Journal of Engineering and Applied Sciences 13 (Special Issue 4): 3786-3788, 2018
ISSN: 1816-949X

Trust Aware Routing and Data Forwarding in Wireless Networks

[1]Shabir Ahmed Mir and [2]T. Padma
[1]Department of Information Technology, AMET University, Chennai, India
[2]Department of Computer Applicaions, Sona College of Technology, Salem, India

Abstract: Community and structural vulnerability assessment, less reliability in Delay Tolerant Networks (DTN), loss of security. Trust aware routing framework, parallelly sense during data communication, network structure remains unchanged, security: route based and content based access with single system access control. Taking consideration of above all factors Trust Aware based Data Forwarding (TADF) technique is proposed. The efficiency is calculated using throughput metric of the network.

Key words: Delay tolerant networks, trust aware based data forwarding, throughput, reliability, access, single

INTRODUCTION

Mobile opportunistic networks are characterized by intermittent and non-deterministic connectivity, often due to Interruptible wireless links, sparse network deployment and/or nodal mobility. Structural susceptibility of public-based forwarder and direction-finding methods are proposed for opportunistic networks (Alim *et al*., 2016). Such opportunistic networking has been discussed in the context of delay/disruption-tolerant networks, sporadically connected sensor networks, vehicular networks, peer-to-peer mobile social networks and 5G networks. Determining the edges based on the number of edges that have at least one end point for identifying the routes availability (Apollonio and Simeone, 2014). These networks do not depend on any infrastructure but instead, exploit opportunistic connections between mobile devices to enable device-to-device communication. In Disruption or Delay Tolerant Networks (DTN) (Zhu *et al*., 2013) social based routing methods have been undertaken and this protocol recently drawn a great attention due to their wide application in pervasive environments such as military operations, space communication and dynamic wireless sensor deployments. In general, DTNs are partitioned wireless ad-hoc networks with the notable characteristic of intermittent connectivity. Community structure Vulnerability Assessment (CVA) issue occurred in the network can be removed by applying the community structure using multiple greedy algorithms (Nguyen *et al*., 2013). Node disruption is evaluated for maintaining the network operability.

Due to this intermittent connectivity, DTNs display unstable network structures are lack of instantaneous end-to-end connections and thus, shall never be fully connected at any point in time. In addition, they often incur a large transmission delay between participating devices together with a probability of unsuccessful transmission (Grubesic *et al*., 2008). These characteristics limit the use of traditional message forwarding protocols, since, they rely on the establishment of a complete end-to-end route from the source to the destination. Genetic algorithms based enhanced K strange points clustering algorithm is also describes that (Johnson and Singh, 2015). Media access delay and throughput analysis of voice codec with silence suppression on wireless ad hoc network explained by Shah and Singh (2016).

MATERIALS AND METHODS

Data forwarding based on trust aware factor-proposed: The proposed model Trust Aware based Data Forwarding (TADF) technique is explained here. It includes reliable communities of nodes that includes secured path and trustable nodes:

- Security of wireless network
- Sense to find the shortest path to the destination
- Explores the structural vulnerability of routing
- On demand dynamic routing protocol is built
- Choose another route when current route fails
- Reduces the throughput delay
- This sensor decreases the traffic demands
- Detects and analysis the malicious attacks
- Improves the reliability of packet forwarding

The nodes are chosen based on their reliability and its community edges available among them are determined. Specific detection algorithm is proposed for identifying the reliable routes among the nodes by using

Corresponding Author: Shabir Ahmed Mir, Department of Information Technology, AMET University, Chennai, India

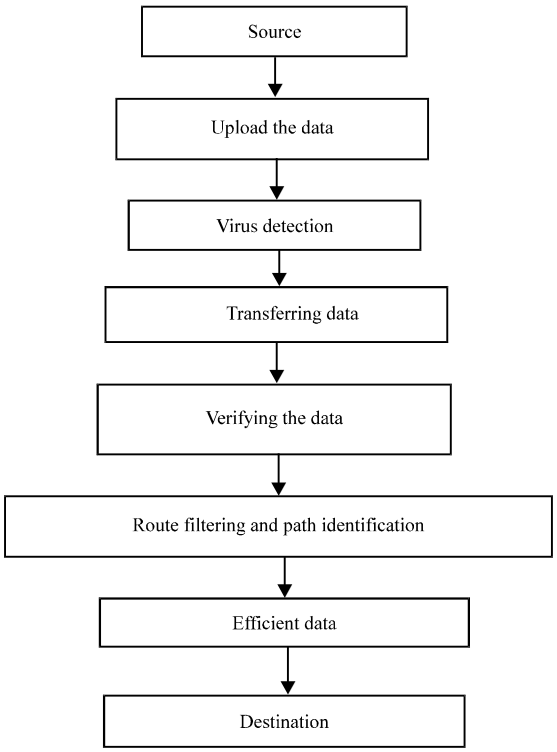

Fig. 1: Architecture of TADF

their Graph G = (V, E), i.e., Vertices and Edges. The detection algorithm is applied for all the nodes and the set of communities formed are $X = \{X_1, X_2, \ldots, X_{n-1}\}$. Once the targeted node is chosen then the community edges are identified and these communities are sub divided into multiple new sub communities. This X community nodes are said to be more optimal and these network density exposes more reliable in all conditions.

The routes are chosen with the sub community nodes and it nodes in the core are incident to both endpoints of this edge. When the source node gets selected then the data is uploaded from the source node and the false ratio (virus) is detected in the destined transferred data. Route filtering mechanism is employed in the route identification method then the trustable nodes (sub communities) transfers the verified data to the targeted node.

Architecture diagram: The architectural system is shown in Fig. 1 for the proposed system TADF. This includes data transferring between source and targeted node with trustable and reliable routing.

RESULTS AND DISCUSSION

We first evaluate the performance of the node selection strategies in terms of NMI score. Because the

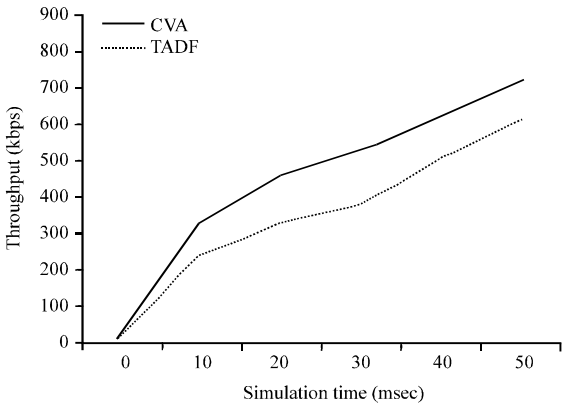

Fig. 2: Throughput (n = 2500)

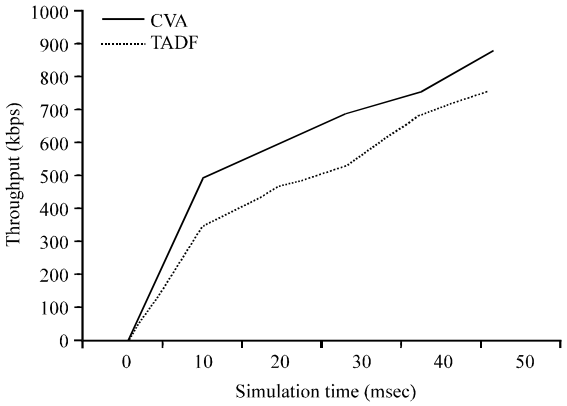

Fig. 3: Throughput (n = 5000)

ground truth communities are given a priori, a comparison through NMI scores among these strategies as well as among detection algorithms is therefore, valid and the lower NMI score a strategy obtains the more effective it seems to be. In addition, the higher the remaining NMI values a detection algorithm obtains after node removal, the more resilient to node vulnerability it appears to be. The quality of node selection for n = 2500 and n = 5000 are reported in Fig. 2 and 3, respectively for different methods.

In general, NMI values tend to drop down quickly as more nodes are removed from the network when n = 2500, however, they do degrade much slowly in networks with n = 5000. The first observation revealed in those figures is that our approach appears to achieve the best (lowest) NMI scores on almost all test cases.

Case 1¬n = 2500: Throughput of the network with node density n = 2500 is given in Fig. 2. The proposed scheme TADF shows better network throughput compared to the conventional scheme CVA.

Case 2→n = 5000: Throughput of the network with node density n = 5000 is given in Fig. 3. The proposed scheme TADF shows better network throughput compared to the conventional scheme CVA.

CONCLUSION

In this research, we have studied the structural vulnerability of social-aware routing and forwarding schemes in opportunistic networks. In order to assess system fragility from community structure point of view, we have proposed the CVA problem, analyzed the minimization of NMI measure and provided key insights into the selection of nodes that are crucial to the community structure. We have suggested an approximation algorithm for the case k = 1 and also presented genEdge, a heuristic for CVA problem when k>1, based on the concept of minimum generating edge set. To certify the effectiveness of the suggested algorithms, we have tested them on synthesized networks with known community structures and the performance of genEdge on these networks sets out the corner stone of deploying it on real-work social and DTN traces.

REFERENCES

Alim, M.A., X. Li, N.P. Nguyen, M.T. Thai and A. Helal, 2016. Structural vulnerability assessment of community-based routing in opportunistic networks. IEEE. Trans. Mobile Comput., 15: 3156-3170.

Apollonio, N. and B. Simeone, 2014. The maximum vertex coverage problem on bipartite graphs. Discrete Appl. Math., 165: 37-48.

Grubesic, T.H., T.C. Matisziw, A.T. Murray and D. Snediker, 2008. Comparative approaches for assessing network vulnerability. J. Int. Regional Sci. Rev., 31: 88-112.

Johnson, T. and S.K. Singh, 2015. Genetic algorithms based enhanced K strange points clustering algorithm. Proceedings of the International Conference on Computing and Network Communications (CoCoNet), December 16-19, 2015, IEEE, Trivandrum, India, ISBN:978-1-4673-7309-8, pp: 737-741.

Nguyen, N.P., M.A. Alim, Y. Shen and M.T. Thai, 2013. Assessing network vulnerability in a community structure point of view. Proceedings of the 2013 IEEE-ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM), August 25-28, 2013, IEEE, Niagara Falls, Ontario, Canada, ISBN:978-1-4503-2240-9, pp: 231-235.

Shah, R.D. and S.K. Singh, 2016. Media access delay and throughput analysis of voice codec with silence suppression on wireless ad hoc network. Procedia Comput. Sci., 79: 940-947.

Zhu, Y., B. Xu, X. Shi and Y. Wang, 2013. A survey of social-based routing in delay tolerant networks: Positive and negative social effects. IEEE. Commun. Surv. Tutorials, 15: 387-401.