VOL. 2, NO. 11, October 2011 ISSN 2079-8407
Journal of Emerging Trends in Computing and Information Sciences

http://www.cisjournal.org

Detection and Control of DDOS Attacks over Reputation and Score Based MANET

Rizwan Khan [1] , A. K. Vatsa [2]
[1]*School of computer Engineering and IT, Shobhit University, Meerut, UP, INDIA.*
{[1] rizwan.khan87@hotmail.com , [2] avimanyou@rediffmail.com}

ABSTRACT

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 defense approaches is overwhelming. These attacks lead toward the degradation or prevention of legitimate use of network resources. There is a need to provide an incentive or credit based mechanism that can provide cooperation among nodes in the network and improve overall network performance and functionality by prevention, detection and control of DOS and DDOS attacks. Therefore, in this paper, we proposed the detection and control mechanism for DDOS attacks over reputation and score based MANET and a clustering technique uses the reputation and score value of nodes.

Keywords: *MANET, DOS, DDOS, Cluster, Attacks, Reputation, Monitor*.

1. INTRODUCTION

The security approach in MANET [10-14] requires an accurate analysis and classification of denial of service attacks (more specifically DDoS) specific to the dynamic (ad-hoc) networks environment. Although mobile ad hoc networks have several advantages over the traditional wired networks, they have associated set of challenges. Firstly, MANETs face challenges in secure communication. For example the resource constraints on nodes in ad hoc networks limit the cryptographic measures that are used for secure messages. Thus it is susceptible to link attacks ranging from passive eavesdropping to active impersonation, message replay and message distortion.

Secondly, mobile nodes without adequate protection are easy to compromise. An attacker can listen, modify and attempt to masquerade all the traffic on the wireless communication channel as one of the legitimate node in the network. Thirdly, static configuration may not beadequate for the dynamically changing topology in terms of security solution. Various attacks like Denial of Service can easily be launched and flood the network with spurious routing messages through a malicious node that gives incorrect updating information by pretending to be a legitimate change of routing information.

Attacks for MANET's [27, 28, 29]. can be identified into two categories either active or passive, according to the attack means [38] [39]. Active attacks can modify data, disrupt network operation, or disable services:

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 behaviors result in performance degradation and cause denial of service attacks, packet losses, longer delays, and low throughput.

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

Ddenial-of-service attack [1,15,16,17] 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 [1] 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

communicating nodes wants to waste the network bandwidth and disrupt connectivity.

Distributed denial of service attack [18,19,20] is an attempt to prevent or degrade availability[Pfl03] 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.

The traditional security technologies such as firewalls [22,23,24] Intrusion Detection Systems (IDSs) [25] and access control lists in routers are unable to defend networks from these attacks. Based on the widely used model, which relies on firewalls and Intrusion Detection Systems (IDS), does not provide the defense required against DoS attacks as long as these devices are an internal part of the victim system. This is because they only respond to an attack, rather than prevent them from being successful, due to following reasons:-

- First, an IDS may not be able to collect all desired information. An IDS may simply be not effective enough to handle all available data, or implementation bugs may make it inclined to crashing.
- The second reason for an IDS being not able to detect all intrusions is the possibility for an evasion or insertion attack against an NIDS.
- The third reason for an IDS being not able to detect all intrusions is the inability to recognize intrusions correctly. This can happen if attack traffic resembles legitimate traffic too much.

Distributed denial-of-service (DDoS) attacks commonly overwhelm their victims by sending a vast amount of legitimate-like packets from multiple attack sites. As a consequence the victim spends its key resources processing the attack packets and cannot attend to its legitimate clients. During very large attacks, The only way to completely eliminate the DDoS threat is to secure all machines on the Internet against misuse, which is unrealistic.

The seriousness of DDoS problem and growing sophistication of attackers have led to development of numerous defense mechanisms [19, 26]. An important requirement for DDoS defenses is to recognize legitimate packets in the flood, separate them from the attack and deliver them safely to the victim. A practical DDoS defense must meet three important goals:

- Accurate attack detection,
- Effective response (dropping or rerouting) to reduce the flood, and
- Precise identification of legitimate traffic and its safe delivery to the victim.

Moreover, as attackers share their attack codes similarly to fight against these attacks, Internet community needs to devise better ways to accumulate details of attack. Only then a comprehensive solution against DDoS attacks can be devised.

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) is a rapidly growing problem. The multitude and variety of both the attacks and the defense approaches is overwhelming. These attacks leads toward the degradation or prevention of legitimate use of network resources. There is a need to provide an incentive or credit based mechanism that can provide cooperation among nodes in the network and improve overall network performance and functionality by prevention, detection and control of DOS and DDOS attacks.

This paper is organized in chapters. In section - 1 we have discussed background of MANET, security issues in MANET, various attack types related to MANET specifically DoS and DDoS attacks, and Problem Identification, subsequently in section 2, we undergoes through literature survey. Section 3, presents Proposed Architecture and mechanism for Detection and control of DDoS attacks & description of the proposed reputation-based incentive scheme (based on the calculation of Node Scorevalue & NodeReputationValue) in MANET. Section 4 mentions about Conclusion of this paper and Section 5 describes further enhancement under heads Future Scope.

2. BACKGROUNDS

The security issues for MANET's [6,7,40] can be analyzed on basis of individual layers[41] 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 [6] for MANET's fall into following two categories:

- Routing attacks and
- Packet forwarding attacks

The security approach in MANET [11,12,13,14] 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.

Sservice 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 disrupts 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 (D)DoS attacks.

A Reputation-based incentive mechanism [31] 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 neighborhood 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 [14] 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 [32]. 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 [42], 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.

3. PROPOSED ARCHITECTURE AND MECHANISM FOR DETECTION, PREVENTION AND CONTROL OF DDOS ATTACKS IN MANET

The proposed architecture and mechanism is mentioned in section 3.1 and 3.2 respectively.

3.1 Architecture of Detection and control of DDoS attacks in MANET

Architecture of Detection, Prevention and control of DDoS attacks in MANET is illustrated by figure -1 : Cluster Formation and Cluster head Selection on basis of Reputation and Node Score and figure – 2 : Custer Head functioning as Reputation management system. The different modules for figure – 1 is as follows:

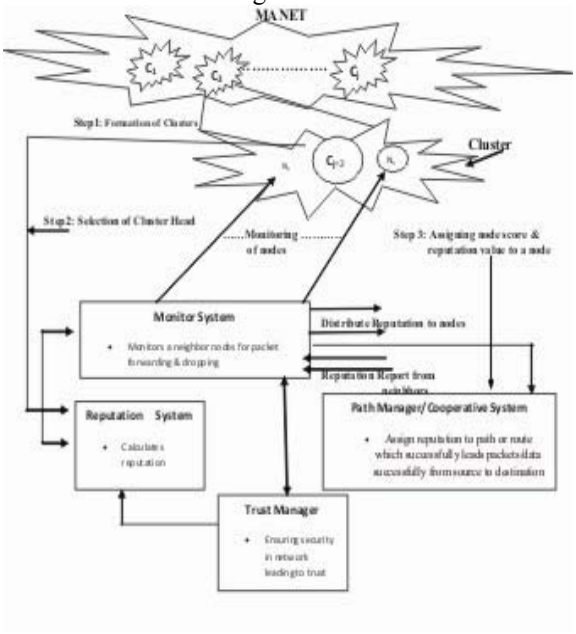

Figure 1: Cluster Formation and Cluster head election on basis of node Reputation and node score value

1) Monitor: The goal of monitoring is to gather first-hand information about the behavior of nodes in the network. Monitoring systems detect misbehavior that can be distinguished from regular behavior by observation. Some of the misbehavior types which are frequently encountered in MANET's are Packet dropping, Modification, Fabrication, Timing misbehavior. The Monitor system that monitors the neighbors of a node under consideration for packet forwarding & routing capability, on evaluation of which thereby leads to the reputation (either co-operative or malicious or selfish node) or credit of a node.

Some critical issue that needs to be taken into consideration by the monitoring systems are:

- Distribution of false reputation reports by malicious neighbors.
- Incorrect monitoring, when packets are dropped due to congestion or collision
- Identify the location of malicious nodes in the network.

2) Reputation System: The module Reputation is mainly responsible for the performance of a node in participating in the base protocol as seen by others. For mobile ad-hoc networking this means Participation in routing and Forwarding capability of a node in the network.

Typically, the functions of reputation management system are: Evaluation, Detection &Reaction. Evaluation functionality of reputation management determines or evaluates the behavior of a node in the network. The evaluation criteria can be based on the Credit_Score (Successful or UnSuccessful) earned by a node, which a quantification of the node's behavior with respect to packet forwarding capability.
The different Credit rating/Score or weight based on the type of behavior detection exhibited by the node which is assumed to follow the order given below:

Using the Detection functionality of Reputation management system on the basis of Net_Credit_Score value calculated using step 2 of Phase I to distinguish between Co-operative & Malicious or Misbehaving node.

The Reaction function or module of reputation system takes action against nodes according to their behavior exhibited in the network. The reaction taken toward nodes identified by the detection function can be as misbehaving can be informative, by notifying other nodes about the misbehaving nodes, and/or disciplinary, by penalizing the misbehaving nodes. On the other hand, the reaction taken toward nodes identified as cooperative can reward cooperation by offering these nodes differentiated levels of service according to their level of cooperation.

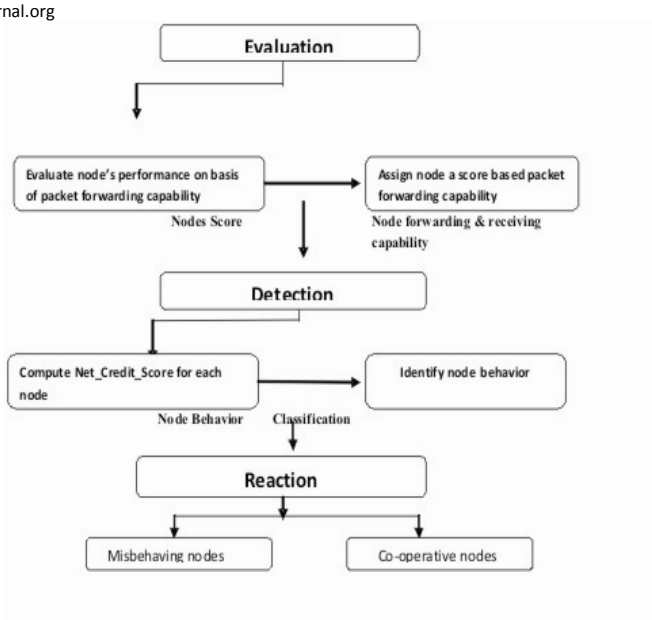

Figure 2: Custer Head functioning as Reputation management system

3) Trust Manager/ Co-operation system: The Trust Manager module in the architecture shown above act as a Co-operation system among the nodes performing the extensive task of Alarm Count and Trust Builder. It keeps track of the incoming and outgoing ALARM messages. ALARM messages are sent by the trust manager of a node to warn others of malicious nodes. As a trust builder it performs the task to differentiate the consequences of packet is lost or drop naturally or whether is it due to likely collision in the network.

4) Path Manager: The Path manager module Assign reputation to path or route which successfully leads packets/data successfully from source to destination.

(Path _rating) $_{\text{evaluated by Cluster Head}}$ > **(Path _rating)** $_{\textit{observed by neighborhood}\ \text{nodes}}$>
(Path _rating) $_{\text{based on information reported}}$
Where
(Path _rating) $_{\text{evaluated by Cluster Head}}$ **:** is the Path rating or score or weight that is assigned to a path by a Cluster Head due to its own experience or monitoring.
(Path _rating)$_{\textit{observed by neighborhood}\ \text{nodes}}$: is the Credit rating/Score or weight that is assigned to a node for observations by the neighbor-hood node in a clusters.
(Path _rating)$_{\text{based on information reported}}$**:**is the Credit rating/Score or weight that is assigned to a node for reported experience.
For a Cluster node the Net_Credit_Score can be calculated using the equation

Net_Path_Score =∑(Path _rating) $_{\text{evaluated by Cluster Head}}$
+ (Path _rating) $_{\text{observed by neighborhood nodes}}$
+ (Path _rating)$_{\text{based on information reported}}$

3.2 Mechanism for Detection and control of DDoS attacks:

Phase-1: Reputation and Score Based Cluster Creation And Cluster Head Selection:

Step 1: Formation of Clusters:

The Cluster Head **(**Cluster_Head**)**$_{i=id}$ of **i**thCluster is given by the pseudo code:-
Node id is assigned as
$\mathbf{N_{id}}$ = Random_generator();
Divide Mobile Nodes in Clusters
Assign each Cluster to Unique Cluster id "$\mathbf{(Cluster)_{id}}$".
The Cluster Head **(**Cluster_Head**)**$_{i=id}$ of **i**thCluster is given by the pseudo code:-
If ($\mathbf{N_i}$<**NodeRange&& Ni** !=$\mathbf{C_k}$) // where $\mathbf{C_k}$ = Set of Clusters in the Network
[$\mathbf{C_i}$] ← ($\mathbf{N_i}$) // **Ni =** is assigned to Cluster$\mathbf{C_i}$
}

Load Balancing of Cluster Head is at most priority since its energy depletes much faster due higher number of communications made

Balance_Cluster_Load()
{
If(Nodes_in_Cluster<=
Cluster_Energy_Dissipation($\mathbf{(Cluster)_{id}}$))
/* where Cluster_Energy_Dissipation is defined/Calculated in terms of Computational overhead of Cluster Head*/
// Cluster_Head_Energy>= ThresholdEnergrgy

{
Allow the node to join cluster
}
else
{
Form new Cluster
Cluster_Formation();
}
}

Step 2: Assignment of parameters NodeScore& Reputation to a node in network

NodeScoreValue( )
{
for(i=1 ; j<=TotNodes; i++)
{
// for each of the total nodes in the network
for(j=1 ; j= allNodeofCluster ; j++)
{
//for each node belonging to a cluster C_i
A = AVG (Energy_level)
// assign to A average value of Node_Energy
B = AVG (NodesNo._in a_Cluster)
// assign to B the average Number of Nodes Under the Cluster Head
}
for (i=0; i<= Setof_CH_node ; i++)
{
If (N_i belongs to NC)
//current node can be attached to Cluster set NC
X = MAX ($(Energy\_level)_i$ from Setof_CH_node)
// Cluster Head with the maximum work budget left i.e. the maximum battery life left
Y = MIN (NN_i from Setof_CH_node)
// ClusterHead with the least number of nodes under it
M = MOD (AVG (Energy_level) - X)
// M1 is the set of ClusterHead node with Maximum life in terms remaining battery life
N = MOD (AVG (NodesNo._in a_CH) - Y)
// M2 is the set of ClusterHead node with Minimum nodes attached to It in its cluster region

Node Score (S) = Max (M*N) /*Since Cluster having large residual energy would have less no. of nodes attached to it and vice a versa*/
return (S); // S is Node score of node of Cluster C_i
}

Node_Reputation ( )
{
For each node Ni belonging to Cluster $\mathbf{C_i}$contains an entry of ordered pair {Node_id, Scredit and Ucredit } where
Node_id= Node id in the cluster
Scredit = is score corresponding to correctly Packet forwarding capability of a node
Ucredit = is score corresponding to Un-correct Packet forwarding capability of a node
Successful_Credit_Score i.e. Scredit(A,B) = 1 , if node A gets service from node B

Similarly
UnSuccessful_Credit_Score i.e. Ucredit(A,B) = - 1, if the service was not successful or denied then a node A may rate the service provided by a node B as negative

Also at each respective node maintains a Net_Credit_Score which signifies its reputation and is Calculated as

Net_Credit_Score = $\sum$ Scredit(i,j) + $\sum$ Ucredit(i,j)
Where node "i" is requesting some service from node "j"
If (Net_Credit_Score>=0)
{
Node has positive reputation, Co-operative
}
else
{

Node is considered to be Non-Co-operative or malicious node

}

return (Net_Credit_Score);

}

Step 3:Selection of Cluster Head based on (Optimum NodeScore&RepuataionValue for a node)

ClusterHeadSelection ( )

{

Assume the following parameters as follows.

Score = NodeScoreValue ();

Reputation = NodeReputation ();

Smax= Scoremax( ); //Assign max. value of Score to the variable Smax

Rmax = Reputationmax( ); //Assign max. value of Reputation to the variable Rmax

For each cluster belonging to MANET

{

For (each node Ni && Ni = 1 to Ni = n)

{

If(Smax || Rmax)

{

Set Node Ni = (ClusterHead)j,

}

else

{

Add node to jth Cluster i.e. Cj

Cj← Ni

}

}

}

}

Scoremax(score of all Nodes in any cluster Cj)

{

- Store the NodeScoreValue for a respective node in an array
- Sort the array to arrange the NodeScoreValue either in an ascending or descending order.
- Return the Score value Smax for Node Id Ni

}

Reputationmax( )

{

- Store the Node Reputation for a respective node in an array
- Sort the array to arrange the Node Reputation either in an ascending or descending order.
- Return node Reputation value Rmax. for Node Id Ni

}

Phase-II: DDOS classification of Attacks and their Detection

The classification of DDoS attacks on a MANET can be broadly classified into following two categories of attacks.

- Connection Depletion attacks.
- Bandwidth Depletion attacks.

Attack_Connection_Depletion

{

- Attacks leading to degraded performance could be due to resource consumption.
- SYN flooding attacks, UDP connection attacks are such kind of attacks.
- Attacks Happened due to Increased CPU utilization and failure of the host to serve other users

}

Detection_of_ Connection_Depletion_Attack

{

- Use sniffers or logging at the router to determine the extent of the attack.
  a) to determine the direction of attack
  b) to identify the pattern or signature of the attack such as
  - Traffic anomalies observed from the set of distributed detection system,
  - Spoofed source IP addresses (DoS attacks to hide the location of an attacker is IP spoofing which means sending packets with a false source IP address.)

In some experience with organizations installing commercial network Intruder Detection System, mis-configured attack signature, provided wrong alert indicators. A sniffer at this point helps to identify the realthreat.

}

In Bandwidth depletion attack an attacker bombards a victim with a high volume of traffic, consuming all the communication bandwidth of the links incident to the victim node, thereby denying the legitimate user's need for bandwidth.

Bandwidth_Depletion_attacks

{

- Networks of compromised machines that are remotely controlled by an attacker called "Botnets".
- Botnets are regularly used for DDoS attacks since their combined bandwidth overwhelms the available bandwidth of most target systems.

}

Detection_of_Bandwidth_Depletion_attacks
{
Tracking Bandwidth Depletion attacks detection such as botnets is clearly a multistep operation consisting following operations:

a) Collecting Malware with Honeypots.

- A honeypot is a resource network (computer, routers, switches etc)deployed to be probed, attacked, and compromised. A honeynet is a network of honeypots.

b) Collecting Malware with Mwcollect

- The drawbacks with botnets was that A honeypot will crash regularly if the bot fails to exploit the offered service, e.g. due to a wrong offset within the exploit.
- Thus an alternative as Mwcollect (a program called mwcollect to capture malware in non-native environments.) for collecting malware.
- In contrast to honeyd(a low-interaction honeypot) it is tailored to collecting of malware and offers better packet handling and more flexibility.

}

Both these categories of attacks can be result of inappropriate functioning of the Network layer of MANET and can be associated with the operational functionality of this layer namely as: routing and packet forwarding operation.

So the Network layer vulnerabilities fall into two categories: routing attacks(specifically those are oppose the routing policies of network) and packet forwarding attacks. Some of the anti-routing based attacks that are considered in our work are:

- Cache Poisoning
- Message Bombing

The consequences of this attack are

a) Degradation in network communications,
b) Unreachable nodes,
c) Routing loops existence.

CachePoisoningAttacks()
{

- In these attacks the attackers take advantage of the promiscuous mode of routing table updating.
- In this scenario a node overhearing any packet may add the routing information contained in that packet header to its own route cache, even if that node is not on the path.
- Suppose a malicious node M wants to poison routes to node X. M could broadcast spoofed packets with source route to X via M itself; thus, neighboring nodes that over hear the packet may add the route to their route caches.

}

MessagebombingAttacks( )
{

- Message bombing is essentially a Incorrect traffic generation attack.
- This category includes attacks which consist in sending false control messages: i.e. control messages sent on behalf of another node (identity- spoofing), or control messages which contain incorrect or outdated routing information.

}

Phase-III: DDoS Control packet Request

The Control frame format depicted in the figure - 3. It consists of different fields which will be used by the various modules (like Monitor , Reputation, Path manager, Trust Manager) discussed in Phase I, to set up reputation of the a node in the network. Consider the situation of management and control frames are not protected, adversaries could exploit this fact to launch (D)DoS attacks on cluster based ad-hoc networks. The most efficient exploit is to flood the surroundings with huge amounts of deauthentication or disassociation frames.

There are three frame types in a cluster based ad-hoc networks: management frames, control frames, and data frames. Where Management frames responsible for network management and admission control, Control frames control access privileges and data frames will carry data.

Each frame type in the control frame request provides certain definite functionality which are listed below:

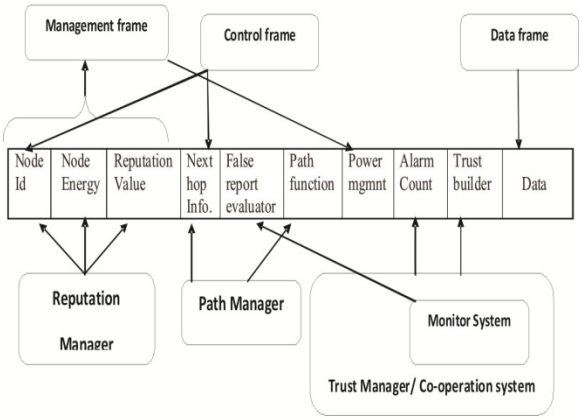

Figure 3: Control Packet format to Control DDoS attack on Reputation and score based MANET

Where :

Node Id: Node Id is unique id of the node.

Node Energy: Node Energy is the level of energy, which is required by a node to maintain itself as an active part of the network ensuring its proper functioning.

Reputation Value: Reputation of node is the measure of co-operative behavior exhibited by a node in the network based on measurable parameters of a node in the network such as Participation in routing and Forwarding capability.

Next hop Information: This field contains the next hop information of a node that is defined in terms of likely route from source to destination and is captured during the route discovery process & is contained within both the Reputation Manager(Cluster Head) & The Path Manager.

False report Evaluator: This field is taken into account due to one of the limitation associate with the reputation based mechanism that there are possibilities of collision leading to natural dropping of packets although in reality there may be no selfish node existing in the network.

Path function: This function returns the path or route which successfully leads packets/data successfully from source to destination by considering those nodes which are optimum requirement of node energy & reputation value.

Alarm Count: This field is essentially acts as a counter for incoming and outgoing ALARM messages. Outgoing ALARMS are generated by the node itself after having experienced, ob-served, or received a report of malicious behavior.

Trust Builder: In order to differentiate consequences of packet is lost or drop naturally or whether is it due to likely collision in the network. A trust builder by taking into account this reason assures trust to prevail among the nodes by identifying real reasons of lost of packets.

4. 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. In this paper, we 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. Here we have used clustering technique that uses the reputation and score value of nodes to elect a cluster head and when a Cluster-Head is subjected to DDoS attack this would have manifolds consequences as the Cluster Heads form a virtual backbone and may be used to maintain routing states information & route packets to nodes in their cluster.

The architecture worked in three phases namely as Phase I: Reputation and Score Based Cluster Creation And Cluster Head Selection, Phase II: presents mentioning of some of DDoS attacks like message bombing and cache poisoning, their detection strategies and Phase III: presents a control frame packet format which can be used as a line of defense mechanism to control and mitigate from DDoS attacks over a Reputation and score based MANET.

5. FUTURE SCOPE

The proposed algorithms are efficient and effective in comparison to existing one as per literature review but more efficient algorithm may be designed by further improvement in proposed mechanisms by considering the critical issues which we have not taken in this work such as mobility issues, as we have assumed the cluster heads to be stationary and only the nodes of cluster able to move freely so therefore compensating on one critical characteristic of node (which can even be a Cluster Head) of MANET ,similarly scalability can be key issue as we have used an algorithm to balance the workload on a cluster head without any consideration of increase in the size of MANET resulting in degraded QoS parameters, and performance for the network.

REFERENCES

[1]. Mieso K. Denko , "Detection and Prevention of Denial of Service (DoS) Attacks in Mobile AdHoc Networks using Reputation - Based Incentive Scheme".

[2] Charles P. Pfleeger and Shari Lawrence Pfleeger, Security in Computing, Third Edition, Prentice Hall PTR, Saddle River, New Jersey,03..

[3] Muftic , S ., Patel, A., Sanders, P., Colon, R., Heijnsdijk, J. & Pulkkinen, U., Security Architecture in Open Distributed Systems, John Wiley & Sons, Bath, UK, 1993.

[4] Dietrich, S., Long, N. & Dittrich, D., "Analyzing Distributed Denial of Service Tools: The Shaft Case, " 14 th Systems Administration Conference (LISA 2000) , New Orleans , Louisiana, 2000.

[5] Power , R., " 2001 CSI/FBI Computer Crime and Security Survey ", Computer Security Institute/Federal Bureau of Investigation Technical Report, vol. 7, no. 1, Spring 2001.

[6] 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.

[7] L. Zhou , Z. J. Haas, Cornell Univ., " Securing adhoc networks, " IEEE Network, Nov/Dec 1999, Volume: 13, Page(s): 24-30, ISSN: 0890-8044

[8] H. Yang, H. Luo, F. Ye, S. Lu, L. Zhang, "Security in mobile ad hoc networks : challenges and solutions," In proc. IEEE Wireless Communication, UCLA , Los Angeles, CA , USA; volume- 11, Page(s):38- 47, ISSN: 1536-1284

[9] P. Michiardi, R. Molva, " Ad hoc networks security, IEEE Press Wiley, New York, 2003.

[10] Ali Ghaffari. "Vulnerability and Security of Mobile Ad hoc Networks", Proceedings of the 6th WSEAS International Conference on Simulation, Modelling and Optimization, Lisbon, Portugal, September 22-24, 2006

[11] Karan Singh, R. S. Yadav , Ranvijay , "A REVIEW PAPER ON AD - HOC NETWORK SECURITY", International Journal of Computer Science and Security, Volume (1): Issue (1)

[12] Levente Butty, Jean-Pierre Hubaux,. "Report on a Working Session on Security in Wireless Ad Hoc Networks", Mobile Computing and Communications Review, Volume 6, Number 4

[13] Pin Nie, "Security in Ad hoc Network",2006.

[14] Kamanshis Biswas and Md. Liakat Ali; "Security Threats in Mobile Ad Hoc Network "; Master Thesis; Thesis no: MCS-2007:07; March 22, 2007.

[15] http://www.merl.com/projects/DenialServiceAttack

[16] M.K. Denko, "A Localized Architecture for Detecting Denial of Service (DoS) Attacks in Wireless Ad Hoc Networks", In Proc. IFIP INTELLCOMM'05, Montreal,Canada,

[17] Carl G., Kesidis G., Brooks R., and Rai S., "Denial of Service Attack Detection Techniques," Computer Journal of IEEE Internet Computing, vol. 10, no. 1, pp. 82-89, 06.

[18] Stephen M. Specht and Ruby B. Lee; Distributed Denial of Service: Taxonomies of Attacks, Tools, and Countermeasures ; Proceedings of the 17th International Conference on Parallel and Distributed Computing Systems, 2004 International Workshop on Security in Parallel and Distributed Systems, pp. 543-550; September 2004.

[19] J. Mirkovic and P. Reiher; A Taxonomy of DDoS Attack and DDoS Defense Mechanisms; ACM Sigcomm Computer Communications Review; Vol. 34, No. 2, Apr. 2004.

[20] Gurjinder Kaur, Yogesh Chaba, V. K. Jain; Distributed Denial of Service Attacks in Mobile Adhoc Networks,2011 World Academy of Science, Engineering and Technology 73 2011.

[21] Chang C., "Defending Against Flooding-Based Distributed Denial of Service Attacks : A Tutorial," Computer Journal of IEEE Communication Magazine, vol. 40, no. 10, pp.42-51, 2002.

[22] Cheswick R. and Bellovin M., Firewalls and Internet Security: Repelling the Wily Hacker, Addison Wesley, 1994.

[23] McAfee, "Personal Firewall,"http:// www.mcafee.com, 2003.

[24] Moore D., Voelker G., and Savage S., "Inferring Internet Denial of Service Activity," in Proceedings of the 10th USENIX Security Symposium, pp. 20-25, Washington, 2001.

[25] Bai Y. and Kobayash H., "Intrusion Detection Systems: Technology and Development," in Proceedings of the 17th International Conference on Advanced Information Networking and Applications, USA, pp. 710-715, 2003.

[26] Chen R. , Park J., and Marchany R., " A Divide and Conquer Strategy for Thwarting Distributed Denial of Service Attacks," Computer Journal of IEEE Transactions on Parallel and Distributed Systems, vol. 18, no. 5, pp. 577-588,07

[27] Abhay Kumar Rai, Rajiv Ranjan Tewari & Saurabh Kant Upadhyay, "Different Types of Attacks on Integrated MANET-Internet Communication", International Journal of Computer Science and Security (IJCSS) Volume (4): Issue (3) 2010.

[28] Hoang Lan Nguyen, Uyen Trang Nguyen. "A study of different types of attacks on multicast in mobile ad hoc networks". Ad Hoc Networks, Volume 6, Issue 1, Pages 32-46, January 2008.

[29] Bin Xie and Anup Kumar. "A Framework for Internet and Ad hoc Network Security". IEEE Symposium on Computers and Communications (ISCC-2004), June 2004.

[30] L. Zhou and Z. J. Haas. "Securing Ad Hoc Networks". IEEE Network Magazine, Volume. 13, no. 6, Pages 24-30, December 1999.

[31] Mieso K. Denko , "Detection and Prevention of Denial of Service (DoS) Attacks in Mobile Ad Hoc Networks using Reputation-Based Incentive Scheme".

[32] Huang Zun -guo, Hu Hua -ping and Gong Zheng-hu Hu Guang -ming, " SLID: A secure Lowest-ID clustering algorithm," Wuhan University Journal of Natural Sciences, vol. 10, no.1, pp. 39-42, January 2005.

[33] Wikipedia; http://en.wikipedia.org/wiki/Wireless_ad_hoc_network

[34] E. M. Royer and C.K. Toh, "A Review of Current routing Protocols for Ad-Hoc MobileWireless Networks," IEEE Personal Communications Magazine, pp. 46–55, April 1999.

[35] C. E. Perkins, Ad Hoc Networking.: Addison--Wesley, 2001.

[36] R. Ramanathan and J. Redi, " A Brief overview of Ad Hoc Networks: Challenge and Directions," IEEE Communication Magazine, vol.40, no. 5, 2002.

[37] Srikanth Krishnamurthy Prasant Mohapatra, Springer Science+Business Media, 2005.

[38] S. Yi and R. Kravets, Composite Key Management for Ad Hoc Networks .Proc. of the 1st Annual International Conference on Mobile and Ubiquitous Systems: Networking and Services (MobiQuitous'04), pp. 52-61, 2004. [39] R. Oppliger, Internet and Intranet Security, Artech House, 1998.

[40] Nishu Garg , R.P.Mahapatra ,"MANET Security Issues", IJCSNS International Journal of Computer Science and Network Security, VOL.9 No.8, August 2009.

[41] Bing Wu, Jianmin Chen, Jie Wu, Mihaela Cardei, "A Survey on Attacks and Counter-measures in Mobile Ad Hoc Networks"

[42] S. Zhong, J. Chen, and Y. Yang, (2003) "Sprite: a simple, cheat-proof, credit based system for mobile ad-hoc networks," IEEE INFOCOM, San Francisco, CA, USA, Vol 3

AUTHOR PROFILE

Rizwan Khan is pursuing M. Tech. from Shobhit University Meerut in 2009-2011. He has worked as software engineer in software industry & currently is a Lecturer in ABIMS, Aligarh (UP). He has been in teaching for a period extending over 2 years. His area of interest includes MANET (Mobile Ad-Hoc network).

Avimanyou Kumar Vatsa is working as Assistant Professor in the School of Computer Engineering and Information Techno-logy at Shobhit University, Meerut (U.P.). He obtained his M-Tech (Computer Engineering) with Hons. from Shobhit University and B-Tech (I.T.) from V.B.S Purvanchal University, Jaunpur (U.P.). He has worked as software engineer in software industry. He has been in teaching from more than one decade. During this short period of time, he has supervised more than 25 dissertations of M.Tech students. He is on the editorial board of few international journals in network and security area. He has been member of several academic and administrative bodies. During his teaching he has coordinated several Technical fests and National Conferences at Institute and University Level. He has attended several seminars, workshops and conferences at various levels. His many papers are published in various national and international journals and conferences. His area of research includes MANET (Mobile Ad-Hoc network), Network Security, Congestion Control and VOIP-SIP (Voice over IP).