A Probabilistic Misbehavior Detection Scheme towards Efficient Trust Establishment in Delay-tolerant Networks

ABSTRACT:
Malicious and selfish behaviors represent a serious threat against routing in Delay/Disruption Tolerant Networks (DTNs). Due to the unique network characteristics, designing a misbehavior detection scheme in DTN is regarded as a great challenge. In this paper, we propose iTrust, a probabilistic misbehavior detection scheme, for secure DTN routing towards efficient trust establishment. The basic idea of iTrust is introducing a periodically available Trusted Authority (TA) to judge the node's behavior based on the collected routing evidences and probabilistically checking. We model iTrust as the Inspection Game and use game theoretical analysis to demonstrate that, by setting an appropriate investigation probability, TA could ensure the security of DTN routing at a reduced cost. To further improve the efficiency of the proposed scheme, we correlate detection probability with a node's reputation, which allows a dynamic detection probability determined by the trust of the users. The extensive analysis and simulation results show that the proposed scheme substantiates the effectiveness and efficiency of the proposed scheme.
EXISTING SYSTEM:

In DTNs, a node could misbehave by dropping packets intentionally even when it has the capability to forward the data (e.g., sufficient buffers and meeting opportunities). Routing misbehavior can be caused by selfish (or rational) nodes that try to maximize their own benefits by enjoying the services provided by DTN while refusing to forward the bundles for others, or malicious nodes that drop packets or modifying the packets to launch attacks.

Recently, there are quite a few proposals for misbehaviors detection in DTNs, most of which are based on forwarding history verification (e.g., multi-layered credit, three-hop feedback mechanism, or encounter ticket), which are costly in terms of transmission overhead and verification cost. The security overhead incurred by forwarding history checking is critical for a DTN since expensive security operations will be translated into more energy consumptions, which represents a fundamental challenge in resource constrained DTN.

PROBLEM DEFINITION:

- Malicious and selfish behaviors represent a serious threat against routing in Delay/Disruption Tolerant Networks (DTNs).
- Due to the unique network characteristics, designing a misbehavior detection scheme in DTN is regarded as a great challenge.
Even though the existing misbehavior detection schemes work well for the traditional wireless networks, the unique network characteristics including lack of contemporaneous path, high variation in network conditions, difficulty to predict mobility patterns, and long feedback delay, have made the neighborhood monitoring based misbehavior detection scheme unsuitable for DTNs.

PROPOSED SYSTEM:

In this paper, we propose iTrust, a probabilistic misbehavior detection scheme, for secure DTN routing towards efficient trust establishment. The basic idea of iTrust is introducing a periodically available Trusted Authority (TA) to judge the node’s behavior based on the collected routing evidences and probabilistically checking.

ADVANTAGES OF PROPOSED SYSTEM:

- Reduce the detection overhead effectively.
- Improved Security.
- Improved Efficiency.
- Will reduce transmission overhead incurred by misbehavior detection and detect the malicious nodes effectively.
SYSTEM ARCHITECTURE:

HARDWARE REQUIREMENTS:

- System: Pentium IV 2.4 GHz.
- Hard Disk: 40 GB.
- Floppy Drive: 1.44 Mb.
- Monitor: 15 VGA Colour.
- Mouse: Logitech.
- Ram: 512 Mb.
SOFTWARE REQUIREMENTS:

- Operating system : Windows XP.
- Coding Language : C#.Net.
- Data Base : SQL Server 2005