

**Mathematical Contest in Modeling and Interdisciplinary Contest in Modeling
Summaries, Pictures and Results
Simpson College
2004**

Betting Against the L_{oops} A_{rches} W_{horls} ...What are the Odds?
by

Teresa Kreykes, Ashley Bennett and Anita Zahs
Meritorious

Are fingerprints truly unique? What are the odds of fingerprint misidentification? How do the odds of fingerprint misidentification differ from the odds of DNA misidentification? Fingerprint analysis can be used to determine if fingerprints are really unique. After a few assumptions, we set out to find the probability that two fingerprints would be the same. We found that there are eight types of fingerprints, which are further classified by the ten types of minutiae. To find a positive identification, there must be a minimum of at least eight matches of minutiae type and location on two separate fingerprints. Although eight matches can be considered a positive match, it is more likely that at least twelve would be used.

Our model used probability to account for three factors of fingerprinting; the minutiae location, the classification of minutiae, and the types of fingerprints. So, we collected actual fingerprints and use this data to assist in the determining the number of possible unique fingerprints using twelve and fourteen minutiae locations. We compared the number of unique fingerprints to the world population which is estimated at seven billion. Using twelve minutiae locations, we found that the odds were seven in three billion that misidentification would occur and one in ninety-three trillion using fourteen locations.

Finally, we compared the odds of fingerprint misidentification with the odds of DNA misidentification. We found that the chance of DNA misidentification – one in 10^{30} (Innes 63) – is much less than that of fingerprint misidentification. This is due to the larger number of factors that can be accounted for in DNA mapping.

Have Fun in No Time
by

Shikha Basnet, Maya Hristakeva and Lwanda Manxodidi
Meritorious

To overcome the problem of having long lines of people waiting to get on their favorite rides in the amusement parks, we are proposing a remake of the existing QuickPass system. The existing quickpass machine issues QuickPasses at random, such that a person who gets a QuickPass earlier than the other might get a return time that is later than that of a person who got the QuickPass later. Well, the system we developed issues people QuickPasses in the order of the succeeding times they come to the kiosk.

This system is especially targeted for popular rides where numbers of people is almost uncontrollable. Our system reduces the long lines by evenly distributing people throughout the day. We have derived and theoretically tested an outstanding set of formulas to work with the regulation of the crowds. The model is designed in such a way that it works at a wider range of conditions. We do not overlook the fact that the use of the QuickPass system will not always work best for everyone, since the returning time could be four hours later from the time one obtains a QuickPass. So, our model has two parts that work



Maya, Lwanda and Shikha making good use of caffeine while they design a quick pass system for amusement parks.

coordinately. One part includes a set of equations that distribute and regulate people with QuickPasses, while the other part works with regulating people without QuickPasses.

The system is set to shift a one hour interval by some number after a certain number of people get the QuickPasses. The only problem is that if the certain number of people necessary for the interval shift is not reached before the lower bound of the following interval, then the following individual would be issued a QuickPass less than an hour long. The system we developed uses a triangular relationship between the distribution intervals, the number of people obtaining the QuickPasses and the current time vs. lower bound of a given interval. The trick on how these are interrelated is clearly disclosed towards the end of "Design and Application of the Model" section.

Even though our scheme does not reduce the waiting time to zero percent, it does a great job reducing the waiting time to negligibly short periods. An optimist would even say the time is reduced to none, while a pessimist would be left with nothing to say besides enjoying the ride.



Scott, Greg and Micah build pyramid models of pop cans when on break from their probability calculations.

Thumbs are not so Dumb

by

Greg Elliott, Scott Roth and Micah Mueller
Honorable Mention

Our problem was to evaluate the uniqueness of thumbprints. We developed two models which analyzed the probability of matching two random thumbprints. We then compared our results to the accuracy of DNA identification and found thumbprints to be more accurate than DNA. With our results from our models we are able to approximate the probability of the existence of non-unique thumbprints.

In model one we use the minutiae point locations to determine the probability of matching random thumbprints.

We use a hypergeometric distribution with the discrete random variable X which counts the number corresponding points between the input and the sample. We evaluated this model by comparing our results to that of DNA accuracy.

In an attempt to improve our model we decided to also consider an additional feature of the minutiae other than location. The second model was a more accurate model and is more closely related to current methods for fingerprint analysis. We improved our results significantly through the addition of a negative binomial distribution to our model in which Y is a discrete random variable that will count the r^{th} success. The second model greatly improves the results proving thumbprint identification is far more precise than DNA identification.

Using data from both of our models we came to the conclusion that all fingerprints are unique, and have been for every person who has lived. We do not rule out the possibility of a duplicate thumbprint, but we do find it to be very unlikely.

Enforcing Network Security

by

Kumud Poudel, Prakash Kayastha and Anuj Kachapati
Successful Participant

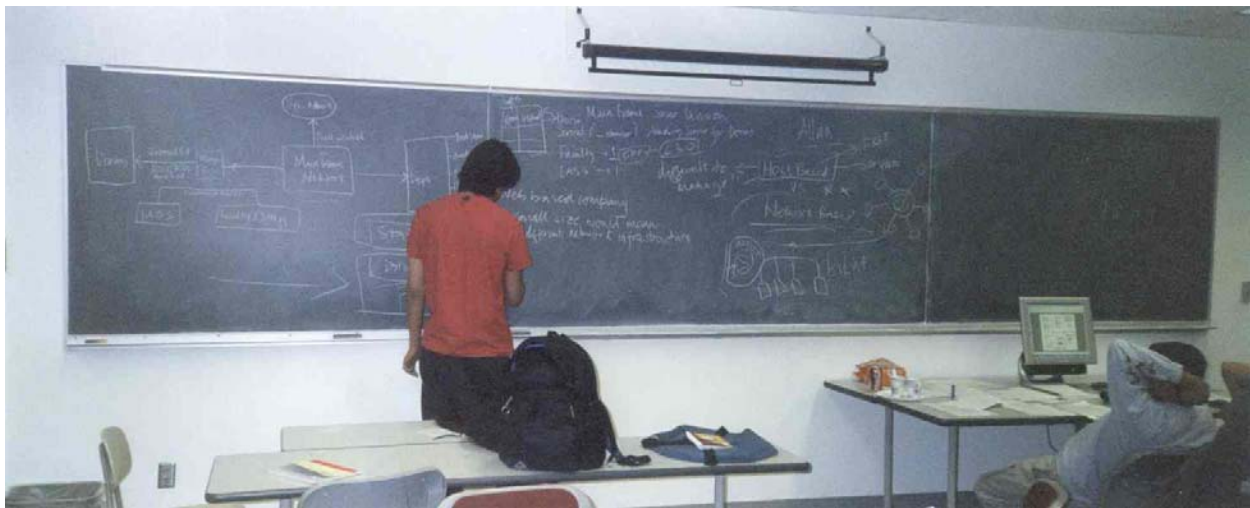
The proposed university network provides an excellent blend of enhanced security features and equally reliable, stable and accessible network connection with a well balanced combination of the technologies and policies. The projected centrally oriented network will facilitate efficiency and better



Kumud, Prakash and Anuj in the middle of a marathon session to design a university network system.

managerial capabilities in a large scale organization. Division of network in VLAN (Virtual LAN) will enable administrators to enforce different security levels. The priority is to restrict accessibility and secure security vulnerabilities. The set of Mainframe servers will ensure faster connection speeds. Faculty/Staff accounts present on server are password protected to maintain confidentiality and technologies like Network Based Firewall, Network based Anti- Virus, SPAM Filter, Network Based Intrusion Detection System, Network Based Vulnerability Scanning and Data Redundancy is employed to protect data flowing through the network and that present in the server. The model supports wireless connection to the network with wireless appliances enabling students to access information at their ease thus improving user productivity. The total cost estimate for the proposed model is \$2,050,800.

On the flip side, there is no practical solution to examine our model unless the network is produced or replicated. Also enhanced level of security and scrutiny against intruders, attacks and attackers would sufficiently restrict student's accessible capabilities. Our disadvantages have equally poised our position like our advantages have favored it, concluding there is no perfect solution in a real life application.



Anuj works at the board while Prakash and Kumud kick back and give advice.

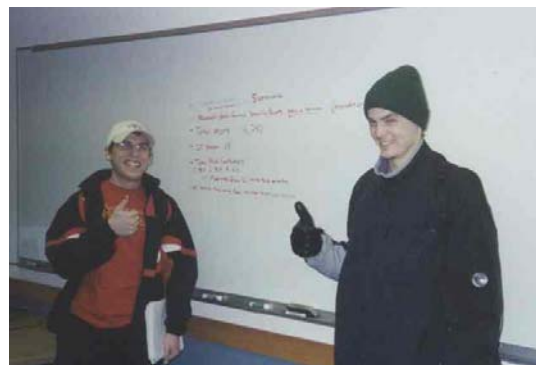
Clever Conclusions for Complex Connections

by

Jean Clipperton, Kris Langgaard and Tony Breitbach
Successful Participant

Rite-On Consulting has been selected to create a network for a soon-to-be-created university. As the lead consultants chosen by Rite-On, we have created a model for the university, as well as chosen several policies and technologies to implement on the network. Our initial task was to create a university-specific model tailored to the university's potential needs.

Once we accomplished this, we altered the model to make it adaptable to almost any situation, not just schools. To do this, we implemented ratios for servers and ratios of system administrators that would allow for customization as well as the ability to adjust for expansion of the network. We also allowed servers for web sites and



Tony and Kris show some enthusiasm about their fitness model for network systems.

secure data (to isolate different levels of access-websites have the most users while secure data will have very few who need access). We also wanted to ensure that if the web server was compromised, the rest of the network could be secure.

After we had our network laid out, we could then determine what services it might need. Our policies could then go on to form the backbone of our network. All technology must support/be supported by these policies. We also wanted to have an unbiased, objective procedure to select which specific products to install. To do this, we evaluated which features (confidentiality (C), integrity (I), availability (A), user productivity (P), and variability (V) of product ratings) would best benefit a university. We then compared these to the percentage share each feature (confidentiality, integrity, and availability) had in the opportunity costs of not having any policies implemented at all. Between these two methods, we found the relative importance for the features and gave them a percentage rating (for example, "C" had .3, 30%, while "A" had only 0.2, or 20%). These values were incorporated into an equation which could be used to compare individual products with respect to how well they could provide desired features. We then divided the first year's cost by the result of the formula to learn the weighted cost per percentage point.

Our model has some sensitivity, which is positive; after all we want small changes in our desires for features to change which products we select when we adjust the formula. We had to make several assumptions in the creation of our model. From these assumptions we could then proceed to the use of our formula. Some weaknesses to our model are that we couldn't be certain of some costs and could not include them. We also couldn't be certain that the university's needs wouldn't change in the future, making some products initially desirable, but then less relevant. Keeping this in mind, we calculated all costs with the same numbers (of IT personnel, users, servers, etc) so that the rankings could be compared to each other. We also sought to allow for flexibility of the model, so that if the university wanted to change the weights, it could without substantial 'head-scratching.' Knowing that the key to a model is its ability to be adapted, we also developed ratios so that it could be adapted or applied to larger or smaller networks.

All in all, we feel that we have created a malleable model with many manners of mobilization.



Amber and Shristi present their work in the Modeling Contest at the 2004 Midwest Undergraduate Mathematics Symposium.

Thumbprints

by

Shristi Upreti, Aye Win and Amber Woodley
Successful Participant

In this paper we have created a simple mathematical model that generates a number of different possible thumbprints. We have examined in depth the large number of variations produced by the different minutiae. We also briefly considered the effect of the basic types of fingerprints and the degree of pattern rotation on the total number of possibilities. Then we took the probability of having one possible thumbprint based on the outcome space of the total possible thumbprints. Because there are so many different thumbprints, the probability that two people have the same print is so low that it is practically impossible. Therefore the odds of misidentification by clear fingerprints, assuming the highest quality testing systems for fingerprints, are very low. We have compared the odds of misidentification by fingerprint testing according to our model to the odds of misidentification by DNA.