**PROVEST Provenance-based Trust Model for Delay Tolerant Networks**

**ABSTRACT:**

Delay tolerant networks (DTNs) are often encountered in military network environments where end-to-end connectivity is not guaranteed due to frequent disconnection or delay. This work proposes a provenance-based trust framework, namely PROVEST (PROVEnance-baSed Trust model) that aims to achieve accurate peer-to-peer trust assessment and maximize the delivery of correct messages received by destination nodes while minimizing message delay and communication cost under resource-constrained network environments. Provenance refers to the history of ownership of a valued object or information. We leverage the interdependency between trustworthiness of information source and information itself in PROVEST. PROVEST takes a data-driven approach to reduce resource consumption in the presence of selfish or malicious nodes while estimating a node’s trust dynamically in response to changes in the environmental and node conditions. This work adopts a model-based method to evaluate the performance of PROVEST (i.e., trust accuracy and routing performance) using Stochastic Petri Nets. We conduct a comparative performance analysis of PROVEST against existing trust-based and non-trust-based DTN routing protocols to analyze the benefits of PROVEST. We validate PROVEST using a real dataset of DTN mobility traces.

**EXISTING SYSTEM:**

* Provenance has been used to verify trust, trustworthiness, or correctness of information in many research areas. Rajbhandari et al. [12] examined how provenance information is associated with a workflow in a Bio-Diversity application. Dai et al. [13] proposed a data provenance trust model to evaluate trustworthiness of data and data providers. Yu et al. [14] presented an agent-based approach to managing information trustworthiness in network centric information sharing environments.
* Golbeck [15] used provenance information to infer trust in Semantic Web based social networks. Zhou et al. [16] used data provenance computations and queries over distributed streams for effective network accountability and forensic analysis to enhance network security. However, the above studies [12]- [16] focused on evaluating trustworthiness in information without considering specific network attack behaviors that may maliciously change the original messages and disrupt system goals.
* Some researchers have made efforts to secure provenance data. Hasan et al. [17] insisted that secure provenance is a critical aspect to increase protection of provenance information. Braun et al. [18] explained that “provenance” consists of relationships (i.e., a graph) and attributes (i.e., attributes of an entity). Hasan et al. [19] presented a provenance-aware prototype to ensure integrity and confidentiality of provenance information based on provenance tracking of data writes at the application layer. Wang et al. [20] proposed a “chain-structure” provenance scheme that provides security assurance for provenance meta-data.
* Gadelha and Mattoso [21] proposed a security architecture framework that protects authorship and temporal information in grid-enabled provenance systems. Lu et al. [22] proposed a provenance scheme using the bilinear pairing techniques in order to secure provenance data of ownership and process history of data object in cloud computing. The above works have studied how to secure provenance data with the existence of a centralized trusted entity.

**Disadvantages**

* There are no Un scalable nodes trust, instead it is scalable.
* More Packet Drops and less throughput.

**PROPOSED SYSTEM:**

* PROVEST significantly reduces communication cost, compared to existing counterparts, by using provenance information (i.e., identification and opinion towards a previous message carrier) tagged in messages. In PROVEST, a trustor does not directly request recommendations from third parties because collecting recommendations requires extra overhead, and recommendations are often not available in a sparse DTN. Rather, PROVEST allows indirect evidence (recommendations) to be collected via message delivery even for two nodes that have not encountered each other for a long time.
* The system proposes to characterize a DTN node with the concept of multidimensional trust, including availability, integrity, and competence, in the context of trust evidence propagation using provenance information. Although multidimensional trust has been considered in other networks (e.g., [7]), we are the first to consider its use in a provenance-based trust model in DTN environments.
* The system considers sophisticated attack scenarios that often happen in dynamic DTN environments where various types of hostile entities exist to interrupt service availability. In particular, we consider the case in which provenance information can be dropped, modified, or forged by attackers in DTNs.
* The system develops a model-based evaluation method based on Stochastic Petri Nets (SPNs) to identify the optimal minimum trust threshold in selecting a message carrier to achieve availability, integrity, and competence. The system conducts a comprehensive performance analysis to demonstrate the superiority of PROVEST, over existing trust-based and non-trust-based DTN routing protocols with simulation validation, in terms of trust accuracy and routing performance.

**Advantages**

* The system is more secure due to the combination of Direct availability, trust Direct integrity trust and Direct competence trust.
* No Packet Drops

**SYSTEM SPECIFICATION**

**Hardware Requirements:**

* System : Pentium IV 3.5 GHz.
* Hard Disk : 40 GB.
* Monitor : 14’ Colour Monitor.
* Mouse : Optical Mouse.
* Ram : 1 GB.

**Software Requirements:**

* Operating system : Windows XP or Windows 7, Windows 8.
* Coding Language : Java – AWT,Swings,Networking
* Data Base : My Sql / MS Access.
* Documentation : MS Office
* IDE : Eclipse Galileo
* Development Kit : JDK 1.6