

Private Network forming Routing Protocol for Adhoc Networks

Nagesh U.B

Department of Information Engineering
Vivekananda College of Engineering and Technology
Puttur, India
nageshub.isc@vcetputtur.ac.in

Abstract—The lack of infrastructure in mobile Ad Hoc networks has posed a lot of opportunities for the researches in relaying the data to destination. Mobility of nodes in such an environment offers many challenges due to link failures. Different routing protocols have considered specific aspect of such a network considerably the energy consumption, bandwidth, geographic location etc. for efficiently routing the packets. If security aspect is considered in such a protocol, they will be concentrating mainly on effect of different type attacks. In this paper a novel approach for securely routing the packets is proposed to support volatile nature of the network. Being membership history count the foundation, the routing decision is made according to the number of registrations made by a node with the source node and by establishing a private trusted path of its own to securely route the packets. The protocol proposed here works in a safe manner to ensure data security and end to end connectivity. The results evaluated in the simulation reveal that, the proposed algorithm provides significant improvement in terms of delivery ratio and level of security.

Keywords—MANET; Membership History; Network Stability; Security factor; Mobility

I. INTRODUCTION

Mobile Adhoc Networks (MANET) and its applications are widely used in today's IOT's and WSN's where in the mobility of nodes will drastically effect the infrastructure less network parameters like, end-to-end connectivity, delivery ratio, stability and energy consumption. The volatile nature of the node locations mainly lead to link failures which in turn may result in network degradation by affecting the performance of routing layer of TCP/IP stack in microkernel based lightweight operating systems like Contiki [1].

The inhabitant sensing nodes in the network are very sensitive to scarce resources. Managing these vital components has become bottleneck to the underlying operating system running on low powered (16 bit) controllers of the node. The node movement throughout the time in the network is more prone to security vulnerabilities, as data rich nodes are passes near an eavesdropping node. So finding a trusted path from source to data collection centers is the major challenge in such infrastructure less networks.

In this paper we propose an effective approach of path selection from source to aggregator where in route failure and

link breakage can be considerably reduced. The algorithm follows a membership history based approach which can be another factor for identifying liveliness in the network like sequence number and distance to every other node. Furthermore this strategy is aimed to achieve more security in the route by employing hash distribution scheme which is entirely dependent on the membership history value of a node.

The reminder of this paper is organized as follows. Section II gives a brief introduction on past researches in the field of routing for Ad Hoc networks and WSN. Section III provides a picture of network model and simulation scenario we are using. Section IV presents the working flow of the proposed protocol. Section V presents the performance evaluation. Finally Section VI concludes this paper with summary.

II. RELATED WORKS

There are many researches on routing strategies for Ad Hoc network and one of its verities, the Wireless Sensor Networks. Here some of the major investigations which are suitable for both these categories are presented.

Data gathering and dropping it in local aggregators can be achieved in different ways such as by local storage using collaborative storage mechanisms (CBSM) [2], where data collected will be stored locally in a cluster based on the residual energy and importance of gathered data. But the freshness of data may override the storage capacity in nodes which leads to data loss.

However if the carrying of data to destination is the alternative solution, there are different strategies classified as reactive and proactive. The conventional proactive routing methods like DSDV and CGSR uses one of the parameter of the network to find out the path. In DSDV [3], the Bellman-Ford algorithm of finding shortest next hop node along with a destination sequence number is used to update a table entry and in turn to identify the most recent and best path in the network. Where as in CGSR [4], the available nodes are organized into clusters and by electing a cluster head according to LCC algorithm, the member nodes will communicate to the head by spreading codes on a CDMA system so as to carry the data packets from registered members of a cluster to the sink node.

In reactive routing protocols like TORA [5], it makes use of link reversal techniques to provide loop free paths to the

International Journal of Computer Science and Mobile Computing



A Monthly Journal of Computer Science and Information Technology

ISSN 2320-088X
IMPACT FACTOR: 5.258

IJCSMC, Vol. 5, Issue. 4, April 2016, pg.529 – 533

DATA DEDUPLICATION FOR NON SECURE TEXT AND DOC FILES IN CLOUD

Mallika D K G¹, Prof. Sudheer Shetty²

¹Department of Computer Science & Engineering, Sahyadri College of Engineering & Management,
Mangaluru, Karnataka, India

²Department of Computer Science & Engineering, Sahyadri College of Engineering & Management,
Mangaluru, Karnataka, India

¹ mallika.mtechscs14@sahyadri.edu.in; ² sudheer.cs@sahyadri.edu.in

Abstract— Information when interpreted we get data. Data about this data is called Metadata. For example: File consists of Information. Therefore File is data. And details like File name, file size etc. are Metadata. Data is stored in storage spaces. Currently the most dominantly used storage method is Cloud Storage. There has been a large increase in the usage of the Internet in the past few years. The Cloud has played a huge role in it. Traditional Data systems are slowly fading away and Cloud storage system is falling into place. One of the issues Cloud storage is facing is data redundancy. To solve this issue one should achieve Data Deduplication. Data Deduplication is a concept where unique data or a particular /similar pattern of data is identified and stored. This is then compared to other data available in the system. If a match is found, then the data is replaced by a link or a reference to the stored data.

Keywords— cloud computing, cloud storage, deduplication.

I. INTRODUCTION

Cloud computing is a platform that provides seemingly unlimited “virtualized” resources to users across the whole Internet, while hiding platform and implementation details. Highly available storage and massively parallel computing resources are provided at relatively low costs. Prevalent use of cloud, an increasing amount of data is being stored and shared by users with specified privileges, which define the access rights of the data stored. In short we can say that cloud computing is computing as a business model that provide computing resources as a service on demand to customers over the Internet. [3]

Sudheer
H.O.D.



Privacy Preserving Data Mining in Big Data by using K-means Clustering Algorithm

Anisha K¹, **Sudheer Shetty²**

¹Department of Computer Science & Engineering, Sahyadri College of Engineering & Management, Mangaluru, Karnataka, India

²Department of Computer Science & Engineering, Sahyadri College of Engineering & Management, Mangaluru, Karnataka, India

¹ anishakrishn@gmail.com; ² sudheer.cs@sahyadri.edu.in

Abstract— In current days there is a huge growth in information accumulation because of the advancement in the field of data innovation. It is extremely crucial that the information gets uncovered when the associations begin sharing the information for the mining procedure and protection might be ruptured. Privacy preserving methods gives another track to tackle this issue. The point of Privacy preserving data mining is the extraction of appropriate information from bulk quantity of advanced information while ensuring in the meantime delicate data. Four diverse sorts of clients required in data mining applications, to be specific, data provider, data collector, data miner, and decision maker. In this paper, we talk about the privacy preserving technique utilized for data collector while performing data mining procedure and we have broke down the utilization of normalization techniques in accomplishing privacy and depict an estimated calculation taking into account k- means. It is a novel technique for huge information examination which is quick, versatile and has high precision.

Keywords— Big data, Privacy preserving data mining, Z-Score normalization, K-means clustering algorithm, Centroid

I. INTRODUCTION

Today is the period of Google. The thing which is unfamiliar for us, we Google it, and in divisions of seconds we get the quantity of connections thus. This Big Data is the same thing than out general term information. Simply huge is a watchword utilized with the information to recognize the gathered datasets because of their huge size and complication. We can't organize them with our present systems or data mining programming instruments. The information gathering has become a great deal and is away from the capacity of generally utilized programming apparatuses to catch, organize, and prepare inside a fair time. The Big Data is

"Humps and Pothole Detection and Alerting System for Safe Journey"

Shubhada Vital Poojary¹, Rashmi M², **Sudheer Shetty³**

¹PG scholar, Dept. of Computer science and Engineering, SCEM, Mangalore

²UG student, Dept. of Information science and Engineering, SDMIT, Ujire

³Associate Professor, Dept. of Computer science & Engineering, SCEM, Mangalore

Abstract - Smart phones today are equipped with inbuilt sensors that give safety enhancement to the drivers on road. The accelerometer and a GPS tracking system of smart phone can give assistance to the driver while travelling. In this paper, the accelerometer of an Android based smart phone is used to record motions generated while passing the obstacles like humps and potholes. GPS is also used to find the location of obstacles on the road. This information will be stored on the server and will generate alert message to the drivers before 300 meters before the point of obstacles. With real time analysis and alerts of these factors, we can increase a driver's overall awareness to maximize safety. Google Earth is used to create road condition maps using GPS coordinates. We propose an early warning system that uses a smartphone based application to alert the driver in advance when the vehicle is approaching the obstacles like humps, rough roads or potholes. In addition, the application also generates the report on the condition of the road which will be helpful for the government sector to repair the road.

Key Words: Accelerometer, GPS, Google Map.

1. INTRODUCTION

In Today's life [1] we are focused on arriving at our destination as quickly as possible. Car manufacturers are focused on passive approach, e.g., airbags, seat belts, and antilock brakes, lane departure warning system and collision avoidance systems. But we are not always aware of all the dangerous conditions that are experienced while operating an automobile. Factors such as sudden vehicle fall and hazardous road conditions such as bumps, potholes etc. which often leads to accidents of vehicles.

Roads in India normally have speed breakers [2] so that the vehicle's speed can be controlled to avoid accidents. However, these speed breakers are unevenly

distributed with uneven and unscientific heights. Potholes, formed due to heavy rains and movement of heavy vehicles, also become a major reason for traumatic accidents and loss of human lives. According to the survey report "Road Accidents in India, 2011", by the ministry of road transport and highways, a total of 1,42,485 people had lost their lives due to fatal road accidents.

This paper suggests automated approach for detecting potholes or humps using smartphones embedded with numerous sensors such as accelerometers, Global Positioning Systems (GPSs). This proposal intends to describe the road condition application which aims in detecting and alerting the drivers about the obstacles on the road. Here we make use of accelerometer which is used to detect potholes, rough roads as well as humps. And the GPS is used to find the location of obstacle on the road. This data is stored in the server. When the user will be travelling on the road wherever there is an obstacle, an alert message will be generated and also shows the obstacle in the red mark in the map. Data in the server is updated by collecting it from every user.

2. METHODOLOGY

The author in the paper [1] attempts to find a way to match the local map with actual GPS traces from mobile phones. It has been found that method can be used to obtain 100% map matching, as it ensures matching by comparing the GPS data to a set of pre-determined check points. Monitoring road and traffic conditions is a major problem.

This paper proposed a method that uses sensors present on smartphones. This sensor distinguishes the bumpy road from the smooth one. This can be used to detect speed breakers, potholes and rough surface and other obstacles on the road.

Extracting accurate answers for users query to enhance user satisfaction

Kiran B. Malagi

*Department of Computer Science and Engineering
K.L.E. Institute of Technology, Hubli, Karnataka, India*

Veena M.

Abstract- Accurate Answer Retrieval System which provides platform for people with diverse background to share information or knowledge has become an increasingly popular research topic recently. It provides free environment where people can voluntarily ask and answer questions. Unlike the tradition automatic information retrieval this site allows peer to peer interactions and thereby answers from a large community would be more personalized and specific. Now there needs to be drift, where instead of people responding to some specific question, let the system itself answer. Unlike information retrieval systems, which return whole document or larger sections thereof, question answering systems are designed to deliver much more focused answers. In this paper we propose a novel methodology for the Automatic and accurate answer retrieval system.

Keywords –RBA- Rule based Answer Aggregation, IR- Information Retrieval

I. INTRODUCTION

Day by day internet is becoming so big that any information can be retrieved from the internet, based on the questions we ask. When we are in search of some information, we expect the data provided by the internet to be precise and accurate. But in many cases it doesn't happen. User has to satisfy himself with the answer required by him by browsing the links provided by the search engines. The user always expects the concise and precise answer to his query. When these types of concise answers are provided by the websites, users are satisfied with the answers and confidence on the site is also increased. The time of the user is also saved by not digging into many links with irrelevant data. Question answering systems are intended to provide accurate information in reply to a query. An open domain question answering system should be able to answer a question written in natural language, for a user friendly interaction for humans.

"Do the answer given by the World Wide Web is trustable?", Unfortunately the Answer is "No". We have no certification to prove that the facts provided by the World Wide Web is right. Even worse, different websites often provide conflicting information, as shown in the following example.

Suppose a user is interested to know the height of Eiffel Tower and he search this in yahoo.com by giving query "What is the height of Eiffel Tower?" Among the top 20 results, one he or she will find the following facts: five websites say 324 meters, four websites say 300 meters, one says 312 meters and another one says 317.96 meters. Which answer should the user trust?. The trustworthiness problem of the Web has been realized by today's Internet users. According to a survey on the credibility of websites conducted by Princeton Survey Research in 2005, 54 percent of Internet users trust news websites at least most of time, while this ratio is only 26 percent for websites that offer products for sale and is merely 12 percent for blogs.

There have been many studies on ranking web pages according to authority (or popularity) based on hyperlinks. The most influential studies are Authority-Hub analysis, and PageRank, which lead to Google.com. However, does authority lead to accuracy of information? The answer is unfortunately "NO". Top-ranked websites are usually the most popular ones. However, popularity does not mean accuracy. For example, according to our experiments, the bookstores ranked on top by Google (Barnes & Noble and Powell's books) contain many errors on