REAN (ROBUST EFFICIENT ADAPTIVE NETWORK) FOR MANETS: FEASIBILITY AND ANALYSIS

Prachi Garg*

Shruti Garg*

ABSTRACT

A mobile ad hoc network (MANET) is a spontaneous network that can be established with no fixed infrastructure. This means that all its nodes behave as routers and take part in its discovery and maintenance of routes to other nodes in the network i.e. nodes within each other's radio range communicate directly via wireless links, while those that are further apart use other nodes as relays. Ad hoc networks have a wide array of military and commercial applications. They are ideal in situations where installing an infrastructure network is not possible or when the purpose of the network is too transient or even for the reason that the previous infrastructure network was destroyed. Security issues are the critical part in such type of networks. DDoS attack is the one of them in MANET. The proposed solution reduces the effect of DDoS attack and the designed network is robust and efficient enough to resolve all the problems related to DDoS. Detection and Prevention of DDoS are two main issues to be tackled.

Keywords *– MANET, DDoS.*

*Assistant Professor Dept of Computer Science, Geeta Institute of Technology & Management, Kanipla

I. INTRODUCTION

In view of the increasing demand for wireless information and data services, providing faster and reliable mobile access is becoming an important concern. Nowadays, not only mobile phones, but also laptops and PDAs are used by people in their professional and private lives. These devices are used separately for the most part that is their applications do not interact. Sometimes, however, a group of mobile devices form a spontaneous, temporary network as they approach each other. This allows e.g. participants at a meeting to share documents, presentations and other useful information. This kind of spontaneous, temporary network referred to as mobile ad hoc networks (MANETs) sometimes just called ad hoc networks or multi-hop wireless networks, and are expected to play an important role in our daily lives in near future.

A mobile ad hoc network (MANET) is a spontaneous network that can be established with no fixed infrastructure. This means that all its nodes behave as routers and take part in its discovery and maintenance of routes to other nodes in the network i.e. nodes within each other's radio range communicate directly via wireless links, while those that are further apart use other nodes as relays. Its routing protocol has to be able to cope with the new challenges that a MANET creates such as nodes mobility, security maintenance, quality of service, limited bandwidth and limited power supply. These challenges set new demands on MANET routing protocols.

Ad hoc networks have a wide array of military and commercial applications. They are ideal in situations where installing an infrastructure network is not possible or when the purpose of the network is too transient or even for the reason that the previous infrastructure network was destroyed.

Security in mobile ad hoc networks is a hard to achieve due to dynamically changing and fully decentralized topology as well as the vulnerabilities and limitations of wireless data transmissions. Existing solutions that are applied in wired networks can be used to obtain a certain level of security. Nonetheless, these solutions are not always being suitable to wireless networks. Therefore ad hoc networks have their own vulnerabilities that cannot be always tackled by these wired network security solutions.

One of the very distinct characteristics of MANETs is that all participating nodes have to be involved in the routing process. Traditional routing protocols designed for infrastructure networks cannot be applied in ad hoc networks, thus ad hoc routing protocols were designed to satisfy the needs of infrastructure less networks. Due to the different characteristics of

wired and wireless media the task of providing seamless environments for wired and wireless networks is very complicated. One of the major factors is that the wireless medium is inherently less secure than their wired counterpart. Most traditional applications do not provide user level security schemes based on the fact that physical network wiring provides some level of security. The routing protocol sets the upper limit to security in any packet network. If routing can be misdirected, the entire network can be paralyzed. This problem is enlarged in ad hoc networks since routing usually needs to rely on the trustworthiness of all nodes that are participating in the routing process. An additional difficulty is that it is hard to distinguish compromised nodes from nodes that are suffering from broken links.

Recent wireless research indicates that the wireless MANET presents a larger security problem than conventional wired and wireless networks[3]. Distributed Denial of Service (DDoS) attacks has also become a problem for users of computer systems connected to the Internet. A DDoS attack is a distributed, large-scale attempt by malicious users to flood the victim network with an enormous number of packets. This exhausts the victim network of resources such as bandwidth, computing power, etc. The victim is unable to provide services to its legitimate clients and network performance is greatly deteriorated.

II. DISTRIBUTED DENIAL OF SERVICE (DDOS) ATTACK

DoS Attack

A denial of service (DoS) attack is characterized by an explicit attempt by an attacker to prevent legitimate users of a service from using the desired resources [6]. Examples of denial of service attacks include:

- attempts to “flood” a network, thereby preventing legitimate network traffic
- attempts to disrupt connections between two machines, thereby preventing access to a service
- attempts to prevent a particular individual from accessing a service
- attempts to disrupt service to a specific system or person.

DDoS Attack

A DDoS (Distributed Denial-Of-Service) attack is a distributed, large-scale attempt by malicious users to flood the victim network with an enormous number of packets [4]. This exhausts the victim network of resources such as bandwidth, computing power, etc. The victim is unable to provide services to its legitimate clients and network performance is greatly deteriorated. The distributed format adds the “many to one” dimension that makes these attacks more difficult to prevent. A distributed denial of service attack is composed of

four elements. First, it involves a victim, i.e., the target host that has been chosen to receive the brunt of the attack. Second, it involves the presence of the attack daemon agents. These are agent programs that actually conduct the attack on the target victim. Attack daemons are usually deployed in host computers. These daemons affect both the target and the host computers.

The task of deploying these attack daemons requires the attacker to gain access and infiltrate the host computers. The third component of a distributed denial of service attack is the control master program. Its task is to coordinate the attack. Finally, there is the real attacker, the mastermind behind the attack. By using a control master program, the real attacker can stay behind the scenes of the attack. The following steps take place during a distributed attack:

- The real attacker sends an "execute" message to the control master program.
- The control master program receives the "execute" message and propagates the command to the attack daemons under its control.
- Upon receiving the attack command, the attack daemons begin the attack on the victim.

III. INTRODUCTION TO REAN (ROBUST EFFICIENT ADAPTIVE NETWORK)

To address different problems in networks we have designed a robust, efficient, adaptive network named as REAN which has following characteristics:-

ROBUST- Robustness is defined as "the ability of a system to resist change without adapting its initial stable configuration".

EFFICIENT- The extent to which time or effort is well used for the intended task or purpose.

ADAPTIVE- Adaptive behavior is a type of behavior that is used to adjust to another type of behavior or situation. This is often characterized by a kind of behavior that allows an individual to change an unconstructive or disruptive behavior to something more constructive.

NETWORK- A network is a telecommunication network that allows computer to exchange data. The physical connection between networked computing devices is established using either cable media or wireless media.

PROTOCOL- A set of rules and regulations that determine how data is transmitted in telecommunications and computer networking.

IV. WORKING OF REAN

Create a network consists of 30 nodes using AODV protocol. Create clusters and make cluster head, gateway nodes using cluster head gateway protocol. For sending data from one node to other we have to select a path that is best over the other paths (i.e. with minimum hopes). After selection of path we have to detect where the DDoS is attacking in the network, then the prevention mechanism is to be applied on that affected area. In the end we apply the maintenance procedure for the nodes in the network. And this maintenance procedure is working till the network is alive.

Parameter used in REAN

In our network use use the following number of parameters which are mentioned below:-

C_i = Cluster node,

C_{Hi} = Head cluster,

C_{Gi} = Gateway node,

N_{Ci} = Centre node,

B.W = Bandwidth,

N_i = Node,

P_{Ni} = Participating node,

P_i = Path selected,

W_i = Weight,

$L.B_i$ = Load balancing Factor,

$D.L_i$ = Delay,

Q = Priority Queue,

VAL $[N_i]$ = Value of i^{th} Node,

$N_{[RT]}$ = Routing table of node,

P_f = Path formation,

F_{id} = Flow id,

S_{id} = Source id,

D_{id} = Destination id,

$P_{[SR]}$ = Packet sending rate,

W [f(x)] = Weight function of x.

V. PROPOSED ALGORITHM

In this section we discuss about the proposed algorithm.

- Create a network consists of 30 nodes using AODV protocol.

- Create clusters and make cluster head, gateway nodes using cluster head gateway protocol.

i. Condition for node to be cluster head: - Node should be in centre within cluster and bandwidth of that particular node should be the maximum among all nodes within the cluster.

ii. Condition for node to be cluster gateway: - node should lie between two or more clusters.

iii. Rest of the nodes are participating nodes.

- ELECTION OF PATH:-

  We would use the path formation and path maintenance procedure of AODV and we will pick best three paths among all paths from source to destination.

  Condition of selection of path :- path should contain less hopes, weight factor(combination of load balancing +delay rate in respect with network)

  Maintain a priority queue to place all 3 paths for communication and pick a particular path only on the basis of priority

- MAINTENANCE OF PATH:-

  Periodically all cluster head will flood a status packet to ensure whether all nodes are still within the vicinity of its clusters.

  Condition for maintenance of path:- if value of node = '1' then check the IP address of node in the path routing table and remove the path which contains non-participating node(factor value =1) and refresh the routing table.

- DETECTION OF DDOS:-

  Pocket formation: - flow id +source id+ destination id +packet sending rate

  Calculate the weight factor [Wf(x)]:-

  If Wf(x) of each node lies within the range start the communication and periodically applies the detection of DDOS.

  Else: - PREVENTION OF DDOS

  Select second path from path routing table on the basis of their priority from priority queue.

- Repeat step 2 to above step.
- Stop communication.

Pseudo Notations

REAN(This algorithm is designed for network using these notations :- C_i =Cluster node, C_{Hi} = Head cluster, C_{Gi} =Gateway node, N_{Ci} = Centre node, B.W = Bandwidth, N_i = Node, P_{Ni} = Participating node, P_i = Path selected, W_i = Weight, $L.B_i$ =Load balancing Factor, $D.L_i$ = Delay, Q= Priority Queue, $VAL[N_i]$= Value of i^{th} Node, $N_{[RT]}$ =Routing table of node, P_f = Path formation, F_{id} = Flow id, S_{id} =Source id, D_{id} = Destination id, $P_{[SR]}$ = Packet sending rate, W[f(x)]= Weight function of x)

Step 1. Start.

Step 2. Create a network consists of 50 nodes using AODV.

Step 3. Create $[C_i]$, $[C_{Hi}]$ & $[C_{Gi}]$

For node to be $[CH_i]$

$N_i=N_{ci}$ && $B.W[N_i]=Max[N_{1,2,3,.....N}]$

For node to be $[C_{Gi}]$

N_i lies b/w 2 or more clusters

If $N_i != C_{Hi}$ && $N_i != C_{Gi}$

Then $N_i = P_{Ni}$

Step 4. [Election of path]

Pick best three paths among all paths [P_i] from source to destination.

P_i -> Min hopes

$W_i = [L.B_i + D.L_i]$

Queue = Q[P_1 , P_2 , P_3]

Choose path from the priority queue with highest priority.

Step 5. [Maintenance of Path]

Periodically all CH_i will flood a status packet.

If $VAL[N_i] = 0$

Then Node is outside the cluster & check $N_{[IP]}$ of Node in Path routing table & remove the path.

Refresh the $N_{[RT]}$ or update.

Step 6. [Detection of DDOS]

Packet Formation $[P_f]$

$P_f= F_{id} + S_{id} + D_{id} + P_{[SR]}$

b) Calculate Wt. Factor (W[f(x)])

if 0<(W[F(x)])<7

Then Start Communication & periodically applies detection of DDOS.

Step 7. Else [Prevention of DDOS]

Select P_i from routing table

$P_i = Q[P_2, P_3, P_4]$

Step 8. Repeat Step 3 to 6

Step 9. Stop communication.

VI. CONCLUSION AND FUTURE PROSPECT

Conclusion

Detection & Prevention of DDoS attacks is a part of an overall risk management strategy for an organization. Each organization must identify the most important DDoS risks, and implement a cost-effective set of defense mechanisms against those attack types causing the highest risk for business continuity. Studies and news about real-life DDoS attacks indicate that these attacks are not only among the most prevalent network security risks, but that these attacks can also block whole organizations out of the Internet for the duration of an attack. The risk from DDoS attacks should not thus be underestimated, but not overestimated, either. In this dissertation we try to overcome problem of DDoS attack.

Future Scope

In future, we will evaluate our framework for more internet topologies. In particular, we plan to investigate the following issues in more detail.

1. Introduction to load balancing in REAN: This dissertation only uses the load balancing factor but we can't adjust the factor according to our needs. So this issue can be considered for the further research work in future.
2. Quality of service (QOS): In our dissertation the concept of QOS is not introduced, due to bandwidth constraints and dynamic topology of Mobile Ad-hoc Network (MANET) , supporting QOS in MANET is a challenging task. So we plan to implement QOS while designing a network.
3. Under water networks: Further we also try to resolve the underwater problem.

REFERENCES

[1] Ajay Jangra, Sunita Beniwal, Anil Garg, "Co-existence behavior study of Bluetooth & Wi-Fi for 2.4 GHz ISM band" 2006

[2] Alessandro Mei, Julinda Stefa, "Routing in Outer Space: Fair Traffic Load in Multi-Hop Wireless Networks" MobiHoc'08, Hong Kong SAR, China in May 26–30, 2008.

[3] Binod Vaidya, Sang-Soo Yeo, Dong-You Choi , Seung Jo Han, "Robust and secure routing scheme for wireless multihop network" Published online: 4 April 2009, in Springer-Verlag London Limited 2009.

[4] Bogdan Carbunar, Ioanis Ioannidis and Cristina Nita-Rotaru, "JANUS: Towards Robust and Malicious Resilient Routing in Hybrid Wireless Networks" WiSe'04, October 1, 2004.

[5] Caroline Gabriel, "WiMax", ARCchart ltd., London EC2A 1LN

[6] Carlos A. Flores-Cortés, Gordon S. Blair, Paul Grace, "A Multi-protocol Framework for Ad-hoc Service Discovery" Melbourne, Australia MPAC '06, November 27-December 1, 2006.

[7] Charikleia Zouridaki, Brian L. Mark, Marek Hejmo and Roshan K. Thomas in October 2008.

[8] Chien-Chung Shen, Chaiporn Jaikaeo, "Ad Hoc Multicast Routing Algorithm with Swarm Intelligence" Mobile Networks and Applications 10, Springer Science + Business Media, Inc. Manufactured in The Netherlands, 47–59, 2005.

[9] Chin-Yang Tseng, Poornima Balasubramanyam, Calvin Ko, Rattapon Limprasittiporn, Jeff Rowe, Karl Levitt, "A Specification-based Intrusion Detection System for AODV" Proceedings of the 1st ACM Workshop Security of Ad Hoc and Sensor Networks Fairfax, Virginia © 2003 ACM-1-58113-783-4/03/0010.

[10] Chin-Fu Kuo, Hsueh-Wen Tseng, Ai-Chun Pang, "A Fragment-Based Retransmission Scheme with QoS Considerations for Wireless Networks" IWCMC'07, August 12{16, 2007, Honolulu, Hawaii, USA}.

[11] Claude Castelluccia, Nitesh Saxena, Jeong Hyun Yi, "Robust self-keying mobile ad hoc networks" Computer Networks 51 (2007) 1169–1182 1389-1286 2006 Elsevier B.V. doi:10.1016/j.comnet.2006.07.009.

[12] C.Siva Ram Murthy & B.S Manoj, "Mobile Ad Hoc Networks- Architectures & Protocols" , Pearson Education, New Delhi, 2004.

[13] Danesh, A. and Inkpen K., "Collaborating on Ad Hoc Wireless network", at www.parc.xerox.com/sl/projects/ubicomp-workshop/positionpapers/danessh.pdf.

[14] Dr. Sanjeev Sofat, Prof. Divya bansal and Rajinder Kumar, "Security in Mobile Ad Hoc networks", COIT-2008 March 29.