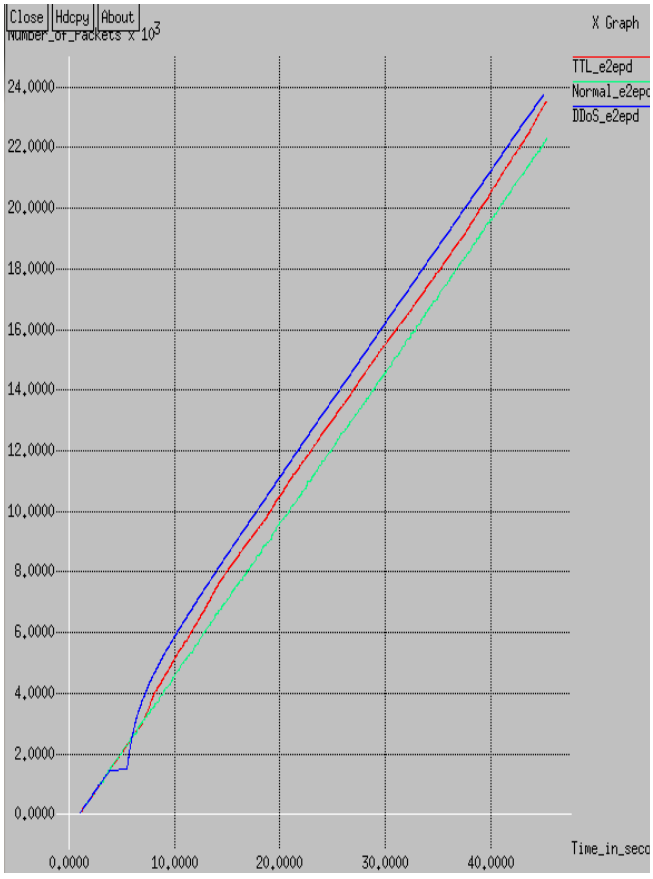


Figure 5: Average End to End Packet Delay Comparison

5. Normalized Routing Load (NRL) - Normalized Routing Load (or Normalized Routing Overhead) is defined as the total number of routing packet transmitted per data packet.

Table 4.1 Simulation Results & Comparison

Parameter	PDR	Throughput	RO	E2EPD	NRL
Normal	93.7	44.28	19.8	221.59	4.7
DDoS	50	39.95	12.2	237.98	23.4
Proposed	90.34	43.98	17.6	234.2	5.3

chart Represation of above table-

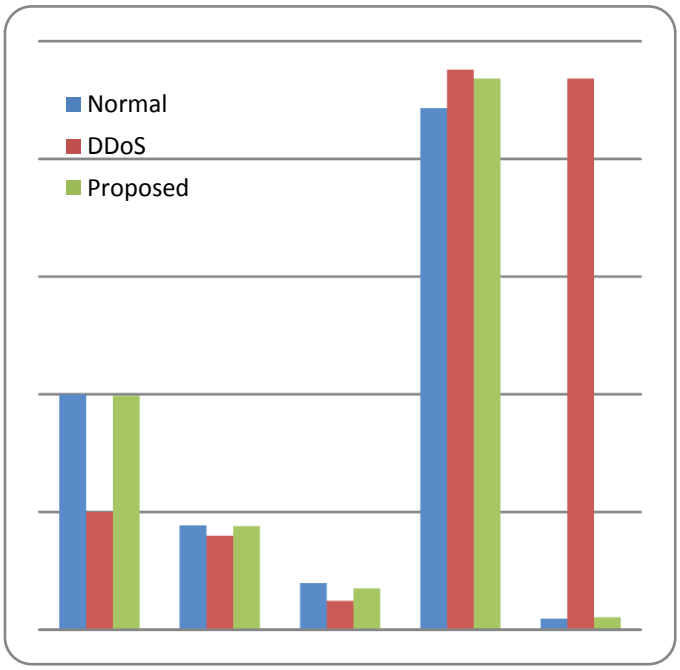


Figure 6: Comparison of Normal, DDoS and Proposed scenarios

8. CONCLUSION

Traditional network needs a fixed infrastructure to establish but mobile ad-hoc network has a different approach. Mobile ad-hoc network does not need fix infrastructure. It provides facility to node that they can join or leave network any time. Ad hoc network is a very broad area for research due to its wide collection of concepts. Security of the network is one of the important features for its deployment. The proposed approach tried to identify the malicious node in the network. Nodes in the networks which interrupt packet transmission and try to capture transmitted information. In this work we have focused on detection of DoS attack. Previous research concentrates on identify a malicious node by calculation there response value if retains count goes to zero then they announce node as the malicious node but there was one problem that initially all nodes have zero value so in this

situation it's very difficult to identify malicious node and it is the basic motivation to define new approach so new approach follow a different way to identify DoS attack by introduced a RL packet send at the beginning of transmission when all nodes have zero RL value. Approach work in the manner by tracking response of nodes means those nodes who respond to sender of packet than increase its RL value by 1 but it also might be possible in case suspicious node that may not respond to sender so if any sender does not get a response from the receiver node than the sender decrement RL value of that node by 1 and when a node reaches less than zero value, it announce as a malicious node. This approach reduces the packet drop ratio and retransmission time.

Future Work

Wireless Ad-Hoc networks are widely used networks due to their flexible infrastructure, i.e. it does not depend upon geographic constraints which make it easily deployable. These networks are exposed to both external and internal attacks as there is not centralized security mechanism. A lot of research work is still needed in this area. By this work, try to detect DOS attack in MANET but still there are many more possibilities to find such malicious node in the network and provide a proper valid mechanism to reduce the possibility of interruptions from those suspicious nodes and feel free to transmit data over the network. It always observed that there is also certain area available in where researchers have to find the impact of the DoS attack in other mobile ad-hoc network routing protocols such as DSR, TORA and GRP along with AODV and OLSR protocols. Other types of attacks like Wormhole, Sybil and Jellyfish attacks are needed to be studied along with the DoS attack. They can be classified on the basis of how much they affect the performance of the network. The detection of this behavior of a DOS attack as well as the elimination strategy for such behavior has to be carried out for further research

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

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

[6] D. Barreto, Y. Liu, J. Pan and F. Wang, "Reputation-based participation enforcement for adhoc networks", 2002.

[7] 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.

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

[9] 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.

[10] P. Michiardi and R. Molva, "Making greed work in mobile ad hoc networks," Technical report , Institut Eur´ecom , 2002.

[11] 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.

[12] 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.

[13] 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.

[14] Security Scheme for Distributed DoS in Mobile Ad Hoc Networks, ACM, Newyork,USA, 2004.

[15] 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.

[16] Vikram Gupta, Srikanth Krishnamurthy and Michalis Faloutsos, 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, MILCOM-Network Security, Anaheim, October 2002.

[17] Perkins, C.; Belding-Royer, E.; Das, S. Adhoc on-Demand Distance Vector (AODV) Routing", July 2003.

[18] Network Simulator- ns-2. http://www.isi.edu/ nsnam /ns/.

[19] Deepak Vishwakarma, D.S.Rao, 'Detection mechanism for distributed denial of service (DDoS) attack in Mobile Ad-hoc networks", Volume-102, September 2014.