International Journal of Trend in Scientific Research and Development (IJTSRD)
International Open Access Journal
ISSN No: 2456 - 6470 | www.ijtsrd.com | Volume - 2 | Issue – 3

Rumour Source Identification in Network

M. Anitha, P. Ananthi, Dr. S. P. Rajagopalan
Department of Computer Science and Engineering, G.K.M. College
of Engineering and Technology, Chennai, Tamil Nadu, India

ABSTRACT

Identification of rumour sources in a network plays a critical role in limiting the damage caused by them through the timely quarantine of the sources. However, the temporal variation in the topology of networks and the ongoing dynamic processes challenge our traditional source identification techniques that are considered in static networks. Reduction of the time-varying networks is defined by an ordered stream of interactions between individual node. And then instead of inspecting every individual in traditional techniques, we adopt a reverse dissemination strategy to specify a set of suspects of the real rumor source. The node from which all the path covering all the observed nodes. In this process gives near to the rumour but not giving exact rumour in the network. To determine the exact real source a microscopic rumour spreading method is used. The results further indicate that our method can accurately identify the real source, or an individual who is very close to the real source. To the best of our knowledge, the proposed method is the first that can be used to identify rumor sources in time-varying network.

Keywords: *Network, Source estimation, Data count, Novel source, Reverse process*

Introduction

Network allows a number of users to send information. A simple network will be created in this model. In this network, each user is considering as a node and its neighbouring nodes are considered as friends. Time-Varying network is defined by an ordered stream of interaction between individual node. Not only promote the efficiency of information sharing but also dramatically accelerate the speed of rumour spreading. The main goal of this paper is to identify the person who send the fake messages, and finding the fake message it automatically start a reverse dissemination strategy to specify a suspect of the real rumour source and it eliminate the source from a network. This project proposes a novel source identification method to overcome the challenges. Each and every node possesses one unique number and with the help of this, we are able to identify the sender node. All edges and nodes are present in a time- integrating window. The use of time-integrating window is to identify the accurate time of the messages which was shared by the users. Using Microscopic method, the source whose having high data count will be the real rumour source and then exact rumour will be identified.

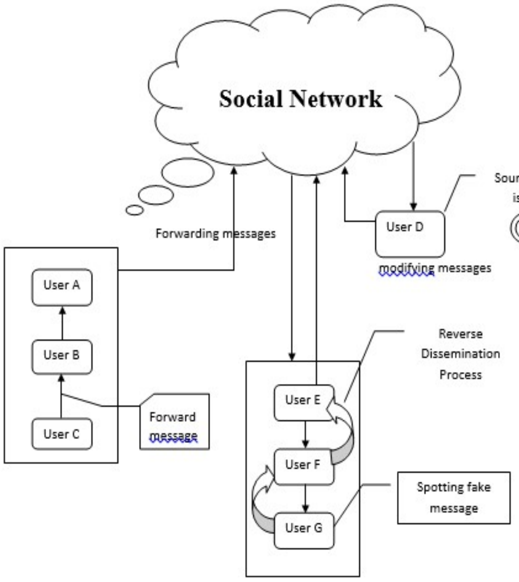
Related Works

An Ribeiro, Perra and Baronchelli, proposed a method to Qualifying the effect of temporal resolution on time-varying networks, Scientific reports, (2013). An Vana, Amancio, and L.Costa, introduced On time varying collaboration networks,"Journal of Informetrics. (2013). A Shah et al. [6] proposed the rumour method to detect rumour source in a network. They claimed that the user with maximum closeness centrality is the rumour source. Later the rumour method was extended by many other researches, which can identify rumour sources with different propagation models and observations. Luo et al. prposed a system extended the rumour method by considering multiple source instead of a single source. Dong et al [27] further proposed a local rumour method. All of these methods use the breadth first search (BFS) technique to construct tree topologies upon networks.

An D. Shah and T. Zaman, “Detecting sources of computer viruses in a networks”and Luo, Tay, and Leng, proposed a system to “Identifying infection sources and region in large networks (2013). Then Wang, Dong, Zhang and Tan, are introduced Rumour source detection with multiple observation: Fundamental limits and algorithm (2014). An Pinto, Thiran, Vetterli are introduced Locating the source of diffusion in large-scale networks (2012).This project introduced the Source detection in SIR model: A sample path based approach where infection nodes may recover, which can occur in many practical scenarios. Because of node recovery the information source detection problem under SIR model (2013).

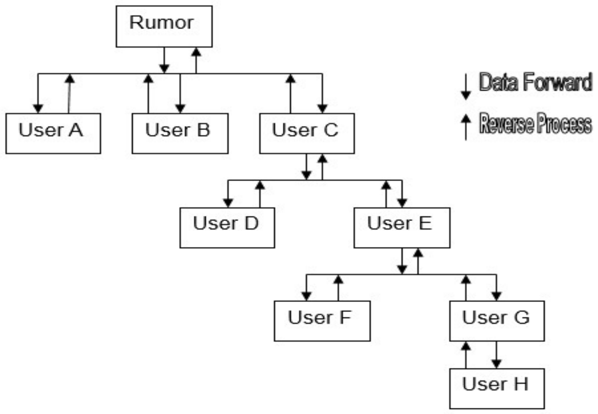
Proposed System

The proposed system is designed with additional features in the existing system such that it is planned to add novel source identification method to overcome the challenges. And it can be able to identify the real rumour source in a network.



A. Network formation

A simple network will be created in this model. In this network, each user is consider as a node and its neighbouring nodes are considered as friends. Each node possesses one unique number and with the help of this, we are able to identify the sender node. The system time running at the top of node would provide the time at which the message was sent. we need to change the network from dynamic to static so we can maintained the received time for every individual by using system time.

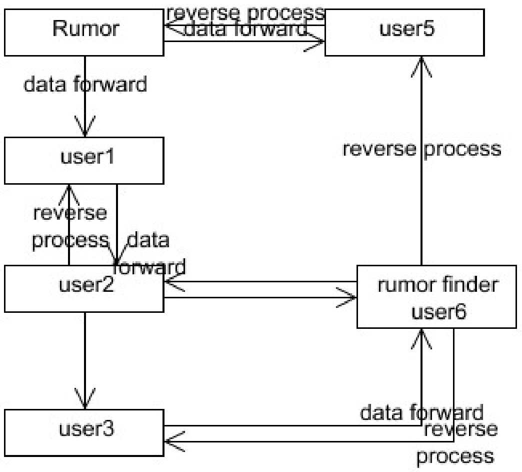


B. Novel source identification

Time varying network is defined by an ordered stream of interactions between individual node. Time progress interaction structure keeps changing in the network. Spreading rumours is affected by duration, sequence, and concurrency of contact among people. In this work, we reduce time-varying networks to a series of static networks by introducing a time integrating window. Each integrating window aggregates all edges and nodes present in the corresponding time duration.

C. Reverse dissemination process

The reverse dissemination method is to send copies of rumours along the reversed dynamic connections from observed nodes to exhaust all possible spreading paths leading to the observation. The node from which all the paths, covering all the observed nodes. The reverse dissemination method is inspired from the Jordan method. The reverse dissemination method is different from the Jordan method, because our method is based on time-varying networks. And it gives near to the rumour but not giving exact rumour in the network.



D. Identifying rumour source and elimination

Rumour sources are to design a good measure to specify the real source. A novel rumour spreading model will also be introduced to rumour spreading in time varying networks. Every user maintained two types of table, one is received message table and another one is fake message table. Using this method the exact rumour will be identified and the fake message will not be transferred anymore after finding the real source in the network.

E. Conclusion

This paper developed Novel source identification method, and proposed time integrating window. Reduction of the time-varying networks to a series of static networks by introducing a time integrating window. Each integrating window aggregates all edges and nodes present in the corresponding time duration. Hence instead of inspecting every individual in traditional techniques, we adopt a reverse dissemination strategy to specify a set of suspects of the real rumour source. By microscopic method the exact rumour will be identified and the fake message will not be transferred anymore after finding the real source in the network.

REFERENCES

1. D. Shah and T. Zaman, “Detecting sources of computer viruses in networks: Theory and experiment,” in Proc. Ann. ACM SIGMETRICS Conf., New York, NY, 2010, pp. 203–214.

2. W. Luo and W. P. Tay, “Identifying multiple infection sources in a network,” in Proc. Asilomar Conf. Signals, Systems and Computers, 2012.

3. W. Luo, W. P. Tay, and M. Leng, “Identifying infection sources and regions in large networks,” IEEE Trans. Signal Process., vol. 61, pp. 2850–2865.

4. N. Karamchandani and M. Franceschetti, “Rumor source detection under probabilistic sampling,” in Proc. IEEE Int. Symp. Information Theory (ISIT), Istanbul, Turkey, July 2013.

5. W. Dong, W. Zhang, and C. W. Tan, “Rooting out the rumour culprit from suspects,” in Proc. IEEE Int. Symp. Information Theory (ISIT), Istanbul, Turkey, 2013, pp. 2671–2675.

6. K. Zhu and L. Ying, “Information source detection in the SIR model: A sample path based approach,” in Proc. Information Theory and Applications Workshop (ITA), Feb. 2013.

7. ——, “A robust information source estimator with sparse observations,” in Proc. IEEE Int. Conf. Computer Communications (INFOCOM), Toronto, Canada, April-May 2014.

8. W. Luo and W. P. Tay, “Finding an infection source under the SIS model,” in Proc. IEEE Int. Conf. Acoustics, Speech, and Signal Processing (ICASSP), Vancouver, BC, May 2013.

9. B. A. Prakash, J. Vreeken, and C. Faloutsos, “Spotting culprits in epidemics: How many and which ones?” in IEEE Int. Conf. Data Mining (ICDM), Brussels, Belgium, 2012, pp. 11–20.

10. A. Agaskar and Y. M. Lu, “A fast monte carlo algorithm for source localization on graphs,” in SPIE Optical Engineering and Applications, 2013.

11. Seo, P. Mohapatra, and T. Abdelzaher, “Identifying rumours and their sources in social networks,” in SPIE Defense, Security, and Sensing, 2012