Localizing Node Failures in Network Topology and Locations of Monitors

[1]Malla Navya, [2]Dakineni Durga Prasad
[1,2]Dept. of CSE, Baba Institute of Technology and Sciences, Visakhapatnam, AP, India

Abstract
Identifying node failures in wireless networks is extremely testing on the grounds that the network topology can be exceptionally unique, the network may not be constantly associated, and the assets are constrained. In this paper, I adopt a probabilistic strategy and propose two node disappointment discovery conspires that methodically consolidate confined checking, area estimation and node joint effort. Broad recreation results in both associated and detached networks show that our plans accomplish high disappointment recognition rates (near an upper bound) and low false positive rates, and cause low correspondence overhead. Contrasted with approaches that utilization brought together checking, our approach has up to 80% lower correspondence overhead, and just marginally bring down recognition rates and somewhat higher false positive rates. Also, our approach has the preferred standpoint that it is appropriate to both associated and separated networks while incorporated checking is just pertinent to associated networks. Contrasted with different methodologies that utilization restricted checking techniques. The people who can't get information adequately brisk get none by any stretch of the creative energy, paying little mind to the likelihood that they hold up near the supporter. Various mystery enhancing techniques have been proposed in perspective of package encryption to guarantee the correspondence lack of clarity of versatile frameworks. Regardless, in this paper, we exhibit that Mobile wireless Networks are up 'til now vulnerable under segregated statistical traffic examination attacks.

Keywords
Network Tomography, Failure Localization, Identifiability Condition, Maximum Identifiability Index.

I. Introduction

Wireless networks have been utilized for some mission basic applications, including pursuit and safeguard, condition checking, calamity help, and military activities. Such versatile networks are commonly framed in a specially appointed way, with either constant or discontinuous network availability. Nodes in such networks are vulnerable to failures because of battery seepage, equipment deserts or a brutal domain. Node disappointment recognition in portable wireless networks is extremely testing on the grounds that the network topology can be profoundly unique because of node developments [1]. In this way, procedures that are intended for static networks are not relevant. Also, the network may not generally be associated. In this way, approaches depend on network availability have restricted pertinence. Thirdly, the constrained assets (calculation, correspondence and battery life) request that node disappointment discovery must be performed in an asset monitoring way [2]. Node disappointment recognition in portable wireless networks expect network availability. Numerous plans receive test and-ACK (i.e., ping) or pulse based systems that are regularly utilized in appropriated registering. Test and-ACK based systems require a focal screen to send test messages to different nodes. At the point when a node does not answer inside a timeout interim, the focal screen views the node as fizzled. Pulse based procedures vary from test and-ACK based systems in that they take out the examining stage to decrease the measure of messages. A few existing investigations embrace prattle based conventions, where a node, after getting a chatter message on node disappointment data, consolidates its data with the data got, and afterward communicates the joined data [3]. A typical disadvantage of test and-ACK, pulse and prattle based methods is that they are just appropriate to networks that are associated. Also, they prompt a lot of far reaching checking traffic. Interestingly, our approach just creates limited checking traffic and is appropriate to both associated and disengaged networks.

II. Related Work

Traffic analysis attacks against the static wired systems have been all around researched. The animal power assault proposed in [8] tries to track a message by counting every conceivable connection a message could navigate. In hub flushing attacks [9], the aggressor sends a huge amount of messages to the focused on unknown framework (which is known as a blend net). Since the majority of the messages changed and reordered by the framework are created by the assailant, the aggressor can track the rest a couple of (ordinary) messages. The planning attacks as proposed in [10] concentrate on the postponement on every communication way. In the event that the assailant can screen the inactivity of every way, he can relate the messages coming all through the framework by examining their transmission latencies. A planning based approach in [1] to follow down the potential goals given a known source. In this approach, accepting the transmission delays are limited at each hand-off hub, they appraise the stream rates of communication ways utilizing parcel coordinating. At that point in light of the evaluated stream rates, an arrangement of hubs that parcel the system into two sections, one section to which the source can impart in adequate rate and the other to which it can't, are distinguished to appraise the potential goals. An Anonymous On-Demand Routing (ANODR) Protocol [2], is the first to give obscurity and unlinkability to directing in MANETs. ANODR utilizes one-time open/private key sets to accomplish secrecy and unlinkability however neglect to ensure content imperceptibility. An On-Demand Lightweight Anonymous Routing (OLAR)[6] plot which applies the mystery sharing plan in light of the properties of polynomial addition component to accomplish unknown message exchange without per-jump encryptions and decodings. The main assignment for a forwarder is to perform augmentations and duplications, which cost considerably less than conventional cryptographic operations. In [4] Huang formulated a confirmation based statistical traffic investigation show uniquely for MANETs. In this model, each caught bundle is dealt with as confirmation supporting a point to point (one-bounce) transmission between the sender and the beneficiary. A succession of point to point traffic grids is made, and after that they are utilized to determine end to end relations. This approach gives a pragmatic assaulting system against MANETs yet at the same time leaves significant data about the communication designs unfamiliar. To start with, the plan neglects to address a few imperative compels (e.g., most extreme bounce check of a bundle) when inferring the conclusion to-end traffic from the one

jump confirmations. Second, it doesn't give a strategy to recognize the real source and goal hubs. In addition, it just uses a credulous collective traffic proportion to construe the conclusion to-end communication relations (e.g., the likelihood for hub j to be the expected goal of hub i is processed as the proportion of the traffic from i to j to all traffic turning out from hub i), which brings about a great deal of mistake in the inferred likelihood conveyances. To gauge the unlinkability, Huang proposed an answer incorporate the accompanying parts: (i) the transmission model and channel demonstrate for IEEE 802.11b conventions, (ii) an unlinkability assessment display utilizing proof hypothesis, and (iii) a recreation concentrate to approve the proposed models in light of a settled wireless communication framework. Because of the one of a kind qualities of MANETs, exceptionally constrained analysis has been led on traffic investigation with regards to MANETs. In 2008 H.wong et al. proposed a planning based approach in to follow down the potential goals given a known source. In this approach, expecting the transmission delays are limited at each transfer hub, they assess the stream rates of communication ways utilizing parcel coordinating. At that point in light of the evaluated stream rates, an arrangement of hubs that parcel the system into two sections, one section to which the source can impart in adequate rate and the other to which it can't, are recognized to appraise the potential goals.

In [1] the creators utilized Reactive Two-stage Rerouting (RTR) for intra area directing with briefest way recuperation. This convention is utilized to recoup systems from expansive scale disappointments by utilizing two stages. In first stage the RTR advances the parcels towards the neighbor to accumulate the disappointment data and store it in the bundle header. In the second stage it discovers another most brief way and detours the disappointment district which is autonomous of shape and area. This technique accomplishes great execution with 98.6% dependability with least system assets. In [8] the creators utilized various reinforcement ways which is predefined and put away in the hash table. Probabilistically Correlated Failure (PCF) model with a layer mapping methodology is utilized which minimizes and evaluates the IP join disappointment and gives solid reinforcement ways as well. On the off chance that an IP connection comes up short, its movement is part into numerous reinforcement ways such that the rerouted activity ought not surpass the usable data transmission. The creators utilized ISP systems with both optical and IP layer topologies. At least two reinforcement ways are chosen to give unwavering quality up to 18% and the steering disturbance is diminished to around 22%. Thus the interface between rerouted activity and typical movement is stayed away from for this situation. In [9] the creators utilized CP-ABE calculation implied for acknowledging complex access control on scrambled information. By this system the encoded information can be kept classified regardless of the possibility that the stockpiling server is untrusted; in addition, this technique is secure against arrangement assaults. In this technique the ascribes are utilized to depict a client's accreditations, and a gathering encoding information decides an arrangement for who can decode.

A. IP Link Protection Based on Backup Path

Consider backup path selection as a connectivity problem and mainly focus on finding backup paths to bypass the failed IP links. Consequently, the rerouted traffic may causes severe link overload on an backbone IP networks as they ignore the fact that a backup path may not having enough bandwidth as observed by [10]. In recent work, we develop CPF model to highlight the probabilistic correlation between logical link failures, and split the rerouted traffic onto multiple backup paths to avoid link overload and minimizes routing disruption.

B. Correlation between the Logical and Physical Topologies

IP-over-WDM networks consider the correlation between the physical and logical topologies. Minimizing the impact based on fiber and logical links failures [7], showed that topology mapping is strongly affected by the reliability of IP layer. Moreover, our approach is based on a cross-layer design. They aim at finding reliable backup paths; while our objective is to minimize routing disruption. Our paper also considers the topology mapping, but it is different in two aspects. First, the CPF model considers both independent and correlated logical link failures. Second, Multiple backup paths protects each logical link in this paper, But protected by single backup path in [15]

C. Allocation of Bandwidth and Multipath Routing

Quality-of-Service (QoS) routing protocols [5], use multiple paths between a source-destination to achieve traffic engineering goals, e.g., minimizing the maximal link utilization. However, they do not consider the correlation between physical and logical link failures. There are some recovery approaches that are built on multiple recovery paths. The approach in [9] aims at minimizing the bandwidth reserved for backup paths. It assumes that the network has a single logical link failure and only uses IP layer information for backup path selection. IN [4] reroutes traffic with multiple paths and the method in [8] combine addresses failure recovery and traffic engineering in multipath routing. Moreover, they ignore the correlation between logical link failures and consider backup paths should have same reliability and they focus on traffic engineering goals rather than minimizing routing disruption.

III. 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.

A. 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.

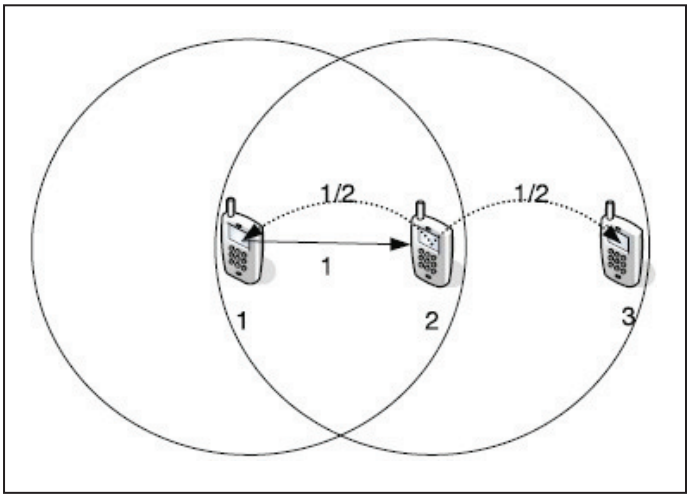

Fig. 1: A Simple Mobile Wireless Network

IV. 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.

A. 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.

B. 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.

C. 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.

D. 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.

V. 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.

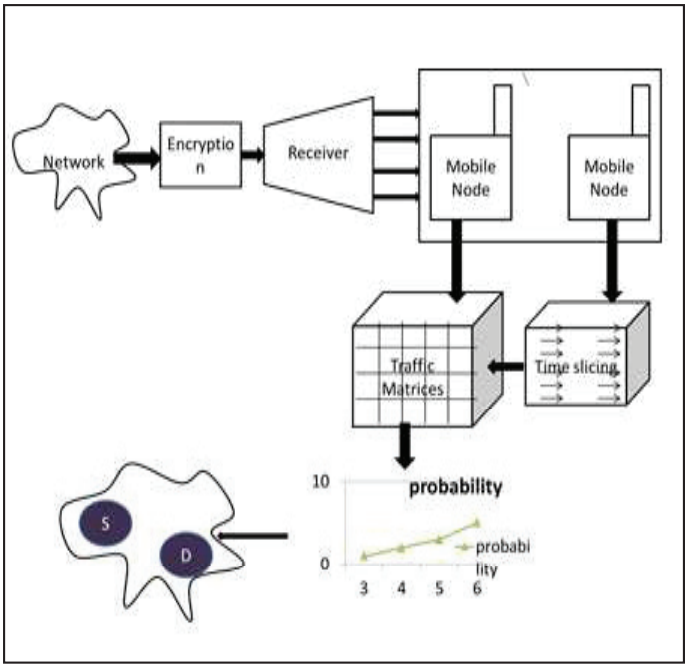

Fig. 2: Proposed System Architecture

Proposed Algorithm

Step 1: The data is sent from the source.
Step 2: The data is passed through the network provider which verifies the sent data.
Step 3: The data is divided into several small packets according to thesize of the nearest node.
Step 4: The small packets of data are scanned and their performance is checked.
Step 5: If the size of the packet match the size of the node, it will be sent to the node.
Step 6: 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.
Step 7: The matched packet of data is sent to the destination.
Step 8: The mobile server receives the data without any drop.
Step 9: The data is sent to the destination.

VI. 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, Vol. 25, Issue 1, 2017.
[2] A. E. Gamal, J. Mammen, B. Prabhakar, 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, 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, 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, 1999.
[8] C.-H. Yeh, 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, 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, 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., pp. 208–212, 2003.

Malla Navya Holds a B.Tech certificate in Computer Science Engineering from the University of JNTU Kakinada. She presently Pursuing M.Tech (CSE) department of computer science engineering from Baba Institute of Technology and Sciences, Visakhapatnam, AP, India.

Dakineni Durga Prasad, B.TECH, M.TECH is working as an Assistant Professor in the Department of Computer Science and Engineering in Baba Institute of Technology and Sciences, Visakhapatnam, A.P, India.