JESS: Joint Entropy-Based DDoS Defense Scheme in SDN

IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, VOL. 36, NO. 10, OCTOBER 2018

Kübra Kalkan, Levent Altay, Gürkan Gür, and Fatih Alagöz

----------------------------------------------------------------------------------------------------

**名义阶段：**

属性对→属性对配置文件→生成基线信息

（在名义阶段结束时，当名义轮廓准备好时，控制器计算每对的联合熵。）

---------------------------------------------------------------------------------------------------------------------------------

**准备阶段：**

在检测到拥塞之后，开始准备阶段。（当业务带宽超过标称阈值时）

（检测到DDoS攻击并确定相关参数）

交换机开始将数据包报头发送到控制器。控制器为每个属性对生成当前对配置文件并计算联合熵。如果任何差异超过θJ，则检测到DDoS攻击。然后，将具有最大差异的对确定为SuspiciousPair。生成的信息将发送到交换机。

---------------------------------------------------------------------------------------------------------------------------------

**缓解阶段：**

确定SuspiciousPair后，将启动主动缓解阶段。

在该阶段的时段期间，交换机创建所识别的SuspiciousPair的当前配置文件SC，并且在每个时段结束时它将SC发送到控制器。控制器计算配置文件中的每个条目的相应分数并生成分数表ST。

随后，通过将每对分数与指定阈值θs进行比较，生成当前规则表rtc。如果某个条目的分数低于此阈值，则相应规则将确定为“转发”，否则为“删除”规则。然后，将当前规则表rtc与上一个规则表rtp进行比较，为了最大限度地减少规则表管理的更新流量，只将不同的规则Δ−rt发送到交换机，因为它们在上一个期间之后发生了更改。然后，开关根据Δ−rt更新其规则表。

生成（解析包集合）→生成（标准配置文件）→生成（P阶标准配置文件）→计算标准对配置文件的联合熵JN

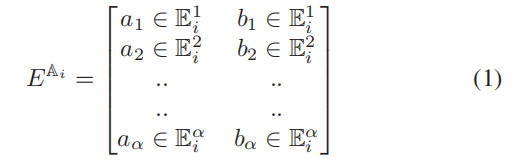
每α个数据包为一个周期

**第一阶段：**

解析包：是第j个解析包。它具有相应属性的aj和bj值， =（aj，bj）。

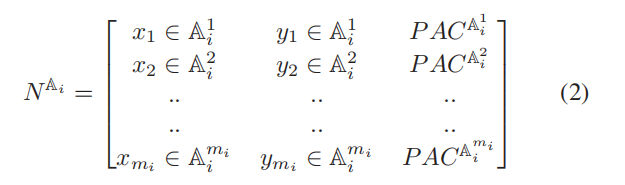
**1）解析包集合：**

α\*k矩阵，。



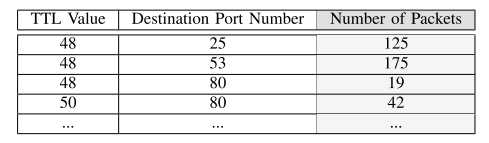
**2）标准配置文件：**

，基于矩阵，通过为中的每个不同的元组=（aj，bj）添加一个新元素，创建一对的标准配置文件。通过计算具有相同属性值的数据包数量，每个交换机在无攻击期间为每个pair属性生成名义配置文件。



其中mi是一个系统特定的正整数，取决于相应周期内不同性质的包的数目。

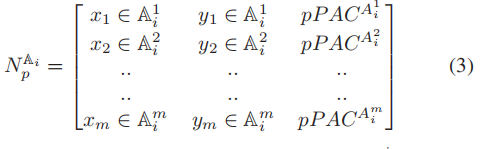
名义配置文件示例（不同类型包的数量）：



 ：类似与上面的，都是的子集。一个属性对。

**3）p阶标准配置文件：**



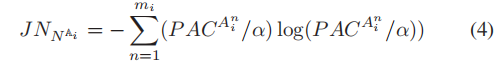


异常检测：

控制器计算每个标准对配置文件的联合熵JN并将其用于检测功能。当比较当前配置文件和标称配置文件的联合熵值时，如果任何一对的差异超过阈值θj，则检测到DDoS。然后将最大差的一对作为当前攻击的决定因素对。

**4）JN具体计算：**

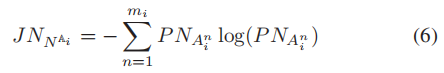
（1）名义周期中的名义配置文件的联合熵计算如下：



我们放弃了 p 因为我们正在使用 p = 1 在我们的实验中。为了便于在前面的等式中表示，术语定义为：



然后，可以简化为：



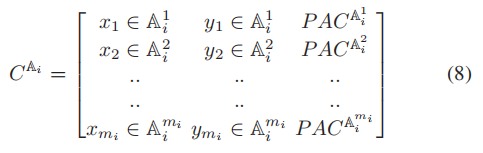
为了使熵值在[0，1]中，我们将其标准化如下：



**第二阶段:**

**1）当前配置文件生成：**

每个交换机在攻击期间为每对配对属性Ai生成当前配置文件。它计算具有相同属性值的数据包的数量。在此分析期间，交换机将所有数据包的标头发送到控制器。因此，控制器为每个组合生成对配置文件。第i个当前配置文件如（8）所示：

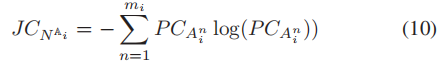


**2）当前剖面的联合熵计算：**

计算每对的联合熵JC，以便与JN进行比较。与类似，术语表示如下：



然后， JC 计算方法如下：



**3）比较：**

当前剖面的联合熵值准备就绪时，将其与相应的名义联合熵值进行比较，并计算出每对的：



先计算JN，再计算JC，接着计算二者的差值



如果有任何差异值超过阈值，则检测到ddos攻击。

检测后，Jess根据操作确定和k=2的最大差值，并识别出最大差值的对。假设ΔJNA2具有该最大差异。然后它将被标记为SuspiciousPair，它被认为是最适合缓解当前攻击流量的一对。因此，控制器向交换机发送信令消息以通知它有关SuspiciousPair的信息。

**第三阶段**

缓解阶段：

#### **1）SuspiciousPair Profile Generation：**

在前两个阶段中，所有数据包报头都从交换机发送到控制器。这种机制显然会在交换机上产生大量的通信负担。在此阶段，此开销减少。由于交换机知道SuspiciousPair，它开始为该对生成当前配置文件SC。它不发送所有数据包的报头，而只是在每个周期结束时将当前配置文件SC发送到控制器。

#### **2）分数计算：**

在SC生成之后，控制器具有SuspiciousPair的标准配置文件SN和当前配置文件SC。取SC的每个条目，并通过考虑其在SN中的对应值来计算其得分β。在确定SuspiciousPair之后，每个条目的得分β计算如下：



所有β值都存储在数据结构中，即得分表ST。

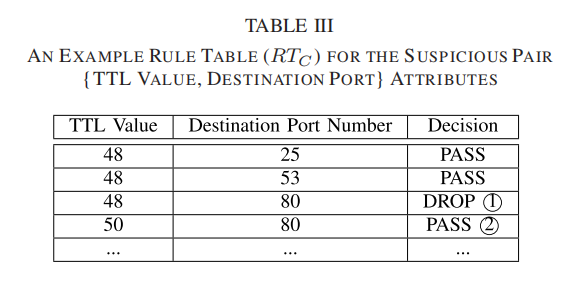
#### **3）阈值确定：**

需要将分组的分数与阈值进行比较以确定丢弃或通过动作。 控制器通过使用减载算法[41]根据ST中的分数的累积分布确定当前阈值。这个分布以符号形式表示为，而Φ是应该减少的流量比。允许通过的流量的一部分是，而φ是可接受的流量，而ψ是总的当前进入交通量。阈值θs由当前θc和上一时期的θp确定，因此计算如下：



#### **4）规则生成：**

控制器计算得分和阈值后，系统准备生成过滤规则。由于计算了SC中每个条目的得分，因此可以通过与该值的比较来提供丢弃或通过的决定。如果得分值超过阈值，则认为数据包是恶意的并被丢弃。否则，它将被转发到目的地。控制器为SC中的每个条目生成一个当前规则表rtc。规则表示例如表III所示。



#### **5）不同的规则（Δ - R u l e s ）测定：**

控制器通过比较当前规则表来确定不同的规则 R T.C 和以前的规则表 R T.P 。具有相同决策的相同规则将不会被发送到交换机以实现更高的效率和开销最小化。例如，下表R T.P 在表III中与之比较R T.C 在表IV中仅列出了最后两条规则（①和②）R T.C 被确定为不同的规则 Δ - R T. ，因为它们与以前的不同。然后，它们被发送到交换机。

考虑到本节中描述的所有组件和算法程序，JESS操作可以基于其三个主要阶段进行总结：名义，准备和主动缓解。通过在标称阶段中为每个属性对创建名义对配置文件来生成基线信息。控制器计算每对的联合熵。在拥塞信令检测到DDoS攻击之后，开始准备阶段，其中控制器生成当前对配置文件并计算每对的联合熵。然后它将这些当前熵与名义熵进行比较，以确定是否存在实际的攻击。因此，具有最大差异的对被标记为SuspiciousPair。确定该对后，启动主动缓解阶段。交换机创建可疑的当前配置文件sc，并在每个周期结束时将sc发送给控制器。控制器计算配置文件中每个条目的得分，并生成得分表st。生成当前规则表rtc。如果一对的得分低于阈值，则转发，否则丢弃，即减轻ddos攻击。另外，由于前一段时间后规则发生了变化，所以只向交换机发送不同的规则Δ−rt，然后交换机根据Δ−rt更新其规则表。

