DEFENSE FRAMEWORK (STREAM) FOR STREAM-BASED DDoS ATTACKS ON MANET

Dr. Imad S. Alshawi¹, Dr. Kareem R. Alsaiedy², Ms. Vinita Yadav³, Ms. Rashmi Ravat⁴

¹, ²(Department of Computer Science, College of Science/ Basra University, Basrah, Iraq)
³, ⁴(Department of Computer Science, Goel Institute of Technology and Management/ U.P Technical University Lucknow India)

ABSTRACT

MANET are usually characterized by limited resources such as bandwidth, battery power, storage space and node mobility. The underlying assumption is that the intermediate nodes cooperate in forwarding packets. Due to lack of infrastructure, the network can be easily affected by several attacks. The security challenges in MANET have become a primary concern to provide secure communication. The Attacks on MANET disrupts network performance and reliability. Nowadays, DoS attacks are usually launched in a distributed way: known as DDoS attacks i.e. the attacks where traffic originates from many attacking sources and the aggregated traffic volume is so big that it can easily deplete the victim’s key computing resources, such as bandwidth and CPU time. These attacks lead toward the degradation or prevention of legitimate use of network resources. Preventing or mitigating DDoS attacks is not an easy job. In this paper we develop the mechanism to deal with a stream-based DDoS defense framework (STREAM) that provides: Protection against different types of DDoS attacks (such as bandwidth flooding attacks and SYN flooding attacks) which are efficient against on-line DDoS detection providing filtering of illegitimate traffic.

Keywords: MANET, DOS, DDOS, Cluster, Attacks, STREAM.
I. INTRODUCTION

Security from the viewpoint of MANET[10-14] have been a primary concern requiring an accurate analysis and classification of denial of service attacks specific to the dynamic (ad-hoc) networks environment. MANETs offer several advantages over the traditional wired networks, they have associated set of challenges. Firstly, MANETs face challenges in secure communication. Since nodes are resource constrained, secondly ad hoc networks limit the cryptographic measures that are used for secure messages. Thereby MANET link attacks ranging from passive eavesdropping to active impersonation, message relay and message distortion. 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 are not adequate 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 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.

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:

- Attacks targeting energy resources, specifically the power source (battery) 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 and preventing other nodes from communicating with it.
- 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 (DDoS) attacks commonly leads to overwhelming the victims by sending a vast amount of legitimate-like packets from multiple attack sites (bots). 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, 30]. 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 these critical issues:

- filter out malicious traffic effectively minimizing the degradation of effective throughput of the legitimate traffic
- Minimizing the degradation of effective throughput of legitimate traffic.

DDoS Defense mechanism can be categorized into two major categories:

**Proactive DDoS defense mechanism**, these defense strategy focus on making malicious packets distinguishable from the legitimate ones, which usually requires the legitimate packets to contain some valid tokens and the corresponding checking procedures to be always turned on at the checking entry points (routers), but they compromise with the throughput of the legitimate traffic when defending DDoS attacks.

On the other hand **Reactive DDoS defense mechanism** does not affect the throughput of the legitimate traffic when there is no attack. 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 chapter - 1 discussed regarding of MANET, security issues in MANET, various attack types related to MANET specifically DoS and DDoS attacks, and Problem Identification, subsequently in chapter 2, we undergo through literature survey. Chapter 3, presents Proposed Architecture and mechanism Defense framework (STREAM) for stream-based DDoS Attacks on MANET which describes the traffic scenario being identified and maintained for the detection in MANET. chapter 4 mention about Conclusion of this Finally Chapter- 5 mention all references used in this paper.

**II. 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 relatively more vulnerable to attacks than all other layers in MANET. A variety of security threats is imposed in this layer. StreamCloud [18], a distributed-parallel stream processing engine, which can handle multi-hundred of thousands packets per second with only using a small number of processing instances. The performance (detection accuracy, filtering efficiency and monitoring overhead) of the proposed method is evaluated using data sets that are derived from real network traffic collected by CAIDA [19] and SUNET [33, 39]. According to the experiment results, STREAM offers good scalability to the incoming traffic load. The DDoS attack from the real network dataset can be quickly detected with low false negatives, and most malicious packets are filtered out, meanwhile keeping high percentage of the legitimate packets unaffected.
III. PROPOSED ARCHITECTURE FOR DEFENSE FRAMEWORK (STREAM) FOR STREAM-BASED DDoS ATTACKS ON MANET

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

3.1 Architecture of creation of cluster in stream-based DDoS attacks in MANET

STREAM monitors the network traffic between cluster nodes and detects the traffic discrepancies by comparing the real time traffic behavior with the expected traffic pattern which is referred to referenced profile. Figure 3.1.1 shows the architecture of node interaction to form a cluster in STREAM and the information flow among cluster nodes:

![Figure 3.1.1: Cluster Node interaction](image)
Cluster node interaction is illustrated by figure -3.1.1, based on the cluster interaction nodes form cluster so that traffic pattern can be evaluated on the basis of traffic source i.e. Cluster \( C_i \).

Cluster node interaction is illustrated by figure-3.1.1, based on the cluster interaction nodes form cluster so that traffic pattern can be evaluated on the basis of traffic source i.e. Cluster \( C_i \). Based on the nature of flooding-based DDoS attacks, where every malicious data packet may seem legitimate, however if each of them analyzed individually but where the overall traffic behavior may suffer abrupt flow variations (e.g. sudden increases of traffic volume), anomaly-based detection is always used to detect flooding-based DDoS attacks.

In recent decades, many anomaly-based detection methods were proposed to identify DDoS attacks from network traffic. Basically, these detection methods can be classified into two categories:

- off-line mode of DDoS detection
- on-line mode of DDoS detection.

Off-line DDoS mining usually try to find attacks by analyzing the main characteristics of feature distributions of the network traffic.

Anomalies in the network traffic can be identified since their dominate states deviate significantly from the normal ones. When the network anomalies are identified, data clustering methods, such as the one given below in order to group different types of anomalies together for further identification and correlating anomalies to attacks.

**Cluster formation(\( N_i \))**

\[
\text{The Cluster Head (Cluster\_Head)}_i = \text{id of } i^{th} \text{Cluster is given by the pseudo code:-}
\]

\[
\text{Node id is assigned as}
\]

\[
N_{id} = \text{Random\_generator();}
\]

\[
\text{Divide Mobile Nodes in Clusters}
\]

\[
\text{Assign each Cluster to Unique Cluster id “(Cluster)\_id”.
}\]

\[
\text{The Cluster Head (Cluster\_Head)}_i = \text{id of } i^{th} \text{Cluster is given by the pseudo code:-}
\]

\[
\text{If (N}_i < \text{NodeRange} \&\& \text{ Ni } \neq \text{C}_k) \quad \text{// where } \text{C}_k = \text{Set of Clusters in the Network}
\]

\[
\text{[C}_i \] } \leftarrow (\text{N}_i) \quad \text{// Ni } \text{ is assigned to ClusterC}_i
\]

**ClusterHeadSelection ( )**

\[
\text{Assume the following parameters as follows.}
\]

\[
\text{Score } = \text{NodeScoreValue();}
\]

\[
\text{Reputation } = \text{NodeReputation();}
\]

\[
\text{Smax } = \text{Scoremax();} \quad \text{//Assign max. value of Score to the variable Smax}
\]

\[
\text{Rmax } = \text{Reputationmax();} \quad \text{//Assign max. value of Reputation to the variable Rmax}
\]

\[
\text{For each cluster belonging to MANET}
\]

\[
\text{For (each node Ni } \&\& \text{ Ni } = 1 \text{ to Ni } = n)
\]
{ If( Smax || Rmax)
    { Set Node Ni = (ClusterHead)j,
    }
  else
    { Add node to jth Cluster i.e. Cj
      Cj ← Ni
    }
  } }

Handling DDOS attacks using STREAM

A. Handling anomalies in data traffic

Step-1: Server received large no. of SYN packets from clients.

observeSYNPacket( )
{
  IF(protocol.type = tcp && tcp.Flag = SYN(k) && destination.IP = victimServer.IP &&
    t<=T && n<= N )
  {
    If(Server monitors SYN packets)
      { Seq_No=Seq_No+1;
      }
    Elseif(Server received SYN packets)
      { Pass SYN packets;
      }
    Else
      { Drop SYN packets;
      }
  }
}

This attack could also use TCP data packets, which would be rejected by the server as not belonging to any known connection. But again, by this time the attack has already succeeded in flooding the links to the server.
Figure 3.1.2: Detection of SYN flooding attacks

Step-2: Monitor Traffic pattern to detect anomalies

- `MonitorTraffic_Profile()`
  
  ```
  Σ; /*Monitor the Traffic profile*/
  If(Davg ≥ Delayth)
  {
    “Normal traffic profile”;
  }
  Else
  {
    “Anomalies in the profile of Traffic flowing”; 
    AH = AH+1;
  }
  ```

Step-3: SYN flooding attack detected

`SYNFloodAttack()`

```
If(AH ≥ Th)
{
  GenerateSYNAlarmMessage()
  {
    “SYN Attack is detected”
  }
}
```
3.2 Defense mechanism

The defense mechanism consists of a filtering table (FT) of all the mobile nodes. It contains time, sender_id, node coordinate axis and receiver_id, transport_info, protocol_type, event_type contained in the filtering unit.

Filtering unit continuously compares traffic pattern with the referenced profile and an alarm is generated any time a suspicious variation between the two patterns is detected. While comparing the real time and the referenced profile, it also maintains and updates the latter. STREAM defines monitoring periods during which the real time and referenced traffic profiles are compared. Each time the monitoring period expires the referenced profile is updated with the real time profile if no attack has been detected.

IV. CONCLUSION

In this study we reviewed the design and implementation of a scalable online DDoS defense algorithm, which can detect and mitigate DDoS attacks, thus offering a protection at an early stage in the network. By investigating the traffic patterns of different forms of DDoS attacks (including connection requests flooding and bandwidth flooding), we proposed an IP-prefix based aggregation method to monitor and detect DDoS related anomalies.

Furthermore, differentiating from the prior DDoS detection solutions, we interrogated the design space of combining parallel-distributed data streaming with both online detection and baseline profile monitoring, and gave detailed solutions for achieving this. The proposed data streaming based DDoS defense solutions are implemented using STREM. DDoS detection can be carried out at the network links, where streams of packets are processed by continuous queries to find anomalous traffic patterns in real time. Data streaming queries are referred to as continuous as they are constantly “standing” over the streaming points and continuously producing spurt traffic flow. Most data-streaming based DDoS detection methods focus on using space efficient and time-efficient algorithm to keep track of the heavy hitters, e.g. a source sending lots of packets to many destinations, in the monitored traffic.

V. REFERENCES


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


BIOGRAPHY

Dr. Imad S. Alshawi (M’12) was born in Basra, Iraq, in 1976. He received the B.Sc. and M.Sc. degrees in computer science from the College of Science, Basra University, Basra, Iraq, in 2001 and 2003, respectively. He received the Ph.D. degree in information and communication system from Southwest Jiaotong University, Chengdu, China. He is currently an Assistant Professor with Computer Science Dept., Basra University. He is a frequent referee for more than 10 journals. He is the author or co-author of more than 30 papers published in prestigious journals and conference proceedings. His current research interests include wireless sensor network and artificial intelligent. Dr. Alshawi is a member of the IEEE, the IEEE Cloud Computing Community and the IEEE Computer Society Technical Committee on Computer Communications.

Dr. Kareem R. Alsaiedy was born in Basra, Iraq, in 1959. He received the B.Sc. degree from engineering collage and M.Sc. degree in computer science from the College of Science, Basra University, Basra, Iraq, in 1985 and 2000, respectively. He received the Ph.D. degree in simulation and control system from Basra University, Iraq. He is currently a lecturer in Computer Science Dept., Basra University. He is a frequent referee for 4 journals. He is the author or co-author of more than 20 papers published in journals and conference proceedings. His current research interests include wireless sensor network and artificial intelligent. Dr. Alsaiedy is a manager of Basra university publishing and book shop center.

Ms. Vinita Yadav is a student of M.Tech, Department of Computer Sc, Goel Institute of Technology and Management, Lucknow, India. Uttar Pradesh Technical University Lucknow India. She did her Bachelor in Engineering from Department of Computer Science; M.B.M Engineering College Jodhpur, India in 2003. She has a work experience of 7 years in the field of Telecommunications (Reliance Communications Limited, India) and teaching. Her areas of interest are Artificial intelligence and Computer Networks.

Ms. Rashmi Ravat is a student of M.Tech, Department of Computer Sc, Goel Institute of Technology and Management, Lucknow, India. Uttar Pradesh Technical University Lucknow India. She did her Bachelor in Engineering from Department of Information Technology, University Institute of Engineering & Technology, Kanpur, India in 2008. She has a work experience of 4 years in the field of Software Development. Her areas of interest are Software Engineering and DataBase Management System.