An Authentication Code Against Pollution Attacks

In Network Coding

**Abstract*—***Systems exploiting network coding to increase their throughput suffer greatly from pollution attacks, which consist of injecting malicious packets in the network. The pollution attacks are amplified by the network coding process, resulting in a greater damage than under traditional routing. We address this issue by designing an unconditionally secure authentication code (that is, which does not rely on computational assumptions) suitable for multicast network coding, where the keying material is initially computed and distributed by a trusted authority to the destinations and intermediate nodes. The proposed scheme allows not only destinations, but also intermediate nodes, to verify the integrity and origin of the packets received without having to decode, and thus detect and discard the malicious messages in transit that fail the verification. This way, the pollution is canceled out before reaching the destinations. The proposed scheme is robust against pollution attacks from outsiders, as well as coalitions of malicious insider nodes, which have the ability to perform the integrity check, but instead get corrupted and use their knowledge to themselves attack the network. We analyze the performance of the scheme in terms of both throughput and goodput and show that the price to pay for tolerating inside attackers is a high decrease in throughput (it is inversely proportional to the number of insider attackers that can collude).

**Exsiting system:**

With the existing system while using to the Compromised Node [CN] and denial of service [DOS] transferring the data there is no security constraints are added. Even though you are transferring the data whole application will be struck. Systems exploiting network coding to increase their throughput suffer greatly from pollution attacks, which consist of injecting malicious packets in the network. The pollution attacks are amplified by the network coding process, resulting in a greater damage than under traditional routing.

Disadvantages:

* Data loss
* Wastage time
* No security

**Proposed system:**

In this proposed system replaced the disadvantage in Existing System. Here we are using randomized routing algorithm as a technique for Securely sending the data through network. So there is no data Losing. The proposed scheme allows not only destinations, but also intermediate nodes, to verify the integrity and origin of the packets received without having to decode, and thus detect and discard the malicious messages in transit that fail the verification. This way, the pollution is canceled out before reaching the destinations. The proposed scheme is robust against pollution attacks from outsiders, as well as coalitions of malicious insider nodes, which have the ability to perform the integrity check, but instead get corrupted and use their knowledge to themselves attack the network.

Advantages:

* No data loss
* Save the time
* Clear path
* Security

**HARDWARE AND SOFTWARE REQUIREMENTS:**

**Software Requirements:**

Language : C#.NET

Technologies : Microsoft.NET Framework,

ASP.NET,ADO.NET

IDE : Visual Studio 2008

Backend : SQL Server 2005

Operating System : Microsoft Windows XP SP2 or Later Version

**Hardware Requirements:**

Processor : Intel Pentium or more

RAM : 512 MB (*Minimum*)

Hard Disk : 40 GB