DETECTING DISTRIBUTED DENIAL OF SERVICE (DDOS) ATTACK USING TTL CONSTRAINT IN MOBILE ADHOC NETWORKS (MANET)

Abdullah Aljumah
College of Computer Engineering & Sciences, Prince Sattam Bin Abdulaziz University, Saudi Arabia
Aljumah@psau.edu.sa

ABSTRACT: *MANET (Mobile Adhoc Networks) are vulnerable to network attacks due to their dynamic topology and mobility and is enhanced by their limited resource constraints like battery life, storage and bandwidth. In such networks, most of the time the routers role is played by intermediate nodes. The attacks on these networks disturb and decline the performance and reliability and one of the major attacks on these networks is Distributed Denial of Service (DDoS) and these attacks are growing rapidly. These attacks make an online service inaccessible by flooding it with malicious data from multiple sources and directions. So, it is extremely important to prevent DDoS attack rather than letting it occur and then defending it. I am going to use TTL (time to live) as the main constraint to prepare a new technique to defend against DDoS Attacks and propose an approach to detect malicious node and DDoS attack.*

Keywords: DDoS, Security, MANET, TTL.

INTRODUCTION

Mobile Ad Hoc Networks (MANET) are self-organized and dynamic networks mainly composed of ambulant and wireless devices [1]. They do not need any pre-existing infrastructure to carry out with the help of multihop nodes in a decentralized manner. Even the topology is dynamic due to mobile nodes [2,3]. These dynamic characteristic of mobile adhoc networks makes it vulnerable to attacks. Since the mobile devices have limited resources like batter power, memory and bandwidth, these limited constraints impose many restrictions to preexisting security solutions in guided networks [4]. Due to dynamism and changing topology and lack of infrastructure the protocols and applications designed for these networks are based on node cooperation (cooperation between nodes) [5,6]. Thus allowing a node to decide whether to forward a data packet to other nodes generated from other node to save battery life or a node may not cooperate to other nodes and will behave maliciously in order to damage the network [7].

Since the Mobile Adhoc Network (MANET) is self-configuring, all the nodes and devices are able to move and relocate independently in many different routes and change its links to other connected devices frequently .The main concern in developing a MANET is preparing all the nodes and devices to keep up the knowledge constantly and frequently needed for the correct and true route traffic [8,9]. Such that the Mobile Adhoc Network (MANET) may operate by themselves or may get connected to the world internet. Proactive and reactive are the two main types of protocols used in MANETs. Reactive routing protocols that creates routes between nodes of the network when needed by applying or requesting a route direction technique including route request (RREQ) and route replies(RREP) [10], a procedure or a technique which really can easily be used for Distributed Denial of Service(DDoS) attack.

DDoS

Denial of service is simply an attack to prevent a genuine user of a network or its services from accessing the services or resources [11]. A Distributed Denial of Service (DDoS) is distributed and large scale attempt using malicious nodes to flood the target network from many directions with large number of packets [12]. Thus declining the performance of a MANET by affecting its bandwidth memory, batter etc. thus compelling a MANET not to provide services to its legitimate users. These types of attacks doesn't cause any harm to the data but do not let to access its resources [13]. It is an integration of compromised nodes which targets a single victim node and causes denial of service for the users of victim system [14]. Following figure-2 shows the components of a Distributed Denial of Service (DDoS) attack.

1. Attacker
2. Handlers or master hosts.
3. Zombies or compromised nodes.
4. Target or victim node.

The distributed denial of service (DDoS) attack can be classified into three main categories.

- Volume Based Attack. This attack is used to consume bandwidth of attacked or victim site and involves UDP floods, ICMP floods, spoofed packet floods etc.
- Protocol attack. This attack is used to consume the victim servers resources and involves Smurf DDoS, Ping to Death, fragmented packet attacks, SYN floods etc.
- Application Layer Attack. This attack is used to crash the target server and involves Slowloris , Zeroday DDoS attack, etc.

Proposed Solution

Mobile Ah Hoc Networks has lot of loopholes due to its infrastructureless structure. These loopholes make it more vulnerable to network attacks. Thus creating opportunities for the attackers to accomplish their network operations. Attackers can use any tool or any method to violate network policies and the most common and most powerful is DDoS (distributed denial of service) attack. This attack can influence the network operations like throughput, end-to-end delay, battery power etc. this attack is applied to individual network layers like network layer, media access control (MAC) in various forms. Following DDoS attacks can be attempted at MAC Layer to be protected.

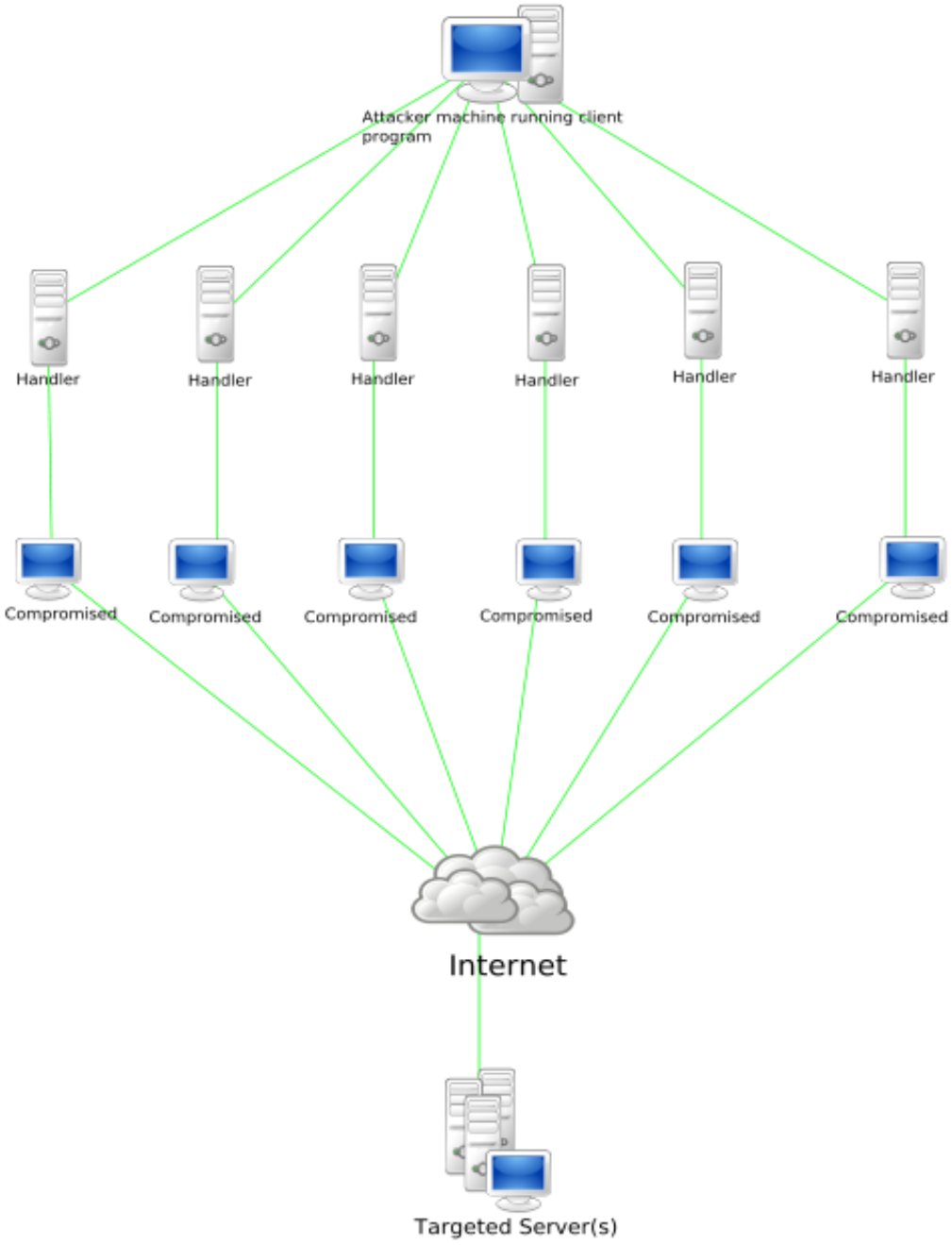


Figure 2. components of a Distributed Denial of Service (DDoS) attack

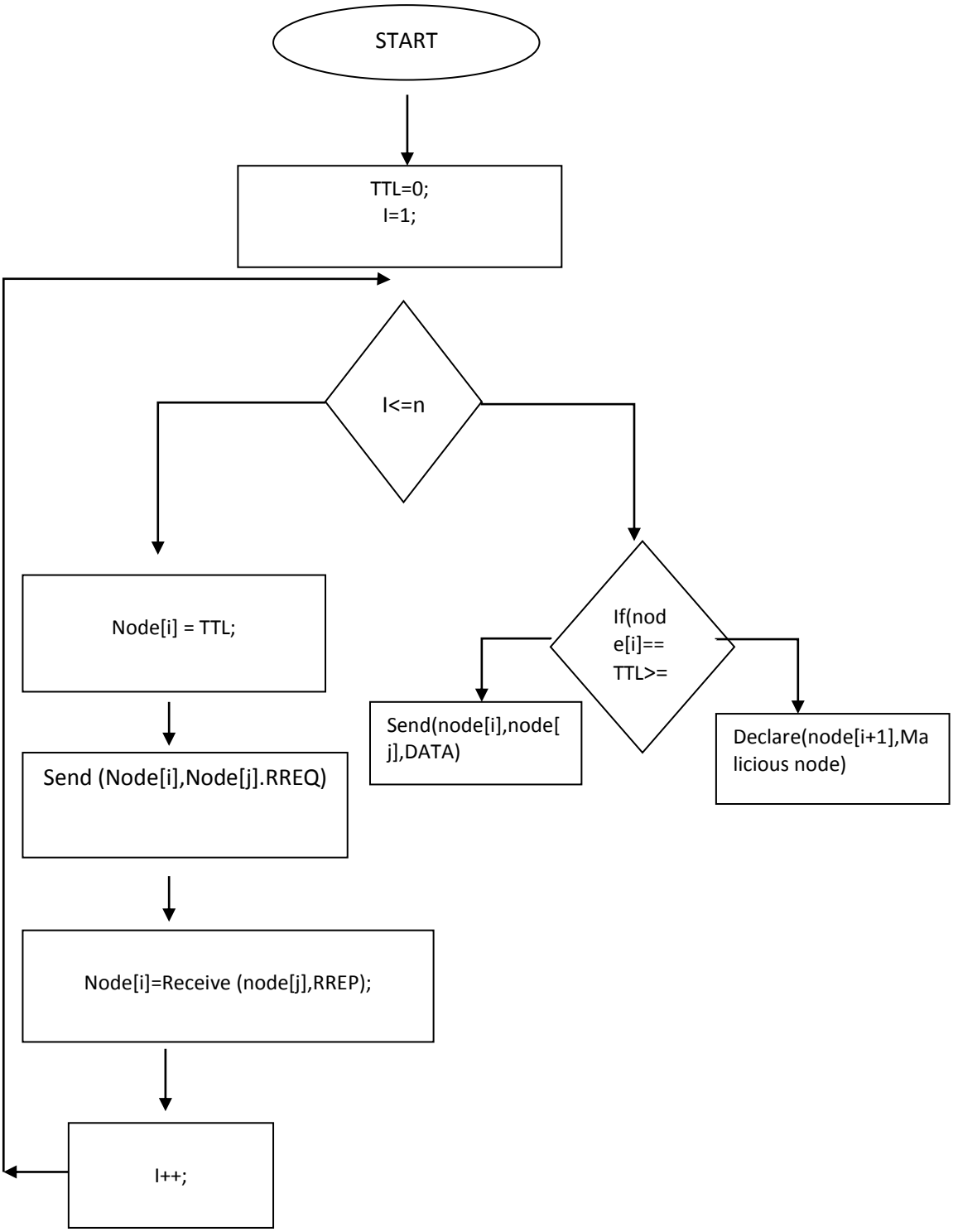
1. Assuming the reuse of only single channel for data, flooding this channel around the node leads to a pure DoS (distributed denial of service) attack
2. Continuous relay of data(false data) from a node can reduce the batter life.

Following are some DDoS (distributed denial of service) attacks at network layer to be protected.

1. The DDoS attacker node involvement in a route results in dropping of data packets, thus deteriorates the quality of connections and harms the performance.
2. The victim node transmits fake route updates and leads to recurrent route failures, thus declines the performance of the network.
3. The stale update reply by the victim or malicious node could also lead to decline in performance.
4. The reduction of TTL (Time To Live) in the IP header never let the data packet to reach its destination.

Several theories and mechanisms have been proposed for DDoS (distributed denial of service) but due to growth in technology they all need some more work to be done.

Flowchart



Flowchart of the proposed Work

Following is the algorithm and flowchart that will prevent data packet loss which usually occurs during deciding the TTL (Time To Live) value of a node and the detection of malicious node in the MANET (Mobile Adhoc Network).

The mechanism uses additional packet field named TTLv (Time To Live) before the data packet is assigned TTL (Time To Live) for the nodes. This TTLv assigned to node is decremented by the malicious node. Our mechanism will check this TTLv of the node and the data packet and in case it is abnormal then the node is declared as malicious or compromised node.

Algorithm

```
Malicious Node = Mn;
Node = N;
{
TTL=0;
For(i=0;i<=n;i++)
{node[i]=TTL;
Send(N[i],N[j],RREQ);
N[i]=Receive(N[j],RREP);
}
If(N[i]==TTL>=0)
Send(N[i],N[j],DATA);
Else
Declare(N(i+1),Mn);
}
```

CONCLUSION

DDoS is a serious issue and a ruthless attack in the networks that need to be detected and defended before reaching its target and cause the damage for the user, data and the services. The proposed approach offers DDoS detection and control technique based on TTL key field and can detect any malicious or suspicious node that can harm network resources and decline network performance. More research is needed to improve the technique for better results.

Acknowledgement

This research was funded and conducted at Prince Sattam bin Abdulaziz University, Alkharj, Saudi Arabia during the academic year 2015/2016 under research number 2015/01/3850.

REFERENCES

[1] L. Zhang, S. Yu, D. Wu, and P. Watters, "A Survey on Latest Botnet Attack and Defense," Proc. of 10th Intl' Conference On Trust, Security and Privacy in Computing and Communications (TrustCom), IEEE, pp. 53-60, November 2011.

[2] Mistry N, Jinwala DC, IAENG, Zaveri M, "Improving AODV Protocol Against Blackhole Attacks", International MultiConference of Engineers and Computer Scientists IMECS Hong Kong, Vol. 2, pp 1-6, 17-19 March, 2010.

[3] A. Mishra, B.B. Gupta, and R.C. Joshi, "A Comparative Study of Distributed Denial of Service Attacks, Intrusion Tolerance and Mitigation Techniques," Proc. of European Intelligence and Security Informatics Conference (EISIC), IEEE, pp. 286-289, September 2011.

[4] K. W. M. Ghazali, and R. Hassan, "Flooding Distributed Denial of Service Attacks-A Review," Journal of Computer Science 7 (8), Science Publications, 2011, pp. 1218-1223.

[5] H. Beitollahi, and G. Deconinck, "Denial of Service Attacks: A Tutorial,", Electrical Engineering Department (ESAT), University of Leuven, Technical Report: 08-2011-0115, August 2011.

[6] Z. Chao-yang, "DoS Attack Analysis and Study of New Measures to Prevent," Proc. of Intl' Conference On Intelligence Science and Information Engineering (ISIE), IEEE, pp. 426-429, August 2011.

[7] Information WeekSecurity: <http://www.informationweek.com>, February 2012.

[8] Business Insider: <http://articles.businessinsider.com>, October 2011.

[9] SecureList: <http://www.securelist.com>, February 2012.

[10] Prolexic Technologies: "Prolexic Attack Report Q1 2012", <http://www.prolexic.com>, April 2012.

[11] 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

[12] Tamilselvan L, Sankaranarayanan V, "Prevention of Blackhole Attack in MANET", 2nd International Conference on Wireless Broadband and Ultra Wideband Communications, Sydney, Australia, 27-30 August 2007.

[13] Raj PN, Swadas PB, "DPRAODV: A Dynamic Learning System against Blackhole Attack in AODV based MANEr', International Journal of Computer Science Issue, Vol. 2, pp 54-59, 2009.

[14] Wang W, Bhargava B, Linderman M, "Defending against Collaborative Packet Drop Attacks on MANETs". 2nd International Workshop on Dependable Network Computing and Mobile Systems, New York, USA, 27 September 2009.