Ascertaining Trust of Information Transmitted During a Disaster

Yunus Yusoff[1], Asmidar Abu Bakar[1], Norshakirah Aziz[2], Roslan Ismail[1], Ramona Ramli[1]
[1]Center of Information & Network Security,
College of Information Technology,
Universiti Tenaga Nasional, Malaysia.
[2]Universiti Teknologi Petronas, Malaysia.
yunusy@uniten.edu.my

***Abstract*—During a disaster, especially at the beginning, a huge amount of information is being communicated by the victims to the authority/rescuer. With the presence of ICT applications and smartphone devices, the communications can be carried out easily. However, these ease of communication created one critical issue that is the reliability of the transmitted information. One of the potential solutions is to use trust algorithm to identify the trusted information. The trust engine can help to filter and verify the reliability and validity of the transmitted information. With the ability to identify trusted information, the authority and rescuer would be able to channel and prioritize their rescue efforts to the more critical disaster areas. A prototype, running on Android platform and Web server, was developed to demonstrate the proposed solution.**

***Index Terms*—Threshold; Android; Channel; Communication.**

I. Introduction

During the event of a disaster, dissemination and sharing of information such as location and situation of the disaster are very much sought after. With the presence of ICT applications and smartphone devices, dissemination and sharing of information can be carried out with ease. Everybody can post and share information about the disaster they are currently experiencing. Although this freely sharing of information is good, it does give rise to one critical issue. Can we trust and verify the information obtained from these technologies? How do we ensure that the information being transmitted is genuine? Based on our interviews with various parties involved in the recent (2015) big flood in Kelantan, Malaysia, it was revealed that extremely huge numbers of messages were received by the rescue centers. However, the rescue centers did not have the ability to ascertain the trust of the transmitted information.

It was also discovered that a number of flood victims did make up the stories to make it look as though they are in a very critical situation, although the truth is otherwise. In order for help to be sent immediately, people may resort to fabricated information so as to make the authority believe that they are in great danger.

In gathering data from users, crowd sourcing is considered as the most suitable approach. This term was coined by Jeff Howe [1] and further refined by other researchers [2]. This approach allows users to give their feedback easily as in data collected in Haiti earthquake in 2010 [3, 4]. This approach was also adopted in other well-known disasters.

The three famous disasters that shocked the world are the Queensland & Australian Flood, the Christchurch Earthquake and the Japan Earthquake [5]. The Queensland & Australian Flood [6], occurred from December 2010 to March 2011, has caused massive loss of lives and billions of dollars. The crowd sourcing application was used to develop the crisis map [7] which was based on the information gathered from the victims. In the Christchurch Earthquake, which occurred in February 2011, the crisis map was also launched which was based on the information obtained from the victims. The Japan Earthquake, which occurred in March 2011, has caused large areas of northern Japan to be completely wiped out. Again, information gathered from the victims was used to identify the critical disaster areas.

Based on the abovementioned scenarios and our interviews with the victim of Kelantan flood, the rescue centres were lacking the necessary methods to check for the trustworthiness of the data captured from the victims. As such, all incoming data (raw data) are always considered as trustable. It is always possible that there exists unreliable, untrusted or fake data, among the huge amount of data being captured form the public. Should the authority acted on this untrusted data, their effort to save the real victims may be hindered.

The objective of this study is to formulate an algorithm to assist the authority in the identification of trusted information gathered from the public. The implementation of the algorithm will enable the rescue personnel to direct their rescue efforts to the genuine disaster areas. The assumption for this study is that the information is transmitted electronically via smart phones that is equipped with Global Position System (GPS) features.

II. Trust Values and Thresholds

Trust is a crucial factor for human interaction due to the fact that our everyday lives are affected by the decision made based on trust on someone or something. Studies on trust span across many areas, from social psychology work by Deutsch, sociology by Luhmann, economics by Hart [8,9] and from mathematic point of view by Gambetta [10]. All these works discuss trust as part of a society and society depends on trust for its appearance [9]. In the computing world, trust can be thought of as a relationship between a trustor and a trustee. A trustor is a subject that trusts a target entity while a trustee is the entity being trusted [11].

The definition of trust depends on what that trust is intended for [12]. A common definition of trust are defined by many dictionaries as a notion of confidence, dependence, belief, faith, hope, expectations and reliance on the integrity, ability or a character of a person or thing [13]. The variety of terms indicated that trust definition is very ambiguous and depends much on the context it is being applied. It is also perceived that trust is a subjective notion; meaning that every individual decides whether to trust based on the evidence available [13, 14].

Many researchers classified trust values in discrete range, 0 to 1 [3, 15, 16]. These researchers categorized trust values to the appropriate trust level such as low, middle and high. It was discovered that the value 0.5 is commonly used as the initial value as stated in [15, 17]. The initial trust value represents a situation between trust and distrust, which can be presented in term of opinion. An opinion about something or someone is given due to lack of information collected while making decisions [18].

Previous works also indicated that higher trust value is required to access sensitive data or information or to show how trusted the information is. A value from 0.7 onwards has been used to represent trust and higher trust, while values ranging from 0.00 to 0.49 have been allocated as no trust in most of the works presented. The comparisons between all these works are presented in Table 1 below. The notation N.A in this table stands for not applicable

Table 1
Trust threshold and initial values by previous researchers

Authors	Trust threshold for high trust	Initial trust value
Almanarez et al.,(2004) [17]	>= 0.75	0.5
Jameel et al.,(2005) [20]	>= 0.50	NA
M.Haque et al.,(2007) [18]	>= 0.80	0.5
Giang et al.,(2007) [21]	>= 0.70	>= 0.55
Lang et al.,(2007) [22]	>= 0.85	NA

For the purpose of this study, we adopt the values as shown in Table 1 to determine the initial and high trust value threshold. We have chosen to adopt 0.5 as the initial trust value and 0.7 as the threshold for high trust value. The value of 0.7 as the threshold of high trust was derived by taking the average of the threshold values as presented in Table 1.

III. PROPOSED TRUST ASSESSMENTS

Taking into consideration of the Kelantan big flood, it was discovered that the GPS location and user information are needed in order to ascertain the trust of the transmitted information. Figure 2 describe the possible sources of information that can serve as parameters to calculate trust in disaster (flooding) situation.

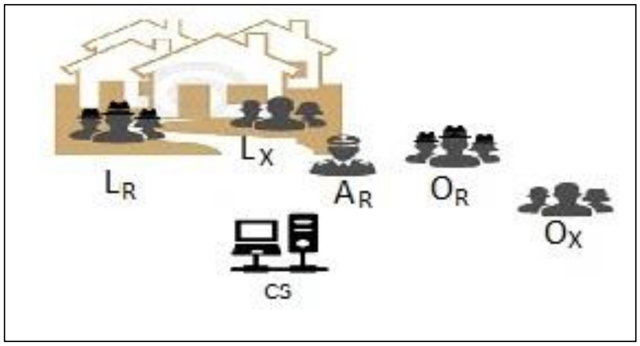


Figure 2: Available users

In Figure 2, the possible users available during the flooding scenario are displayed. These users are categorized based on their physical location and whether they have registered with the rescue center. Local users are those located within the disaster area and Outside users are those outside the disaster area. Description of each category of users is provided in Table 2. Each type of user is assigned with a trust value based on their level of reliability. The more reliable the user, the higher the trust value will be. In Figure 2 & Table 2, the most reliable user is Ar (Registered Authority) and highest trust value of 1.0 is assigned to them. Refer to Table 2 for trust values for the other category of users.

The registered authority (Ar) has a full trust value since they are the authorized personnel to handle the rescue operation. As for the local user, a high trust value (0.7 & above) [6] is assigned to them since they are currently experiencing the disaster.

Table 2
Types of users

User Type	Explanation	Trust Value
Lr	Local Registered User	0.8
Lx	Local not Registered User	0.7
Or	Outside(non-local) Registered User	0.6
Ox	Outside(non-local) not Registered User	0.5
Ar	Authority Registered User	1.0

We propose the following formula for calculating the trust of information received from various individuals affected by flood situation. An initial value of 0.5 is initially assigned to all areas. Whenever a user reports a flooding in a respective area, the trust value (meaning the possibility of flood in that area) will be increased according. Likewise, if a user report that an area is not flooded, the trust value of that area will be reduced accordingly.

$$NATV = CATV + (UTV * AHTV) \text{ or } NATV = CATV - (UTV * AHTV)$$

Where,
NATV = New Area Trust Value
CATV= Current Area Trust Value
UTV = User Trust Value
AHTV = Area History Trust Value
+, if reported flooding, **-,** if reported not flooding

NATV refer to the new area trust value. Whenever a report of flooding or not flooding is received, the NATV is calculated taking into account of the type of user who reported and the current trust value of that area. CATV refers to the current trust value of the respective area.

UTV refers to the trust value of the user. Different user is assigned with different trust value. Local registered users are given a high trust value of 0.8, since they are registered and currently in the disaster area. Local users, but not registered is given a slightly lower trust value of 0.7, since the authority would not be able to immediately ascertain their identities. The same concept is used for outside users whereby Outside but registered user is given 0.6 and Outside but did not register is given 0.5 trust value. AHTV refers to the historical flood situation for the disaster area. There are three historical flood situations namely, frequently flooded, seldom flooded and rarely flooded of which is assigned 0.03, 0.02 and 0.01 trust value respectively. The value for each situation is assigned to ensure that the overall trust value would increase linearly instead of exponentially.

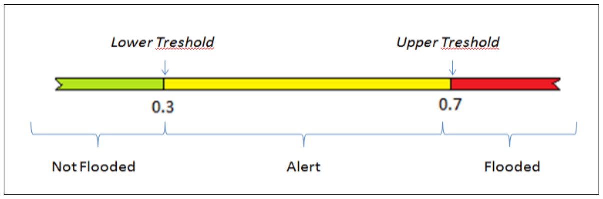


Figure 3: Threshold values

Based on literature review (as discussed in Section 3), we have adopted a value of 0.7 as a threshold for high trust value. The distance between 0.7 to 1.0 is 0.3. Using the similar distance from 0, we have opted to define 0.3 as the threshold for not flooded. Trust values between 0.3 and 0.7 indicate an Alert level for the particular area. Areas with 0.7 & above trust values, indicates that they are experiencing serious flooding and need immediate attention.

IV. SIMULATIONS

Users will send information to the centralized support center via smartphone that transmits their GPS coordinates and other relevant data. The central server will calculate the new trust value of the respective area. The new trust value will be compared against the threshold. A map will be displayed to show the current flood status of the affected areas.

Scenario 1 (Figure 5) refers to the situation whereby a local registered user reported a “flooded” situation. The trust value of that area should be increased accordingly. The Current Area Trust Value(CATV) is assumed to be 0.5 (initial value) and the Area History Trust Value (AHTV) is assumed as 0.03 (always flooded).The information provided by the user is considered as trustable and reliable since the user is registered and located within the disaster area. The NATV for the area is calculated as below:

NATV = CATV + (UTV * AHTV) = 0.5 + (0.8 * 0.03) = 0.524

The current area trust value will be changed from 0.5 to 0.524 (Figure 6). The area is now considered to be under alert.

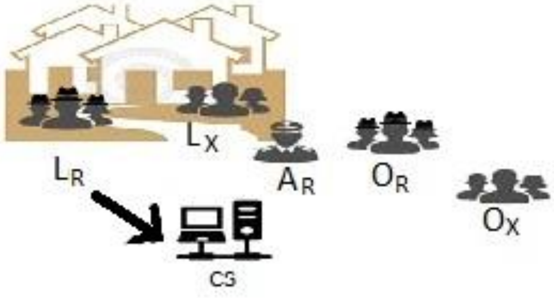


Figure 5: Scenario 1

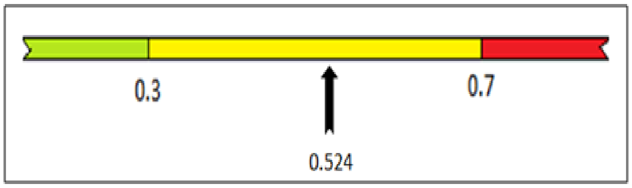


Figure 6: Trust value for Scenario 1

Scenario 2 (Figure 7) refers to the situation whereby a local non registered user reported a “Not flooded” situation. The trust value of that area should be decreased accordingly. The Current Area Trust Value(CATV) is assumed to be 0.5 (initial value) and the Area History Trust Value (AHTV) is assumed as 0.03 (always flooded).The information provided by the user is considered as slightly less trustable since the user is registered and located within the disaster area. The NATV for the area is calculated as below:

NATV = CATV - (UTV * AHTV) = 0.5 - (0.7 * 0.03) = 0.479

The current area trust value will be changed from 0.5 to 0.479 (Figure 8). The area is still considered to be under alert as the trust value is still between 0.3 and 0.7

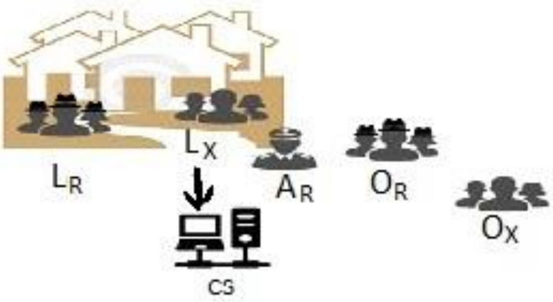


Figure 7: Scenario 2

The above simulations correctly demonstrate the working of the trust algorithm. A message with “flooding” status does increase the trust level of an area, depicting higher possibility of flooding. A message with “Not flooding” status does decease the trust level of an area, depicting lower possibility of flooding.

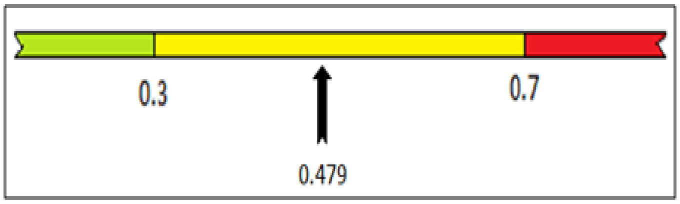
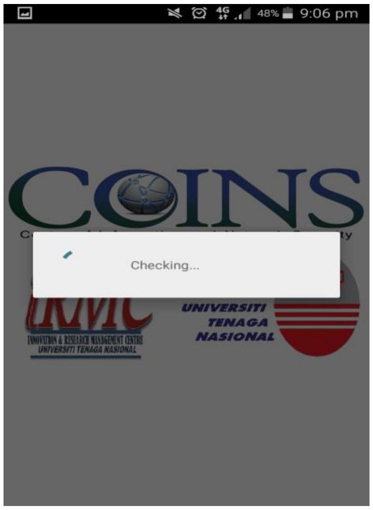


Figure 8: Trust value for Scenario 1

V. Prototype

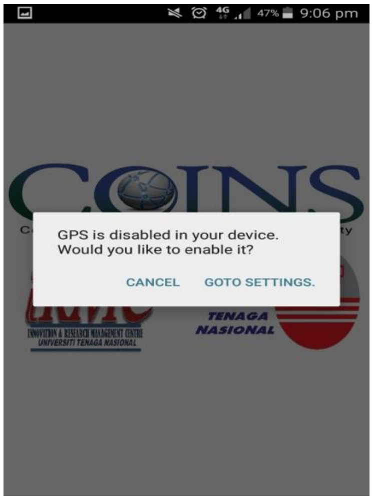
A prototype, running on Android smartphone and web server, was developed to demonstrate the workability of the proposed trust assessments. Upon running the application on an android smartphone, the system will check whether the GPS mode is enabled. Without GPS enabled, the system will not work and proceed to the end. If GPS facility is working, the user will be presented with 2 big buttons (red and green). The user can click on the Red button if the area he is currently in is flooded or the green button if the area he is currently in is not flooded. Once the button is clicked, the system will send a flooded or not-flooded message to a pre-defined recue center number. The trust value of the message is calculated and the map on the web server is updated accordingly. The rescuer will be able to see the live map, depicting the current flood level, on the web server. Those areas, with red colors, are the critical areas that need immediate attention. The rescuer can organize their rescue efforts to those critical areas.

Below are the sample screenshots from the android application and web server.



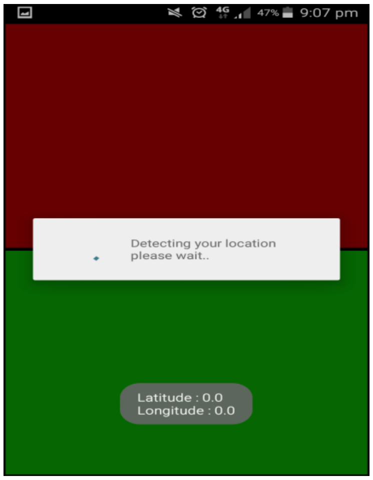
Checking...

Figure 9: Checking for GPS services



GPS is disabled in your device.
Would you like to enable it?

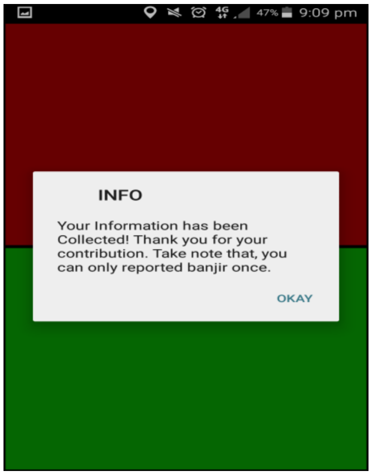
Figure 10: Option to enable GPS



Detecting your location
please wait..

Latitude : 0.0
Longitude : 0.0

Figure 11: Acquiring GPS Coord



INFO

Your Information has been Collected! Thank you for your contribution. Take note that, you can only reported banjir once.

Figure 12: Info send to server

Figure 9 to 12 shows the checking of available GPS services and the extraction of GPS location plus submission of relevant data to the server. Figure 13 shows the screenshot displayed on the web server seen by the rescuer. The colors showed the different critical levels of the disaster scenario from the selected areas.

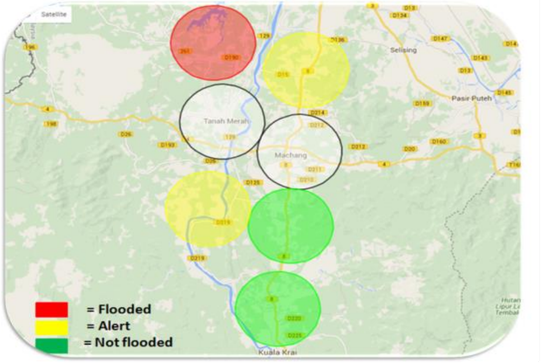


Figure 13: Web server screenshot

The prototype was demonstrated to the public at the PECIPTA2015 exhibition and received favorable comments. This prototype will be further enhanced to include the complete features required by the proposed trust algorithm.

VI. Conclusion and Future Works

A numbers of methods are currently being used to send information regarding the status of a disaster to the relevant authority. It has been observed that during the disaster, a huge numbers of messages were sent to the rescue command center. Those rescuers who work at the command center must decide which areas that warrants for their immediate attention. With the proposed message trust calculation, it is possible for the rescuer to focus their rescue effort on more critical areas. The higher trust values means the situation for that area is critical and need immediate attention from the rescuers. Without the ability to assess the trustworthiness of the received messages, it would be difficult for the rescuer to focus their rescue effort. They may mistakenly send the rescue team to a less critical area instead to those that require urgent attention.

Acknowledgment

This study is conducted under Malaysian FRGS Special Flood Grant.

References

[1] J. Howe, “Crowdsourcing: Why the power of the crowd is driving the future of business,” *New York: Crown Publishing Group*, 2008.

[2] E. Estelles-Arolas and F. Gonzalez-Ladron-de-Guevara, “Towards an integrated crowdsourcing definition,” *Journal of Information Science*, vol. 32, no. 2, pp. 189-200, 2012.

[3] Zook, M., Graham, M., Shelton, T., Gorman, S , “Volunteered Geographic Information and Crowdsourcing Disaster Relief: A Case Study of the Haitian Earthquake,” *World Medical & Health Policy*, Vol. 2, Iss. 2, Art. 2, 2010.

[4] J. Heinzelman and C. Waters, “Crowdsourcing Crisis Information in DisasterAffected Haiti, United States Institute of Peace (USIP),” Washington DC, Special Report 252, Oct. 2010. [Online]. Available: www.usip.org. Accessed: Feb. 03, 2016.

[5] A. Rajabifard and D. Coleman, “Spatially enabling government, industry and citizens: Research and development perspectives,” *Needham, Ma.: GSDI Association Press*, pp 201-214, 2012.

[6] A. Bruns, J. Burgess, K. Crawford, and F. Shaw, “Crisis Communication on Twitter in the 2011 South East Queensland Floods,” *ARC Centre of Excellence for Creative Industries and Innovation, Brisbane*, 2012.

[7] K. McDaugall, “Using Volunteered Information to Map the Queensland Floods,” *Proceeding of the Surveying & Spatial Sciences Biennial Conference 2011*, Wellington, New Zealand, pp. 13–23, 2011.

[8] A. Abu Bakar, Secure Access Control Architecture for Mobile Architecture for Mobile Ad-Hoc Network in Emergency Services, PhD Thesis, Universiti Tenaga Nasional, Malaysia, Dec 2011.

[9] S. Marsh, Formalising Trust as a Computational Concept, Formalising Trust as a Computational Concept, Department of Computing Science and Mathematics, University of Stirling, Mar 1994.

[10] P. Lamsal, Understanding Trust and Security, Department of Computer Science, University of Helsinki, Finland, Technical Report, Oct. 20, 2001. [Online]. Available: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.17.7843&rep=rep1&type=pdf. Accessed: Feb. 03, 2016.

[11] V. Varadharajan, “Evolution and Challenges in Trust and Security in Information System Infrastructures,”*Proceeding of the 2nd International Conference on Security of Information and Networks (SIN ’09)*, North Cyprus,Turkey, 2009.

[12] H. McKnight and N. Chervany, The Meaning of Trust, MISRC Research Center Working Papers, MISRC WP 96-04, 1996. [Online]. Available: http://www.misrc.umn.edu/workingpapers/fullPapers/1996/9604_040100.pdf. Accessed: Feb. 03, 2016.

[13] V. Cahill et al., “Using Trust for Secure Collaboration in Uncertain Environments,” *IEEE Pervasive Computing*, vol. 2, no. 3, pp. 52–61, 2003.

[14] S. Castaldo, K. Premazzi, and F. Zerbini, “The Meaning(s) of Trust. A Content Analysis on the Diverse Conceptualizations of Trust in Scholarly Research on Business Relationships,” *Journal of Business Ethics*, vol. 96, pp. 657-668, 2010.

[15] F. Almenarez, A. Marin, C. Campo, R, C. G, “PTM: A Pervasive Trust Management Model for Dynamic Open Environments,” *First Workshop on Pervasive Security, Privacy and Trust (PSPT'04)*, Aug 2004, Vol 4, pp 1-8, 2004.

[16] B. Lang, Z. Wang, and Q. Wang, Trust Representation and Reasoning for Access Control in Large Scale Distributed Systems, in 2nd International Conference on Pervasive Computing and Applications, 2007. ICPCA 2007., 2007, pp. 436–441. [Online]. Available: DOI: 10.1109/ICPCA.2007.4365483.

[17] M.Haque, M., & I.Ahamad, S. “An Omnipresent Formal Trust Model (FTM) for Pervasive Computing Environment,” *Proceeding of the 31st Annual International Computer Software and Applications Conference (COMPSAC 2007), IEEE Press*, Beijing, China, July 2007, pp 49-56.

[18] A. Josang, “A Logic for Uncertain Probabilities,” *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, Vol. 9, No. 3, June 2001.

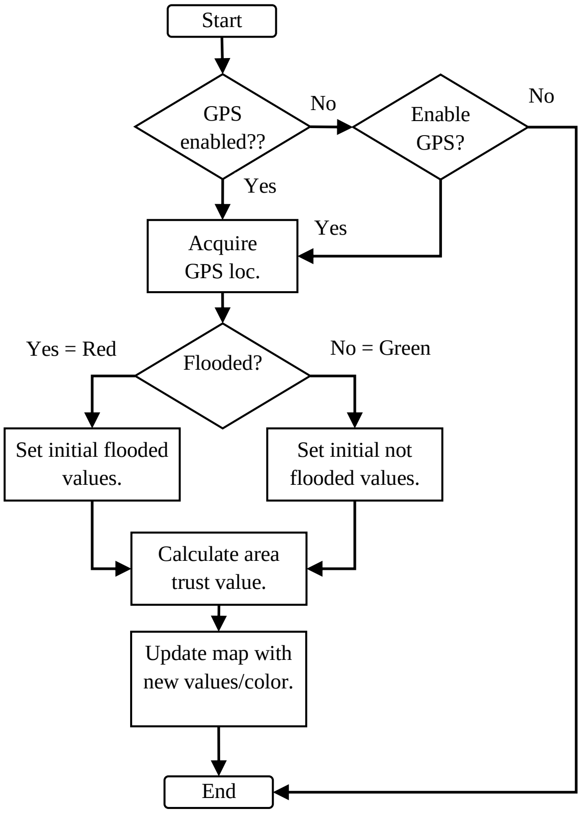

Start
GPS enabled??
No
Enable GPS?
No
Yes
Acquire GPS loc.
Yes
Yes = Red
Flooded?
No = Green
Set initial flooded values.
Set initial not flooded values.
Calculate area trust value.
Update map with new values/color.
End

Figure 14: Prototype flowchart