The Secure Routing Protocol for Traffic analysis attacks in MANET

Inukonda Rama Devi[1], Dr. B V Ram Kumar[2], Dr. G. Satyanarayana[3]
#1 M.Tech Scholar and Department of Computer Science Engineering,
#2 Professor, Department of Computer Science and Engineering, DNR College Of Engineering and Technology, Bhimavaram, AP, India.
#3 Professor, HOD Department of Computer Science and Engineering, DNR College Of Engineering and Technology, Bhimavaram, AP, India.

Abstract

Privacy and security have emerged as an important research issue in mobile Networks wireless communication, Mobile device based data scattering applications that use these abilities. This paper proposes TurfCast, a novel data spread administration that specifically communicates data specifically "turfs," conceptual coherent spaces in which beneficiaries are arranged. Such turfs can be transient or spatial in view of recipients' waiting time or physical zones, individually. TurfCast has numerous applications, for example, electronic nearness promoting and mobile long range interpersonal communication. The individuals who can't get data sufficiently quick get none by any stretch of the imagination, regardless of the possibility that they wait close to the supporter. Numerous secrecy improving strategies have been proposed in view of bundle encryption to ensure the communication obscurity of mobile systems. In any case, in this paper, we demonstrate that Mobile wireless Networks are as yet vulnerable under detached statistical traffic investigation attacks. To exhibit how to find the communication designs without unscrambling the caught bundles, we show TurfCast. It works latently to perform traffic investigation in view of statistical qualities of caught crude traffic. These are fit for finding the sources, the goals, and the conclusion to-end communication relations. Exact analysiss show that accomplishes great precision in uncovering the shrouded traffic designs.

Keywords: Anonymity enhancing techniques, mobile ad-hoc networks, point-to-point transmission, statistical traffic pattern analysis

I. Introduction

TurfCast is a novel administration that use receivers' "turfs" to specifically spread data. Turfs are theoretical coherent in which certain beneficiaries are arranged. Illustration such turfs can be fleeting, in view of the measure of time collectors wait, or spatial, in light of recipients' differing areas or domains. TurfCast's key thought is to spread separated data to various turfs by means of broadcasting. Just "qualified" individuals, i.e. those in one specific turf, can get a specific measure of data. Wireless Networks is a foundation less, wireless and self-arranging system of mobile devices with no brought together administration. These are for the most part utilized as a part of the military field. It is anything but difficult to convey the system with no preplanned. In Wireless Networks to enhance the protected communication, Anonymous Communication is utilized. Unknown communication conceals the connection between the source and goal. It is hard to discover the source or goal of the communication connect and the other middle of the road hubs engaged with it and finding the data or information move through the system. For doing unknown communication in the Wireless Networks numerous mysterious steering conventions are utilized as a part of impromptu directing, for example, MASK. To enhance the secrecy of the communication numerous methods are utilized like onion directing (Reed et al.2002) with the MASK and OLAR conventions which incorporates the different layers of encryption of information. It shrouds the steering data and character of hubs from the aggressor hubs. The obscurity improving systems are utilized to secure the Wireless Networks. The steering data's are recognized by means of the detached attacks which won't interfere with the system condition. Traffic analysis is utilized to track the information. There are many traffic investigation techniques accessible yet they are not well productive in breaking down the traffic in light of the three natures of Wireless Networks. They are communicating nature, specially appointed nature and mobile nature. By methods for broadcasting nature, the parcels are transmitted among hubs where, it is hard to distinguish sender and collector. By methods for specially appointed nature, it is more workable for

a hub to carry on both as sender and recipient. By methods for mobile nature, it is anticipated that the hubs are in versatility; which prompts the Wireless Networks condition to be more unpredictable, for performing analysis. The Mobile specially appointed systems are normally inclined to security dangers and physical security breech comprises of spying, parodying and other sort of system attacks are conceivable to be happened. The primary physical security dangers jeopardized are inactive and dynamic attacks which are more vulnerable to dynamic shaky wireless communication [7]. They alter the hub security and breaking point the energy of hubs without its framework which needs in settled system topology. In an impermanent and dynamic system condition of gathering of mobile hubs with radio recurrence handsets speak with each other [8]. For any unified set up framework for directing the intercession for transmitting the constrained scope of every mobile hub. Assume by sending the messages for accepting the goals which have dependable that can be exceptionally malevolent and risk to security and privacy of information. Dissecting the communication design in the information encryption can secure he traded substance of information in the mobile hubs. Important data about the communication examples of end clients can give security and protection approach of analysis of traffic [9]. Setting up unknown way can trade the steering data viably.

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.

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.

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.

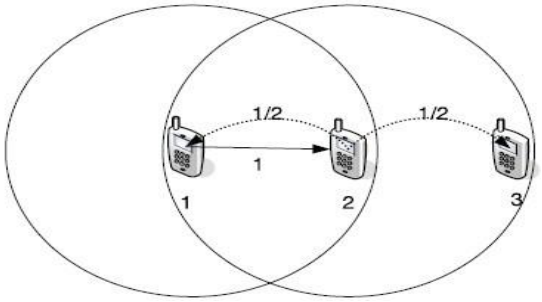

Fig 1. A simple Mobile wireless network

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.

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 to destination 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.

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.

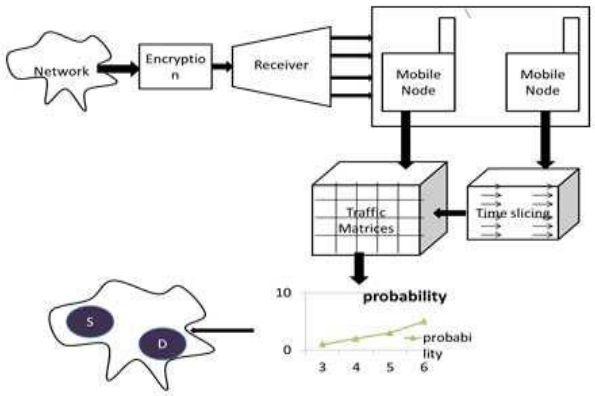

Fig.2. Proposed System Architecture

Proposed Algorithm

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 the size 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.

VII. Conclusion

This paper proposed a routing mechanism in order to ensure QoS through packet scheduling strategy. A strategic MAC and QoS-aware neighbor node selection mechanism is used to meet the transmission delay requirement among the mobile nodes. A distributed packet scheduling mechanism for reducing the transmission delay of packets is also presented. Packet resizing mechanism is proposed that is capable enough to adjust the segment size of the packet in adaptive manner. The simulation is carried out based on pause time and mobility speed. Mobility speed is taken for ensuring the protocol's performance on heterogeneous ad hoc networks. Simulation results prove that the proposed mechanism attains better QoS in terms of throughput, packet delivery ratio, overhead, packets drop and delay based on both pause time and mobility speed. The proposed system will observe the traffic pattern of the adversary. As nodes are hidden in mobile networks a heuristic searching algorithm will be applied. Nodes. Probability of point to point transmission among receivers will be estimated by point-to-point traffic matrix. Then multihop traffic and performing probability distribution the traffic pattern will be discovered. This will provide an approximate traffic pattern with approximate source and destination in the network. The proposed system will reduce the issue of anonymous communication in mobile networks.

Future Scope: Furthermore, to analyze the traffic before sending the packets to the destination. For single destination which have many paths to reach from source. So in case of traffic, user can choose an alternate way to send a message to destination.

References

[1] P. Gupta and P. R. Kumar, "The capacity of wireless networks," IEEE Transactions on Information Theory, vol. 46, no. 2, pp. 388 – 404, 2000.

[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.

Authors

INUKONDA RAMA DEVI holds a B.Tech Degree in Computer science & Engineering from GVIT College of Engineering and Technology, Vempa road Bhimavaram west godavari district Andhra Pradesh. she is presently pursuing M.Tech in Department of Computer science from DNR College of Engineering and Technology.

Dr. B V Ram Kumar M.E, Ph.D is working as a Professor, Department of Computer Science and Engineering, DNR College Of Engineering and Technology, Bhimavaram, West Godavari District, Andhra Pradesh, India, with an experience of 23 years.

Dr. G. Satyanarayana is working as a Professor and HOD in the Department of Computer Science and Engineering, DNR College Of Engineering and Technology, Bhimavaram, West Godavari District, Andhra Pradesh, India.