International Journal of Research
Available at https://journals.pen2print.org/index.php/ijr/
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 06 Issue 08
July 2019

A Review on design and analysis of distributed faulty node detection in DTN

MOUNIKA MULLURI 1, K.V.SRINIVASARAO 2

1 PG Scholar, Dept of CSE, Prakasam Engineering College, Kandukur, Prakasam(Dt), AP, India,kanalasrujana80@gmail.com

2 Associate Professor , Dept of CSE, Prakasam Engineering College,Kandukur, Prakasam(Dt), AP, India

ABSTRACT:

For our circumstance Delay Tolerant Networks (DTN) explicitly, the phenomenal social event events require that center points are viable in spreading perfectly information. Hence, instruments to rapidly recognize possible imperfect centers should be made. Spread broken center point area has been tended to in the composition concerning sensor and vehicular frameworks, anyway starting at now proposed plans experience the evil impacts of long deferrals in perceiving and separating center points making defective data. This is unsatisfactory to DTNs where center points meet only now and again. This paper proposes a totally appropriated and adequately implementable approach to manage empower each DTN center point to rapidly perceive whether its sensors are making broken data. The dynamical lead of the proposed figuring is approximated by some consistent time state conditions, whose parity is depicted. The proximity of acting underhandedly center points, endeavoring to trouble the defective center point revelation process, is also considered. Acknowledgment and false alarm rates are surveyed by taking a gander at both theoretical and reenactment results. Numerical results assess the practicality of the proposed game plan and can be used to give rules for the count plan.

1.INTRODUCTION

In recent years, Wireless Sensor Networks (WSNs) have been widely investigated and many applications have been implemented in industry control, environment surveillance, public security, and many other areas that benefit people's life. One obvious trend in the development of WSNs is the fast increasing system scale, which renders the reliability a significant factor in the design and deployment. In realistic large-scale WSNs deployment,

sensors are normally made cheap but not sufficiently reliable to meet the requirements of the cost effectiveness. Sensors may suffer unnegligible error probability and cannot collect accurate data frequently. As a result, the network performance is deteriorated if the faulty nodes cannot be detected and isolated in time. Therefore, faulty node detection and isolation is playing a more and more important role to improve the network performance. Unfortunately, straightforward solutions to this task are costly and unrealistic because to check the numerous sensor nodes one by one periodically will consume too many network resources, especially for large-scale WSNs. To our best knowledge, several works on faulty node detection in WSNs have been done, but most of them are not dealing with Mobile Ad-hoc Networks (MANETs), particularly intermittently connected Delay Tolerant Networks (DTNs). Furthermore, faulty node isolation in MANETs is rarely investigated. In this paper, one of such mobile sensor networks, namely, the Metropolitan-area Vehicular Sensor NETworks (MVSNETs), is selected as the application scenario to study the faulty node detection and isolation. In MVSNETs, sensors are deployed in metropolis for urban environment surveillance such as air quality, humidity, temperature, etc., and vehicles, which move around the whole city, act as carriers to collect and transmit data. Given that the network system is in large scale and sparse, intermittently connected, frequently changed in topology and limited in computation and storage capacity, a self-organizing, energy-efficient and delay-tolerant distributed faulty node detection and isolation algorithm is proposed. In our MVSNET model, there are three kinds of nodes, a large number of fixed sensor nodes (Sensor), mobile communicators equipped on vehicles (Carrier) and a few sink nodes (Aggregator). Sensors are deployed by road-side. The ”StoreCarry-Forward” strategy is used to convey delay-tolerant data. Data collected by sensors are sent to carriers when they pass through. When two carriers encounter, they exchange data over a short range wireless link. So the network connectivity is acquired by the mobility of vehicles. The design goal of the algorithm is to detect the faulty sensors and shut them down as quickly as possible with small amount of communication and computational overheads. The rationale of the proposed algorithm is to exploit the local spatial correlation of the physical field that is being sampled by sensors, and take advantage of the carrier mobility to reduce the

communication overhead while increase the responding speed to isolate the malfunctioning sensors. The proposed algorithm is simulated on real data to check its performance in reality. For detection algorithm, we analyze the simulation results to investigate how the parameters, such as the node density and the detection window size, affect the performance. For faulty node isolation, optimal parameters are found to minimize the total data traffic in the whole network.

2. LITERATURE SURVEY

Clusters are formed based on their nodal contact probabilities the probability of nodes meeting each other. Based on their nodal contact probability the threshold probability will be calculated , using which the clusters are formed and the gateways nodes are selected to route data from one cluster to another[1][2]. In [9] capacity and delay trade off mechanism, the capacity of the cell partitioned networks and analysis the delay of the capacity achieving relay algorithm. The packet are transmitted and routed according to the timeslot assign to each node without violating the physical constrains of the partitioned cell. The capacity region depends only on the steady-state user location distributaries. Hence, any markovian model of the user mobility which in steady state distribute users independently and the network yields uniformly over the same expression for mobile nodes. A cluster-based self-organizing strategy is proposed for building a backbone among the mobile devices, detecting segmentation, and recovery [3][4]. In this approach, each mobile device is controlled by a multi-role agent, which performs these tasks efficiently based only on local interactions; role management allows the backbone reconfiguration when the nodes leave or arrive to the network yielding a complex global emergent behaviour.[5] Energy saving is achieved by adapting the time interval and power of transmission after the network formation. The inconsistency problem exist both in member and gateway nodes. When two nodes in the same cluster may have two different gateways to another cluster A node may lose its gateway to an adjacent cluster because the gateway node has left. These inconsistency problem employing by synchronization mechanism where nodes exchange and keep only the most up to data information. The replication mechanism that routing protocols adopt to ensure delivery of the original packet to the sink is to transmit multiple copies of the same packet over different paths in order to recover from some path failures Wireless

networks are without a doubt one of the central issues in current research topics due to the harsh environmental conditions in which such networks can be deployed and their unique network characteristics, specifically limited power supply, processing and communication capabilities[6]. [7] Presented with many challenges and design issues that affect the data routing, a need for a fault tolerant routing protocol becomes essential. An algorithm to form the various paths from sender to destination will be provide [8][9].

3.RELATED WORK

In Previous paper "Trustworthiness Management in the Social Internet of Things", IEEE Transactions On Knowledge And Data Engineering, May 2014, M. Nitti, R. Girau, and L. Atzori,[1] focused on how the information provided by members of the social IoT to build a reliable system on the basis of the behavior of the objects. The author proposed two model for the trustworthiness management such as subjective and objective model. In paper "A Probabilistic Misbehavior Detection Scheme toward Efficient Trust Establishment in Delay-Tolerant Networks", IEEE Transactions on Parallel and Distributed Systems, Jan 2014, Haojin Zhu[2] has discussed that a malicious and selfish behavior is serious threat routing in delay/disruption tolerant networks (DTNs). The author proposed a probabilistic Trust model for misbehavior detection in order to establish trust among the nodes. In paper "A Trust Based Approach for Increasing Security in Cloud Computing Infrastructure", IEEE UKSim 15th International Conference on Computer Modelling and Simulation, 2013, H. Banirostam, A. Hedayati, A. Zadeh, and E. Shamsinezhad[3] has discussed about Cloud computing is become an fast growing buzzword, currently not having appropriate tools for their verification of confidentiality, privacy policy, computing accuracy, and Ashwini Borkar et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 6 (1) , 2015, 658-660 www.ijcsit.com 659 data integrity. Hence author suggested new approach called Trusted Cloud Computing Infrastructure. In paper "Privacy Preserving Data Sharing With Anonymous ID Assignment", IEEE Transactions On Information Forensics And Security, Vol. 8, No. 2, February 2013, Larry A. Dunning, and Ray Kresman[4] has discussed that in network, in order to sharing of private data among node, assigning secure and unique ID's is required. The authors examine

International Journal of Research
Available at https://journals.pen2print.org/index.php/ijr/
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 06 Issue 08
July 2019

existing and new algorithms for assigning anonymous IDs, with respect to trade-offs between communication and computational requirements.

4.IMPLEMENTATION

- **Service Provider**

In this module, the Service Provider browses the required file, initializes nodes with digital signature and uploads to the end user (node a, node b, node c, node d, node e, node f) via Router.

- **Router**

The Router is responsible for forwarding the data file in shortest distance to the destination; the Router consists of Group of nodes, the each and every node (n1, n2, n3,n4,n5,n6,n7,n8,n8,n10,n11,n12, n13) consist of Bandwidth and Digital Signature. If router had found any malicious or traffic node in the router then it forwards to the IDS Manager. In Router we can assign the Sleeping time for the nodes and can view the node details with their tags Node Name, Sender IP, Injected data, Digital Signature, Sleeping time and status.

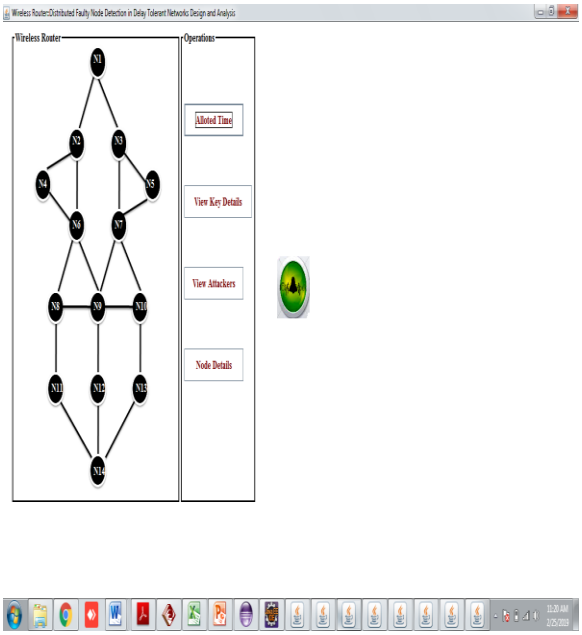
- **End User**

In this module, the End user can receive the data file from the Service Provider which is sent via Router, if malicious or traffic node is found in the router then it never forwards to the end user to filter the content and adds to the attacker profile.

- **Attacker**

In this module, the malicious node or the node details can be identified by a threshold-based classifier is employed in the Attack Detection module to distinguish DoS attacks from legitimate Sleeping Time. The Attacker can inject the fake message and generates the signature to a particular node in the router with the help of threshold-based classifier in testing phase and then adds to the attacker profile.

5.SIMUALATION RESULTS



5.1 Router

International Journal of Research
Available at https://journals.pen2print.org/index.php/ijr/
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 06 Issue 08
July 2019

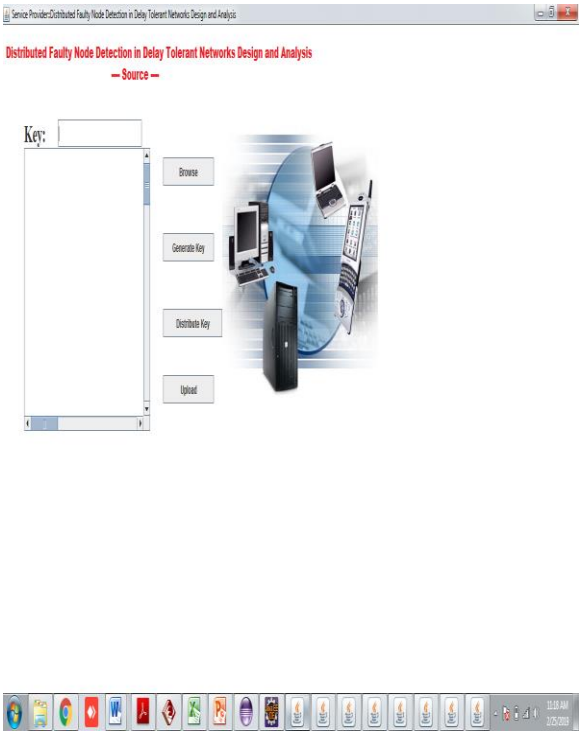


Fig 5.2 Source Provider

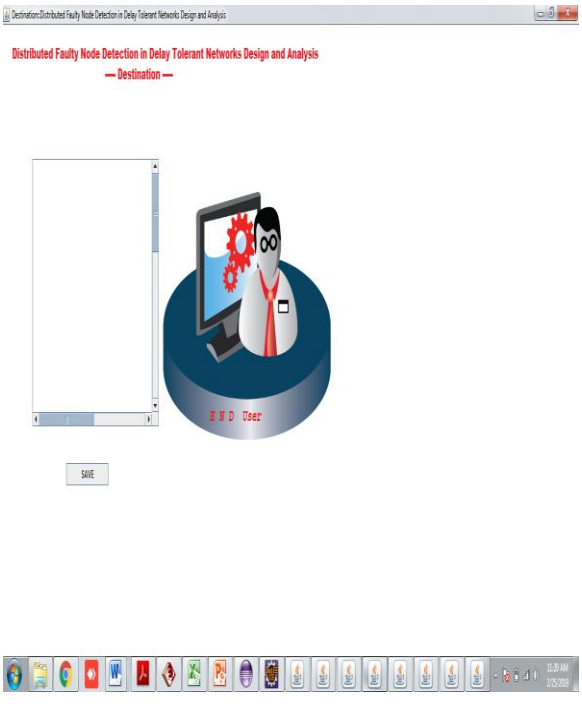


Fig 5.3 Destination Page

6.CONCLUSION

This paper has designed a distributed faulty node detection and isolation algorithm for delay-tolerant vehicular sensor networks. The on-board delay-tolerant distributed faulty node detection algorithm utilizing sample data's spatial correlation demands so low on nodes' communication and computation ability that is suitable for mobile sparse sensor networks. Based on the distributed faulty node detection algorithm, a faulty node isolation algorithm is proposed aiming at both controlling the diffusion of faulty data and reducing communication cost. A temperature collection system is simulated on real data of urban temperature and roads distribution, which suggests the distributed faulty node detection and isolation algorithm effective. By analyzing the simulation results, we describe how the parameters affect the performance of the algorithms and achieve the optimal settings. A list of parameter settings in such metropolitan-area vehicular temperature sensor network is provided to help implementation. With feasible parameter settings, over 70 percent of faulty nodes can be identified. More than half of the faulty data can be reduced in the whole network while the total overhead decreases by 35%. It is noticed that a lot of sensor data, such as

environmental measurements, are correlated in both space and time. So in future researches, the temporal correlation of data should be taken into account to improve the faulty node detection accuracy.

REFERENCES

[1] M. J. Khabbaz, C. M. Assi, and W. F. Fawaz, "Disruption-tolerant networking: A comprehensive survey on recent developments and persisting challenges," IEEE Commun. Surveys Tuts., vol. 14, no. 2, pp. 607–640, Apr.–Jun. 2012.

[2] P. R. Pereira, A. Casaca, J. J. Rodrigues, V. N. Soares, J. Triay, and C. Cervell_o-Pastor, "From delay-tolerant networks to vehicular delay-tolerant networks," IEEE Commun. Surveys Tuts., vol. 14, no. 4, pp. 1166–1182, Oct.–Dec. 2012.

[3] K. Wei, M. Dong, J. Weng, G. Shi, K. Ota, and K. Xu, "Congestionaware message forwarding in delay tolerant networks: A community perspective," Concurrency Comput.: Practice Experience, vol. 27, no. 18, pp. 5722–5734, 2015.

[4] P. Hui, J. Crowcroft, and E. Yoneki, "BUBBLE rap: Social-based forwarding in delay-tolerant networks," IEEE Trans. Mobile Comput., vol. 10, no. 11, pp. 1576–1589, Nov. 2011.

[5] V. N. Soares, J. J. Rodrigues, and F. Farahmand, "GeoSpray: A geographic routing protocol for vehicular delay-tolerant networks," Inf. Fusion, vol. 15, pp. 102–113, 2014.

[6] H. Zhu, S. Du, Z. Gao, M. Dong, and Z. Cao, "A probabilistic misbehavior detection scheme toward efficient trust establishment in delay-tolerant networks," IEEE Trans. Parallel Distrib. Syst., vol. 25, no. 1, pp. 22–32, Jan. 2014.

[7] L. Galluccio, B. Lorenzo, and S. Glisic, "Sociality-aided new adaptive infection recovery schemes for multicast DTNs," IEEE Trans. Veh. Tech., vol. 65, no. 5, pp. 3360–3376, May 2016.

[8] M. Panda, A. Ali, T. Chahed, and E. Altman, "Tracking message spread in mobile delay tolerant networks," IEEE Trans. Mobile Comput., vol. 14, no. 8, pp. 1737–1750, Aug. 2015.

[9] W. Li, F. Bassi, D. Dardari, M. Kieffer, and G. Pasolini, "Defective sensor identification for WSNs involving generic local outlier detection tests," IEEE Trans. Signal Inf. Process. Over Netw., vol. 2, no. 1, pp. 29–48, Mar. 2016.

[10] J. Chen, S. Kher, and A. Somani, "Distributed fault detection of wireless sensor networks," in Proc. Workshop

Depend. Issues Wireless Ad Hoc Netw. Sensor Netw., 2006, pp. 65–72.

technological university, ananthapur During 2015-19, respectively