Design and Analysis of Distributed Faulty Node Detection in Networks

AYYALASOMAYAJULA SWATHI
Student of M.Tech (CSE), Department of Computer Science & Engineering, KIET, Kakinada, AP, India

D.SRINUVAS
Asst.Prof, Depart of Computer Science & Engineering, KIET, Kakinada, AP, India

Abstract: **Propagation of faulty data is a critical issue. In case of Delay Tolerant Networks (DTN) in particular, the rare meeting events require that nodes are efficient in propagating only correct information. For that purpose, mechanisms to rapidly identify possible faulty nodes should be developed. Distributed faulty node detection has been addressed in the literature in the context of sensor and vehicular networks, but already proposed solutions suffer from long delays in identifying and isolating nodes producing faulty data. This is unsuitable to DTNs where nodes meet only rarely. This paper proposes a fully distributed and easily implementable approach to allow each DTN node to rapidly identify whether its sensors are producing faulty data. The dynamical behavior of the proposed algorithm is approximated by some continuous-time state equations, whose equilibrium is characterized. The presence of misbehaving nodes, trying to perturb the faulty node detection process, is also taken into account. Detection and false alarm rates are estimated by comparing both theoretical and simulation results. Numerical results assess the effectiveness of the proposed solution and can be used to give guidelines for the algorithm design. PRD assigns weights to individual links as well as end-to-end delay, so as to reflect the node status in the long run of the network. Large-scale simulation results demonstrate that PRD performs better than the widely used ETX metric as well as other two metrics devised recently in terms of energy consumption and end-to-end delay, while guaranteeing packet delivery ratio.**

Keywords: **Network Tomography; Failure Localization; Identifiability Condition; Maximum Identifiability Index;**

INTRODUCTION

Overlay directing has been proposed as of late as a successful method to accomplish certain steering properties, without going into the long and repetitive procedure of institutionalization and worldwide arrangement of another directing convention. For instance, in [1], overlay directing was utilized to enhance TCP execution over the Internet, where the fundamental thought is to break the conclusion to-end criticism circle into littler circles. This necessitates nodes equipped for performing TCP Piping would be available along the course at generally little separations. Different precedents for the utilization of overlay directing are ventures like RON [2] and Detour [3], where overlay steering is utilized to enhance unwavering quality. Amazingly, one more model is the idea of the "Worldwide ISP" worldview presented in [4], where an overlay node is utilized to decrease inertness in BGP steering. With the end goal to convey overlay steering over the genuine physical foundation, one needs to send and oversee overlay nodes that will have the new additional usefulness. This accompanies a non-unimportant cost both as far as capital and working expenses. In this way, it is essential to consider the advantage one gets from enhancing the steering metric against this expense. In this task, we focus on this point and concentrate the base number of framework nodes that should be included request to keep up a particular property in the overlay steering.

RELATED WORK

Most existing analyses on node disappointment discovery in portable wireless networks expect network availability. Numerous plans receive test and-ACK (i.e., ping) or heartbeat based systems that are regularly utilized in conveyed processing. Test and-ACK based methods require a focal screen to send test messages to different nodes [4]. At the point when a node does not answer inside a timeout interim, the focal screen views the node as fizzled. Heartbeat based procedures vary from test and-ACK based systems in that they dispense with the examining stage to diminish the measure of messages. A few existing examinations embrace prattle based conventions, where a node, after accepting a chatter message on node disappointment data, blends its data with the data got, and after that communicates the joined data [5]. A typical disadvantage of test and-ACK, heartbeat and babble based methods is that they are just material to networks that are associated. What's more, they prompt a lot of expansive observing movement. Conversely, our methodology just generates confined checking activity and is pertinent to both associated and detached networks. In [1] the makers used Reactive Two-organize Rerouting (RTR) for intra territory coordinating with briefest way recovery. This tradition is used to recover frameworks from broad scale frustrations by using two phases. In first stage the RTR progresses the packages towards the neighbor to amass the mistake information and store it in the package header. In the second stage it finds another most short way and temporary routes the mistake locale which is self-sufficient of shape and zone. This procedure achieves incredible execution with 98.6% trustworthiness with minimum framework resources. In [8] the makers used different fortification ways which is predefined and secured in the hash table. Probabilistically Correlated Failure (PCF) demonstrate with a layer mapping procedure is used which limits and assesses the IP join dissatisfaction and gives strong support courses too. In case an IP association misses the mark, its development is part into various fortification ways with the end goal that the rerouted movement should not outperform the usable information transmission. The makers used ISP frameworks with both optical and IP layer topologies. Somewhere around two fortification ways are surrendered immovable quality to 18% and the guiding unsettling influence is lessened to around 22%. In this way the interface between rerouted action and run of the mill development is avoided for this circumstance. In [9] the makers used CP-ABE count inferred for recognizing complex access control on mixed data. By this framework the encoded data can be kept grouped paying little mind to the likelihood that the accumulating server is untrusted; likewise, this procedure is secure against course of action strikes. In this strategy the attributes are used to portray a customer's accreditations, and a social event encoding data chooses a course of action for who can decipher.

IP Link Protection Based On Backup Path.

Consider reinforcement way choice as a network issue and basically center around discovering reinforcement ways to sidestep the fizzled IP joins. Thusly, the rerouted movement may causes serious connection over-burden on a spine IP networks as they disregard the way that a reinforcement way may not having enough data transfer capacity as seen by [10]. In ongoing work, we create CPF model to feature the probabilistic relationship between's consistent connection failures, and split the rerouted movement onto various reinforcement ways to maintain a strategic distance from connection over-burden and limits directing interruption.

Connection between's the Logical and Physical Topologies

IP-over-WDM networks consider the connection between's the physical and consistent topologies. Limiting the effect dependent on fiber and coherent connections failures [7], demonstrated that topology mapping is emphatically influenced by the dependability of IP layer. Additionally, our methodology depends on a cross-layer plan. They go for finding dependable reinforcement ways; while our goal is to limit directing interruption. Our paper additionally considers the topology mapping, yet it is diverse in two angles. To start with, the CPF demonstrate considers both autonomous and related coherent connection failures. Second, Multiple reinforcement ways ensures each coherent connection in this paper, But secured by single reinforcement way in [15]

Allocation of Bandwidth and Multipath Routing

Nature of-Service (QoS) directing conventions [5], utilize numerous ways between a source-goal to accomplish activity building objectives, e.g., limiting the maximal connection use. In any case, they don't think about the relationship among's physical and sensible connection failures. There are some recuperation approaches that are based on numerous recuperation ways. The methodology in [9] goes for limiting the data transmission saved for reinforcement ways. It accept that the network has a solitary coherent connection disappointment and just uses IP layer data for reinforcement way determination. IN [4] reroutes activity with various ways and the strategy in [8] consolidate addresses disappointment recuperation and movement building in multipath directing. Besides, they overlook the connection between's legitimate connection failures and consider reinforcement ways ought to have same dependability and they center around activity designing objectives as opposed to limiting steering interruption.

SYSTEM MODEL

MANET communication system is subject to the following model:

1. The PHY/MAC layer is controlled by the commonly used 802.11(a/b/g) protocol. But all MAC frames (packets) are encrypted so that the adversaries cannot decrypt them to look into the contents.

2. Padding is applied so that all MAC frames (packets) have the same size. Nobody can trace a packet according to its unique size.

3. The “virtual carrier sensing” option is disabled. The source/destination addresses in MAC and IP headers are set to a broadcasting address (i.e., all “1”) or to use identifier changing techniques. In this case, adversaries are prevented from identifying point to point communication relations.

4. No information about the traffic patterns is disclosed from the routing layer and above.

5. Dummy traffic and dummy delay are not used due to the highly restricted resources in MANETs.

Attack Model

The attacker's goal is to discover the traffic patterns among mobile nodes. Particularly, we have the following four assumptions for attackers:

1. The adversaries are passive signal detectors, i.e. they are not actively involved in the communications. They can monitor every single packet transmitted through the network.

2. The adversary nodes are connected through an additional channel which is different from the one used by the target MANET. Therefore, the communication between adversaries will not influence the MANET communication.

3. The adversaries can locate the signal source according to certain properties (e.g., transmission power and direction) of the detected signal, by using wireless location tracking technique. Note that none of these techniques can identify the source of a signal from several nodes very close to each other. Hence, this assumption actually indicates that the targeted networks are sparse in terms of the node density. In other words, any two nodes in such a network are distant from each other so that the location tracking techniques in use are able to uniquely identify the source of a wireless signal.

4. The adversaries can trace the movement of each mobile node, by using cameras or other types of sensors. In this case, the signals (packets) transmitted by a node can always be associated with it even when the node moves from one spot to another.

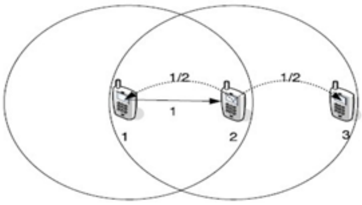

Fig 1. A simple Mobile wireless network

EARLIER APPROACH OF TRAFFIC ON ANONYMOUS SYSTEM

From the past few years, traffic analysis models have been widely investigated for static wired networks. The simplest approach is the brute force in which a message is traced by enumerating all doable links in which a message may traverse. But these attacks did not work properly. Previously, attackers collect information and analysis is performed quietly while not changing the behavior of the network flow. The forerunner attack and the revelation attack are the two representatives. To overcome this, the new numerous techniques have been employed in this paper. The two problems which incurred in the existing paper such as offered mobile computing services in a very commercially viable manner, however terribly difficult as on lives money issue. The next main challenge is to find the best tradeoff between two contradicting objectives: reducing the packet drop and increasing response over the service and also satisfactory computing demands for high end network technique, which may incur huge financial burden.

Network Infrastructure

This specifies point to point message transmission between the nodes, usually nodes can serve as both a host and a router. In this model, every captured packet is treated as evidence supporting a point-to-point transmission between the sender and the receiver. The sender can able to send a message and transmit todestination via multi-hop with split the messages into multiple numbers of packets. The packets can be split based on the size of the file.

Global Traffic Detection

This is to build point-to-point traffic matrices such that two packets captured at different time could be the same packet appearing at different locations, such as the two packets sent by node 1 and node 2 consecutively. A node can be either a sender or a receiver within this time interval. But it cannot be both. Identify those events in the network. Each traffic matrix must correctly represent the one-hop transmissions during the corresponding time interval. The "time slicing" has to make sure that all packets captured in any of the time intervals are independent with each other. In other words, two packets residing in different entries of the same matrix must not be the same packet transmitted through multiple hops.

Super Node

Analyze the traffic in the network, even when nodes are close to each other by treating the close nodes as a super node. STARS does not need the signal detectors to be able to precisely locate the signal source. They are only required to determine which super node (region) the signals are sent from. Moreover, the actual receiver of a point-to-point transmission is not identifiable among all the potential receivers within the sender's transmitting range. This inaccuracy can be mitigated because most potential receivers of a packet will be contained within one or a few super nodes.

Probability Distribution

This module, source/destination and end-end link approaches are partial attacks in the sense that they either only tries to identify the source or destination nodes or to find out the corresponding destination/source nodes for given particular source or destination nodes. The adversaries are not able to determine whether a particular node is a destination depending on whether the node sends out traffic. By using these approaches we find out the actual source and destination of the particular packet and then send the packet to the correct destination.

PROPOSED METHODOLOGY

To disclose the hidden pattern in communication system, our proposed system composed of two steps. First, it constructs point-to-point traffic matrices by using the raw captured packets and constructs end-to-end traffic matrix. Second, it identifies the source node and destination node with the possible probability. This working model is illustrated in Fig.2 in as system architecture that the function taken place. Initially we need to build the point-to-point matrices with the captured packets at the certain period T. Time slicing technique is used to avoid the point-to-point traffic matrix from containing two dependent packets which takes the snapshot of entire network. Fig.2. Working Model of STAR With a sequence of point-to-point traffic matrices we derive the end-to-end traffic matrix. This is termed as accumulative traffic matrix. We assume the timing and hop count thresholds with the end-to-end matrices which do not filter any packet in the network. The deduced end-to-end traffic matrices are still need to perform the further implementation to identify the actual source and destination probability distribution and end-to-end link probability. Finally evaluation is done with the probability distribution vectors in which all the vectors are normalized and it make sense only to the relative orders among the elements of each vector. In this paper, we present different modules such as topology module, attacker's module, etc.

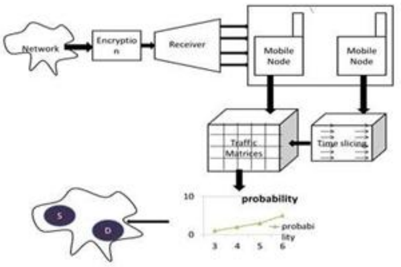

Fig.2. Proposed System Architecture

Proposed Algorithm

Step1: The data is sent from the source.

Step2: The data is passed through the network provider which verifies the sent data.

Step3: The data is divided into several small packets according to thesize of the nearest node.

Step4: The small packets of data are scanned and their performance is checked.

Step5: If the size of the packet match the size of the node, it will be sent to the node.

Step6: If the size of the packet do not match the size of the node, it will be again sent to the network provider for verifying.

Step7: The matched packet of data is sent to the destination.

Step8: The mobile server receives the data without any drop.

Step9: The data is sent to the destination.

CONCLUSION

We studied the fundamental capability of a network in localizing failed nodes from binary measurements (normal/failed) of paths between monitors. We proposed two novel measures: maximum identifiability index that quantifies the scale of uniquely localizable failures wrt a given node set, and maximum identifiable set that quantifies the scope of unique localization under a given scale of failures. We showed that both measures are functions of the maximum identifiability index per node. We studied these measures for three types of probing mechanisms that offer different controllability of probes and complexity of implementation. For each probing mechanism, we established necessary/sufficient conditions for unique failure localization based on network topology, placement of monitors, constraints on measurement paths, and scale of failures. We further showed that these conditions lead to tight upper/lower bounds on the maximum identifiability index, as well as inner/outer bounds on the maximum identifiable set. We showed that both the conditions and the bounds can be evaluated efficiently using polynomialtime algorithms. Our evaluations on random and real network topologies showed that probing mechanisms that allow monitors to control the routing of probes have significantly better capability to uniquely localize failures.

REFERENCES

[1] Liang Ma ; Ting He ; Ananthram Swami ; Don Towsley ; Kin K. Leung, Network Capability in Localizing Node Failures via End-to-End Path Measurements.IEEE/ACM Transactions on Networking (Volume: 25, Issue: 1, Feb. 2017)

[2] A. E. Gamal, J. Mammen, B. Prabhakar and D. Shah, "Throughput-Delay Trade-off in Wireless Networks," Twenty-third Annual Joint Conference of the IEEE Computer and Communications Societies, INFOCOM 2004, vol.1, 2004.

[3] 802.11e IEEE Std. Inform. Technol.–Telecommun. and Inform. Exchange Between Syst.-Local and Metropolitan Area Networks-Specific Requirements Part II:

Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Amendment 8: Medium Access Control (MAC) Quality Service Enhancements, IEEE 802.11 WG, 2005.

[4] Wei Liu, Nishiyama, Ansari, Jie Yang, Kato, "ClusterBased Certificate Revocation with Vindication Capability for Mobile Ad Hoc Networks", IEEE Transactions on Parallel and Distributed Systems, Vol.24, No.2, pp. 239 - 249, 2013.

[5] Yang Qin, Dijiang Huang, Bing Li, "STARS: A Statistical Traffic Pattern Discovery System for MANETs", IEEE Transactions on Dependable and Secure Computing, Vol.11, No.2, pp. 181 – 192, 2014.

[6] L. Romdhani, Q. Ni, and T. Turletti, “Adaptive EDCF: Enhanced service differentiation for IEEE 802.11 wireless ad-hoc networks,” in Proc. Wireless Commun. Networking Conf., vol. 2. New Orleans, LA, 2003, pp. 1373–1378.

[7] J. L. Sobrinho and A. S. Krishnakumar, “Quality-ofservice in ad hoc carrier sense multiple access wireless networks,” IEEE J. Select. Areas Commun., vol. 17, no. 8, pp. 1353–1368, Aug. 1999.

[8] C.-H. Yeh and T. You, “A QoS MAC protocol for differentiated service in mobile ad hoc networks,” in Proc. Int. Conf. Parallel Process., Kaohsiung, Taiwan, Oct. 2003, pp. 349–356.

[9] S. Sivavakeesar and G. Pavlou, “Quality of service aware MAC based on IEEE 802.11 for multihop ad hoc networks,” in Proc. IEEE Wireless Commun. Networking Conf., vol. 3, Atlanta, GA, Mar. 2004, pp. 1482–1487.

[10] A. Chen, Y. T. L. Wang Su, Y. X. Zheng, B. Yang, D. S. L. Wei, and K. Naik, “Nice - a decentralized medium access control using neighbourhood information classification and estimation for multimedia applications in ad hoc 802.11 wireless lans,” in Proc. IEEE Int. Conf. Commun., May 2003, pp. 208–212.

AUTHOR’s PROFILE

AYYALASOMAYAJULA SWATHI is pursuing M.Tech(CSE) in the department of CSE from Kakinada Institute of Engineering & Technology,Korangi.

D.SRINUVAS is working as an Assistant Professor in Department of CSE, Kakinada Institute of Engineering & Technology ,Korangi,Kakinada