International Journal of Science Engineering and Advance Technology

Identity Systematizing Conviction Model For Peer To Peer Systems

Durgabhavani.K #1, Rajesh.A #2
#1, 2 Student of M.Tech Department of Computer Science Enginering
G.V.R&S colege of Enginering& Technology, Guntur

Abstract

A "mobile ad hoc network" (MANET) is an autonomous system of mobile routers (and associated hosts) connected by wireless links --the union of which form an arbitrary graph. The routers are free to move randomly and organize themselves arbitrarily; thus, the network's wireless topology may change rapidly and unpredictably. Such a network may operate in a standalone fashion, or may be connected to the larger Internet. Sensor nodes consist of sensing, data processing, and communication components and typically form ad hoc networks. Due to a lack of infrastructure support, each node acts as a router, forwarding data packets for other nodes.Open nature of peer-to-peer systems exposes them to malicious activity. Building trust relationships among peers can mitigate attacks of malicious peers. And the un structured peers are having lack of bandwidth, mobility .So in this paper presents distributed algorithms that enable a peer to reason about trustworthiness of other peers based on past interactions and recommendations.

Index Terms-Peer to Peer, Reputation, Trust management, security.

I INTRODUCTION

Information exchange in a network of mobile and wireless nodes without any infrastructural support. Such networks are often called ad hocnetworks to emphasize that they do not depend on infrastructural support. A mobile ad-hoc network is a mobile, multi-hop wireless network which is capable of autonomous operation.

The purpose of an ad hoc network is to set up (possibly) a short-lived network for a collection of nodes.A **router** receives a packet from a network and passes it to another network. At the Router a Routing Table is maintained which may be Static or Dynamic. A router is usually attached to several networks. When it receives a packet, to which network should it pass the packet? The decision is based on optimization: which of the available pathways is the optimum pathway? Routing is the act of moving information across an internetwork from a source to a destination. Along the way, at least one intermediate node typically is encountered.

Routing involves two basic activities: determining optimal routing paths and transporting information groups (typically called packets) through an internetwork. A node does not perform route discovery or maintenance until it needs a route to another node or it offers its services as an intermediate node.Nodes that are not on active paths do not maintain routing information and do not participate in routing table exchanges. But here not satisfied the trustability.

2 problem statement:

Limitations of the Wireless Networkpacket loss due to transmission errors variable capacity links frequent disconnections/ partitions limited communication bandwidth Broadcast nature of the communications Limitations Imposed by Mobility dynamically changing topologies/route slack of mobility awareness by system/applications Limitations of the Mobile Computer short battery life time limited capacities .

3.THE FRAMEWORK

3.1 The Design

A framework is to outline probable lines of acts or to depict a favored approach to a proposal or notion. A framework can work that is approximating to a plot giving reasoning to pragmatic inquisition. For software development point of view, a framework, that is used by software developers to implement the standard structure for an application. An excellent framework should be conceptual and absolute, obvious and definite, summarized and comprehensible, straightforward to sustain and cost

efficient. Above all, it should be valuable. An abstract representation of the proposed framework is shown in Fig 1.

The Ad hoc Network Set Up should have the description classes essentially- network parameters, application and the node parameters. An exhaustive study of the literature and simulation tools for ad hoc networks acknowledged the subsequent network parameters—Geographical Area, Number of Nodes, Placement of nodes, Mobility model, Terrain and some other optional parameters. The application class expresses the catalog of possible applications that can be accomplished e.g. Email, ftp, chatting, video conferencing and so on. The node parameters are used to depict the parameters of node in provisions of battery, memory, mobility speed, clock speed.

The trusted protocol is an enhanced adaptation of an existing protocol. The protocol may be a routing protocol, or an authentication protocol or an access control protocol. Thus this flexibility in the proposed framework results it as a generalized framework. The protocol is customized so that it should take trust value in concern while making decisions. We have presented a relative study of performance of ad hoc routing protocols in our prior work [13]. On the source of the results of that study we have selected the OLSR routing protocol for demonstrative purposes. Subsequent to the selection of protocol, the next step is to make it trusted protocol. The formal specifications of the trusted OLSR protocol in formal language Z is given in the paper [14]. The trusted protocol with the ad hoc network setup granted a trusted ad hoc network i.e. an ad hoc network that too considers trust value while making decisions.

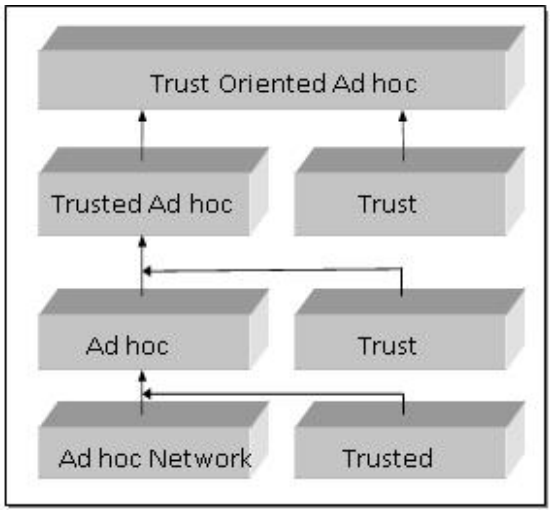

Figure 1: Abstract Representation of Trust oriented Ad hoc Network Framework

The trust model is intended to work as a trust service. This service is accountable for the trust evaluation, trust updation and trust propagation. The trust model encompassed the following components – Trust Configuration, Trust Assessment and Trust Appliance. The trust configuration in essence engrosses--characterizations of trust relationships, a range of trust categories, probable trust values. The trust assessment module is accountable for the trust evaluation. The trust appliance entailed the supply of trust values to the calling module. A trust value is a compute or quantification assigned by a source unit to its confidence in the trustworthiness of target unit. The trust value often signifies the prospect of a successful interaction, through which some desired outcome will be attained [2]. This trust service is called for in the situation where the recommendation from the rest of the nodes in the network is required by a node in the network. The trusts on recommendations are largely classified into two sorts- direct trust and indirect trust. The direct trust a node has on the basis of its own experience and indirect trust on the basis of other's node experience with the node in question. The alternatives available in the projected framework for trust evaluation purposes are

Risk or Context of the Operation/Application i.e. No Risk, Low Risk, Medium Risk, High Risk and Highest Risk application Global Trust or Local Trust.

Different or Same weights to recommendations

The risk or context is defined with the operation or application on run. The purpose of associating it is required as the trust requirement to allow or disallow any operation depends on the requirement of the context associated with the application e.g. Low risk applications are allowed even with the low value of trust and on the other hand high trust value is required for high risk applications. The preference of Global Trust and Local Trust is made available as many researchers either prefer global or local trust depending on their means of trust evaluation and the same notion is behind in presenting the weight option to recommendations.

The trust policy adopted to allow or discard an interaction on the basis of trust and the context of the application. As the policy varies and it is largely dependent on the area of application of the ad hoc network, so this is the constraint that it should be abstract from the rest of the environment.

3.2 The Approach

Nowadays, ontologies are used into an extensive range of applications. Besides the Semantic Web, they are even functional to knowledge management, content and document management,

information and model integration, etc [8]. The researchers who need to share information are provided with common vocabulary by the ontology [6]. The machine-interpretable descriptions of fundamental concepts in the domain and relations along with them are presented by it. The ontology structure the glossary by defining the central vocabulary and relations to model a domain. These glossaries are used in creating knowledge bases, developing services that function on knowledge bases and building system that are combination of these knowledge bases and services [10]. The process of developing ontology is analogous of the description of set of data and their composition for further programs to exercise. Each ontology O contains a set of concepts (classes) C and a set of properties P. A class is a collection of individuals and a property is a collection of relationships between individuals (and data). Individuals are the specific concepts. The relation between an individual to another individual is represented by property called an object property. The datatype property is specified to depict the mapping of an individual to a data literal. Every property has domain and range as the other mathematical functions. While both domain and range of object properties are ontology classes, the range of datatype properties are data literals such as integer, time, etc.

MANET is a multi-hop self-configuring network without any fixed infrastructure to communicate. Its topology changes dynamically and each node faces challenges from its processor, power, size, storage etc. Because the uncertainty exists in all of the evaluation factors, fuzzy theory is suitable for the evaluation of the uncertainty and the boundary.

In this paper, based on the classic fuzzy theory, the trust evaluation modeling and the dynamic routing protocols for MANET are introduced and verified. First, it has introduced the fuzzy trust evaluation model about each MANET node, including direct trust evaluation according to the features of the node and trust evaluation with fuzzy logic to model the node, the network and the environment. Second, the routing decision with fuzzy dynamic programming is discussed, focus on each step of the algorithm and how to make the multi-stage decision, then it represents the process to establish the fuzzy trusted DSR, and gives two optimization methods for FTDSR. The experiments use OPNET to simulate a MANET environment. The result has shown that FTDSR protocols can improve the network security, reduce the Packet Drop Ratio, and enhance the throughput with the acceptable End to End Delay.

In the future work, more optimization should be done to improve the efficiency of the FDP for the better use in the real MANET environments.

CONTRIBUTION

In SORT, to evaluate interactions and recommendations better, importance, recentness, and peer satisfaction parameters are considered. Recommender‟s trustworthiness and confidence about recommendation are considered when evaluating recommendations. Additionally, service and recommendation contexts are separated. This enabled us to measure trustworthiness in a wide variety of attack scenarios. Most trust models do not consider how interactions are rated and assume that a rating mechanism exists. In this study, we suggest an interaction rating mechanism on a file sharing application and consider many real-life parameters to make simulations more realistic.

A good peer uploads authentic files and gives fair recommendations. A malicious peer (attacker) performs both service and recommendation-based attacks. Four different attack behaviors are studied for malicious peers: naive, discriminatory, hypocritical, and oscillatory behaviours. A non-malicious network consists of only good peers. A malicious network contains both good and malicious peers. The satisfaction parameter is calculated based on following variables: The ratio of average bandwidth (AveBw) and agreed bandwidth (AgrBw) is a measure of reliability of an uploader in terms of bandwidth. The ratio of online (OnP) and offline (OffP) periods represents availability of an uploader.

Network architecture

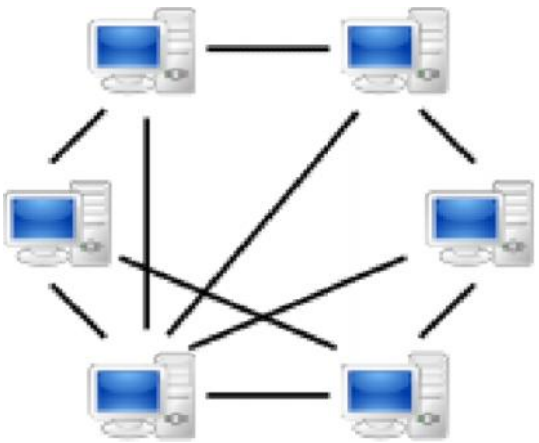

Fig b: General Structure of Peer to Peer networks

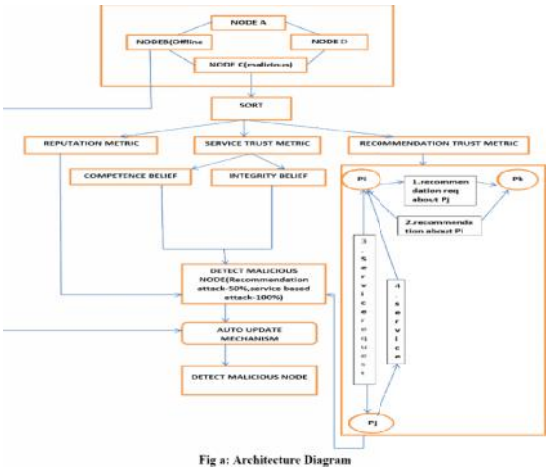

Fig a: Architecture Diagram

THE EIGER TRUST ALGORITHM IN P2P SYSTEM

It presented [3] a method to minimize the impact of malicious peers on the performance of a P2P system. The system computes a global trust value for a peer by calculating the left principal eigenvector of a matrix of normalized local trust values, thus taking into consideration the entire system's history with each single peer.

We also show how to carry out the computations in a scalable and distributed manner. In P2P simulations, using these trust values to bias download has shown to reduce the number of inauthentic files on the network under a variety of threat scenarios. Furthermore, rewarding highly reputable peers with better quality of service incents non-malicious peers to share more files and to self police their own file repository for inauthentic files.

Service-based attacks

Table shows the percentage of service-based attacks prevented by each trust calculation method. When a malicious peer uploads an infected/ inauthentic file, it is recorded as a service-based attack.

Number of attacks in No Trust method is considered as the base case to understand how many attacks can happen without using trust information. Then, number of attacks observed for each trust calculation method is compared with the base case to determine the percentage of attacks prevented. In the table, NoRQ and FloodRQ denote "No reputation query" and "Flood reputation query" methods, respectively.

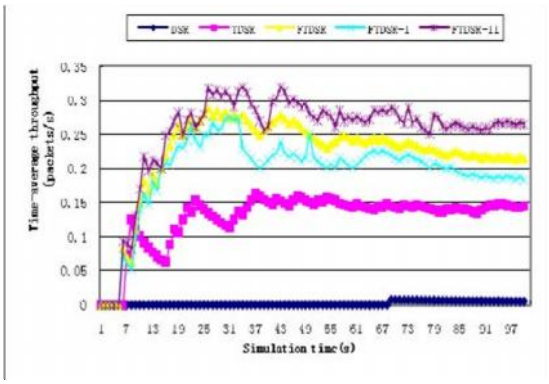

Figure8. Throughput with 12% malicious nodes

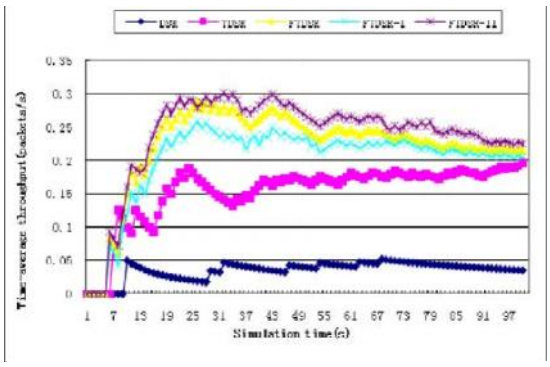

Figure9. Throughput with 25% malicious nodes

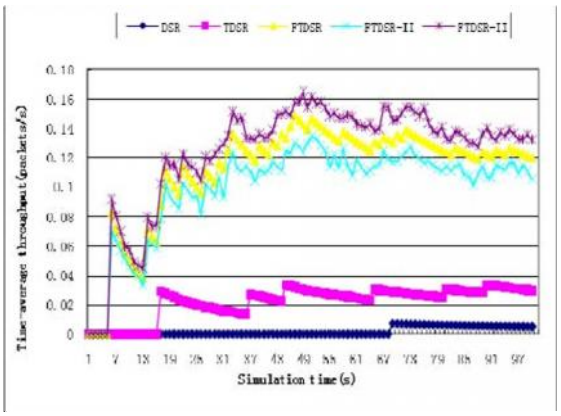

Figure10. Throughput with 35% malicious nodes

GOSSIP TRUST FOR FAST REPUTATION AGGREGATION

In P2P network, global reputation aggregation [5] is quite expensive when the network grows to reach millions of nodes. To our best knowledge, Gossip Trust offers the very first attempt to extend the gossip protocol for reputation aggregation in P2P networks without any structured overlay support.

CONCLUSION

SORT mitigated both service and recommendation-based attacks in most experiments. However, in

extremely malicious environments such as a 50 percent malicious network, collaborators can continue to disseminate large amount of misleading recommendations. Another issue about SORT is maintaining trust all over the network. These issues might be studied as a future work to extend the trust model. Using trust information does not solve all security problems in P2P systems but can enhance security and effectiveness of systems.

REFERENCES

[1] AhmetBurakCan and Bharat(2013),"A Self-Organizing Trust Model for Peer-to-Peer Systems"IEEETrans.Dependable and Secure Computing,vol 10,No.1.

[2] Aberer.K and Despotovic.Z(2001), „Managing Trust in a Peer-2-Peer Information System" Proc. 10th Intl Conf. Information and Knowledge Management (CIKM).

[3] Kamvar.S, Schlosser.M, and Garcia-Molina.H,(2003) „The (Eigentrust) Algorithm for Reputation Management in P2P Networks" Proc. 12th World Wide Web Conf. (WWW).

[4] SelcukA.A ,Uzun.E, and Pariente.M.R(2004), „A Reputation-Based Trust Management System for P2P Networks" Proc. IEEE/ACM Fourth Int"lSymp. Cluster Computing and the Grid (CCGRID).

[5] Zhou. R, Hwang. K, and Cai. M(2008), „Gossiptrust for Fast Reputation Aggregation in Peer-to-Peer Networks" IEEE Trans. Knowledge and Data Eng., vol. 20, no. 9.

[6] Abdul-Rahman. A and Hailes.S(2008), „Supporting Trust in Virtual Communities" Proc. 33rd Hawaii Int"l Conf. System Sciences (HICSS).

[7] Yu. B and Singh.M(2000), „A Social Mechanism of Reputation Management in Electronic Communities" Proc. Cooperative Information Agents (CIA)

AUTHORS:

DurgaBhavani.Kis a student of Computer Science Engineering from G.V.R&S College of Engineering and Technology ,Presently pursuing M.Tech (CSE) from this college. She received M.C.A from IGNOU (INDIRA GANDHI NATIONAL OPEN UNIVERSITY) in the year Of 2009.

Rajesh.A is a Assistant Professor of G.V.R&S College of Engineering & Technology ,GUNTUR .He received M.Tech in Computer Science Engineering from GITAM University. He gained 2years Experience on Teaching . He is a good Researcher in Java, Cryptography , Computer Networks. He attended Various National and International Workshops and Conferences.