1. **Mitigating DNS Query-Based DDoS Attacks with Machine Learning on Software-Defined Networking**

Due to *lack of stringent security* measures in IoT systems, *DNS protocol exploitation*, and *limitations of packet forwarding* in traditional networks, mitigation against DDoS attacks is a big challenge for military organizations.

Two famous DNS query-based DDoS attacks are: -

1. DNS amplification

To launch such attack, attackers send large volume of forged DNS queries with spoofed IP address of victim to open DNS resolvers to prompt them to send massive volumes of DNS query responses to the victim with that address.

To amplify such attack, DNS request can be sent using EDNS0 or DNSSEC DNS protocol extension or with spoofed queries of type ANY. These results in amplification factor of 70:1.

1. DNS flooding

These attacks attempt to target server-side resources with a flood of UDP requests, generated by scripts running on botnet devices. Layer 7 attacks and DNS NXDOMAIN flood attacks are more common. The DNS server expends all its resource looking for false records filling its cache thus no resources to serve legitimate requests.

Since SDN controller maintain global view of entire network and dynamically manage switches in an SDN environment, if seems effective to develop mitigation solutions for DDoS attacks. Features of SDN used for mitigation are: -

1. Decoupled control and data planes
2. Dynamic updating of forwarding rules
3. Software-based traffic analysis

Dirichlet Process Mixture Model (DPMM) is proposes as a nonparametric Bayesian approach for clustering traffic application where nonparametric means that no. of traffic app. Are unknown and may grow over time.

To study effectiveness of proposed DPMM approach for attack detection we evaluate following: -

1. Attack traffic classification accuracy
2. Overall classification accuracy
3. Misclassification rate
4. **Mitigating DNS DoS Attacks**

As explained in previous paper that DNS flooding attacks target the server-side resources and the caches. Therefore, proposed resolver modification focuses on change of caching behaviour of DNS resolvers so that they can shoulder more of the resolution burden, especially when nameservers are unavailable.

Proposed change in the operation of DNS resolvers are: -

1. Stale cache

Resolvers don’t completely expunge records whose TTL value has expired. Rather, such records are evicted from the cache and stored in a separate *stale cache.* In effect, the stale cache together with the resolver cache represents the part of global DNS database that has been accessed by the resolver.

1. Resolving queries

In our proposed modification, first two steps are as same as of todays DNS resolver but the third step is modified as:

In case the resolution process fails due to inability of the resolver to contact all the nameservers of the relevant zone at any step of traversal, search the stale cache for the required record and if found, the resolution process can continue on basis of this stale record.

1. Stale cache clean-up

Existing resolvers cache the responses to the queries made during the resolution process but in this proposed modification these responses are also used to evict the corresponding stale records from the stale cache.

Advantages of proposed modification: -

1. DNS Robustness
2. Simplicity

* Does not change the basic protocol operation and infrastructure
* Does not impose any load on DNS
* Does not impact the latency of query resolution

1. Incremental Deployment
2. Motivation for Deployment

Objections of proposed modification: -

1. DNS caching semantics and the possibility of inaccurate information being used
2. Autonomy for zone operators
3. Attackers attempting to force the use of inaccurate information
4. Privacy concerns
5. Resolution latency in the face of an attack
6. **Denial of Service Attack and Prevention on SIP VoIP Infrastructure Using DNS Flooding**

The goal of attack is to make SIP infrastructure inoperable for as long as possible. These attacks can target any kind of SIP entity like user agent, proxy, registrars, and redirect proxy but are most effective against proxies and redirectors.

Scope of Attack: -

Whenever a SIP proxy encounters a fully qualified URL in a header field necessary for routing, it issues a query to the local name server to receive a valid address mapping. Usually it takes around 1.3 DNS queries to receive an answer with mean resolution latency of less than 100ms. But these values can be high due to configuration errors.

These relatively high processing time are major targets of the SIP DNS attack. It is done by specially crafted SIP messages containing URLs that will cause an even higher processing time at DNS server by using a URL in a routing header of which the attacker is sure that its mapping will not be in cache or will trigger to authoritative server having low response time.

Issuing SIP queries with a variation of URLs that are well formatted, complying with the SIP standards and can’t be filtered out by Intrusion Detection System, will stop operation at a SIP proxy for a considerable time. Since SIP proxy can continue its operation only after receiving an answer from DNS server, if no answer is received within timeout period, a negative reply is generated.

Existing solution against DNS attacks: -

General method is to trace the source of attack and block the traffic from is but for SIP network that runs at application layer, back tracing is costly and not much efficient. Thus, Synchronous and Asynchronous DNS implementation were proposed but they too are not sufficient to withstand a DNS attack with large no. of malicious messages per second.

Proposed solution against DNS attack: -

In proposed system, we use Non-Blocking Cache Design that is based on caching the results of successful DNS queries. This is implemented for a synchronous working server.

Steps involved are: -

1. DNS Attack Detection and Prevention (DADP)
2. Implementation of DADP

* Performance Evaluation of DADP
* Cache Replacement Policies Evaluation
* Evaluation of Cache Entry Numbers