ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 4, Special Issue 11, September 2015

National Conference on Emerging Trends in Computing, Communication & Control Engineering [NCET 2K15]

On 4th September, 2015

Organized by

Department of CSE, ECE & EEE, Magna College of Engineering, Chennai-600055, India.

Novel Statistical Traffic Pattern Discovery System to Protect MANETS from Vulnerability

Dr. G. Arul Dalton[1], A.Bamila Virgin Louis [2]

Professor and Head, Dept. of CSE, Magna College of Engineering, Chennai, Tamil Nadu, India[1]

Assistant Professor, St. Xavier's Catholic College of Engineering, Tamil Nadu, India[2]

ABSTRACT: Number of techniques has been proposed based on packet encryption to protect the communication in MANETs; Still MANETs are vulnerable to certain statistical traffic analysis attacks. In this paper we present a Novel statistical traffic pattern discovery system (STARS). STARS functioning based on statically characteristics of captured raw traffic. STARS discover the relationships of source to destination communication. Studies conclude STARS achieve good accuracy in hidden traffic patterns. In this traffic pattern we aims to derive the source/destination probability distribution, i.e., the probability for each node to be a message source/destination, and the end-to-end link probability distribution, i.e., the probability for each pair of nodes to be an end-to-end communication pair. Here we construct point-to-point traffic matrices using the time-slicing technique, and then derive the end-to-end traffic matrix with a set of traffic filtering rules; and apply a heuristic nodes, and then correlate the source nodes with their approach to identify the actual source and destination corresponding destinations.

KEYWORDS: Traffic, Matrix, Link Probability

I. INTRODUCTION

Mobile Adhoc Network (MANET) is a wireless network consisting of a collection of mobile nodes with no fixed infrastructure. In MANET, all nodes are mobile and connected dynamically in an arbitrary manner. Each node behaves as a router and takes part in discovery and maintenance of routes to others in the network. The nodes can move freely at any time, so the network structure changes dynamically due to mobility. The main characteristics of the MANET are dynamic topology, bandwidth constrained, variable capacity links, energy constrained operation, limited physical security and quickly deployable. .The research challenges in MANET are related to routing, security, reliability, scalability, quality of service, internetworking, power consumption and multimedia applications. The routing protocols designed for wired networks are not suitable for wireless networks due to the node mobility. The routing problem becomes more serious in the MANET due to lack of infrastructure.

The different protocols are proposed to deal with routing problem in the MANET. These routing protocols can be classified into two main categories namely table driven routing protocol and on-demand routing protocol. The protocols to be used in the MANET should have the following features .

The protocol should adapt quickly to topology changes and should provide loop free routing. The protocol should provide multiple routes from the source to destination; this will solve the problems of congestion to some extent and supports reliability in case of link or node failure.

The protocol should have minimum control message overhead due to exchange of routing information when topology changes occur. The protocol should use minimum resources like bandwidth, power and should support Quality of Service (QoS) and security. Becomes more serious in the MANET due to lack of infrastructure.

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 4, Special Issue 11, September 2015

National Conference on Emerging Trends in Computing, Communication & Control Engineering [NCET 2K15]

On 4th September, 2015

Organized by

Department of CSE, ECE & EEE, Magna College of Engineering, Chennai-600055, India.

The different protocols are proposed to deal with routing problem in the MANET. These routing protocols can be classified into two main categories namely table driven routing protocol and on-demand routing protocol. The protocols to be used in the MANET should have the following features[1].

The protocol should adapt quickly to topology changes and should provide loop free routing. The protocol should provide multiple routes from the source to destination; this will solve the problems of congestion to some extent and supports reliability in case of link or node failure. The protocol should have minimum control message overhead due to exchange of routing information when topology changes occur. The protocol should use minimum resources like bandwidth, power and should support Quality of Service (QoS) and security.

Performance gains can significantly improve the scalability, the delay performance and the throughput .The cross-layer approaches have increasingly attracted the attention of researchers and communication system designers, this attention came from the challenging networking environments such as MANETs, next generation cellular networks or sensor networks.

This papers aims to overcome mobile adhoc network performance problems by allowing protocols belonging to different layers to cooperate and share network information while still maintaining separated layers. Rest of the paper is organized as follows. Section 2 describes related work and motivation, the proposed work is discussed in section 3, section 4 describes the simulation and results. Conclusions and future work are presented in section 5.

II. RELATED WORK

1) Ad-hoc On-Demand Distance Vector Routing----> Charles E. Perkins, Elizabeth M. Royer. In this paper, author presents Ad-hoc On Demand Distance Vector Routing (AODV), a novel algorithm for the operation of such ad-hoc networks. Each Mobile Host operates as a specialized router, and routes are obtained as needed (i.e., on-demand) with little or no reliance on periodic advertisements. Pros and cons: AODV is an on demand routing protocol in which routes are established on demand and destination sequence numbers are used to find the latest route to the destination. The connection setup delay is less. The HELLO messages supporting the routes maintenance are range-limited, so they do not cause unnecessary overhead in the network but the intermediate nodes can lead to inconsistent routes if the source sequence number is very old and the intermediate nodes have a higher but not the latest destination sequence number, thereby having stale entries.

2) Routing Overhead as A Function of Node Mobility: Modeling Framework and Implications on Proactive Routing---->Xianren Wu, Hamid R. Sadjadpour and J.J.Garcia-Luna-Aceves. In this paper, author presents a mathematical framework for quantifying the overhead of proactive routing protocols in mobile ad hoc networks (MANETs). He focus on situations where the nodes are randomly moving around but the wireless transmissions can be decoded reliably, when nodes are within communication range of each other. Pros and cons: In this paper author explains to reduce overhead problem in the proactive type routing protocols but not discussed about the overhead problem in the reactive type routing protocols.

3) A survey of data replication techniques for mobile ad hoc network databases---> Prasanna Padmanabhan, Le Gruenwald, Anita Vallur, Mohammed Atiquzzaman. In this paper, author presented a survey and classification of data replication techniques for MANET databases and identified the issues to be considered when developing a replication technique for such databases. He compared the Existing replication techniques based on how they addressed the identified issues. Pros and cons: In this paper author identifies issues involved in MANET data replication and attempts to classify existing MANET data replication techniques based on the issues they address and it also discuss on future research directions.

4) Cooperation in Wireless Ad Hoc Networks---> Vikram Srinivasan, Pavan Nuggehalli, Carla F. Chiasserini, Ramesh R. Rao. In wireless ad hoc networks, nodes communicate with far off destinations using intermediate nodes as relays.

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 4, Special Issue 11, September 2015

National Conference on Emerging Trends in Computing, Communication & Control Engineering [NCET 2K15]

On 4th September, 2015

Organized by

Department of CSE, ECE & EEE, Magna College of Engineering, Chennai-600055, India.

Since wireless nodes are energy constrained, it may not be in the best interest of a node to always accept relay requests. On the other hand, if all nodes decide not to expend energy in relaying, then network throughput will drop dramatically. Both these extreme scenarios (complete cooperation and complete noncooperation) are inimical to the interests of a user. In this paper, author addresses the issue of user cooperation in ad hoc networks. We assume that nodes are rational, i.e., their actions are strictly determined by self interest, and that each node is associated with a minimum lifetime constraint. Given these lifetime constraints and the assumption of rational behavior, we are able to determine the optimal throughput that each node should receive. Pros and cons: In this paper author proposes a distributed and scalable acceptance algorithm called Generous TIT-FOR-TAT and it is used by the nodes to decide whether to accept or reject a relay request but it assume that all rational nodes can determine their own optimal strategies to maximize their profit.

5) A Routing Strategy for Mobile Ad-hoc Networ in City Environments---> Christian Lochert, Hannes Hartenstein, Jing Tian, Holger Füßler Dagmar and Hermann Martin Mauve.
In this paper, author analyze a position-based routing approach that makes use of the navigational systems of vehicles and compare this approach with non-position-based ad-hoc routing strategies (Dynamic Source Routing and Ad-Hoc On-Demand Distance Vector Routing).
The first detailed micro-level analysis of pathologies for geographic face-based routing protocols, in the presence of location errors in static sensor networks was done but the Location errors can severely degrade performance in location-based forwarding schemes, making accurate location information a necessity for most geographic routing protocols.

III. PROPOSED WORK

The main aim of proposed method is to study traffic analysis attacks and to discover the communication pattern between the source and destination. Also help to find the raw traffic and hidden traffic between the source and destination. This can be achieved by the following modules.

3.1.1 Network

A MANET is represented by undirected graph, G= (V,E) where V is the set of nodes and E is the set of bidirectional links. It is assumed that, at any time, nodes are situated randomly throughout the network area in accordance with a two-dimensional uniform random variable distribution. Each node is equipped with a single network interface card and has a transmission radius of r. If the distance separating a pair of nodes is less than r, then bidirectional link connects them and they are considered to be neighbours. Otherwise, the nodes are not connected. Each node is assumed to have fixed velocity and have uniformly distributed. Each node randomly chooses a new direction. The mobility is defined as the distance moved per unit time by a node in the network. Suppose at time t1 the node ni is at (x1, y1) and by time t2 the node ni has moved to (x2, y2), then the mobility of the node ni denoted by.
Each node has a cost. It is assumed that the number of route requests is denoted by λ follows poison process and call holding time follows exponential distribution, when a route request occurs. Two nodes are randomly selected as source and destination.

3.1.2 Bandwidth Estimation

The bandwidth estimation is most important to provide QoS in MANET, the nodes share the bandwidth with their neighbors and thus the bandwidth available to a node is a dynamic value that is affected by its neighbors' traffic. Therefore, the two key problems in bandwidth estimation are how exactly to estimate the available bandwidth and how frequently to do the estimations. Also, the trade-off between the benefit from using bandwidth estimation and the cost in terms of packet overhead and computing resources used for the bandwidth estimation is another key issue. A node's available bandwidth is not only decided by the raw channel bandwidth, but also by its neighbor's bandwidth usage and interference caused by other sources, each of which reduces a node's available bandwidth for transmitting data.

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 4, Special Issue 11, September 2015

National Conference on Emerging Trends in Computing, Communication & Control Engineering [NCET 2K15]

On 4th September, 2015

Organized by

Department of CSE, ECE & EEE, Magna College of Engineering, Chennai-600055, India.

However, the bandwidth estimation is extremely difficult, because each node has imprecise knowledge of the network status and links change dynamically. Therefore, an effective bandwidth estimation scheme is highly desirable. The bandwidth estimation can be done using various methods[19]. Here, it uses following efficient technique, which in turn induces only little bit overhead and does not take any extra time, it is clearly explained in section 3.2.2.

To know the frequency reuse pattern, we first study the underlying IEEE 802.11 MAC. As defined in the IEEE 802.11 MAC, the nodes are allowed to access the wireless channel when the media is free. The media can be free if no nodes are transmitting packets within the interference range. Normally, the interference range is twice the transmission range, based on the settings of the 914MHz Lucent Wave LAN card. Therefore, the frequency can be reused outside of the second neighbouring node's range. The actual upper bound of the bandwidth in the two-hop circle varies with the topology and the traffic status, but the raw channel bandwidth is the soft upper bound of total bandwidth [19]. It uses soft upper bound bandwidth in the estimation to approximate the bandwidth usage. With the above frequency reuse pattern, it can simplify the bandwidth calculation problem for determining the residual bandwidth within the two-hop neighbourhood range. Therefore, each node can approximate its residual bandwidth information based on the information from nodes within two-hops(the interference range.

The residual bandwidth is simply the raw channel bandwidth minus the overall consumed bandwidth, divided by a weight factor. It needs to divide the residual bandwidth by a weight factor due to the IEEE 802.11 MAC nature and some overhead required by the routing protocol. So bandwidth of ni is denoted by

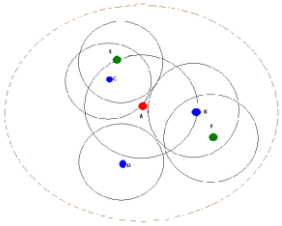


Fig. The outside big dotted circle indicates node A's interference range and the other small-size circles indicate node A and its neighbors' transmission ranges.

3.1.3 Route Discovery The route selection is based on the route discovery. In order to facilitate the computation of multiple node disjoint paths from the source to destination, it chooses an Adhoc On-Demand Distance Vector Multipath (AODVM) protocol as a candidate protocol and makes modifications to it to enable the discovery of such paths to support QoS. The AODVM is the extension of AODV to provide multiple nodes disjoint paths. Here, we briefly describe the AODV and AODVM. The on demand routing protocols consume low overhead than pro-active routing protocols. Second, as compared to DSR, the AODV avoids the high source routing overhead. The AODV provides loop-free routes using sequence numbers that indicates how new, or fresh, a route is. When a source node desires a route to a destination for which it does not have a route, it broadcast a Route Request (RREQ) packet across the network. The nodes receiving this and update routing information for the source node and set up backwards pointers to the source node in the route tables is sown. In addition to the source node's ID, current sequence number, and broadcast ID, it also contains the most recent sequence number for the destination of which the source node is aware. The source sequence number is used to maintain freshness information about the reverse route to the source. This is to make sure that packets from the destination to the source follow a path, which was set up by the route request packet for this session.

The destination sequence number specifies how fresh a route to the destination must be before it can be accepted by the source. A node receiving the RREQ may send a Route Reply (RREP) packet if it is either the destination or if it has a route to the destination with corresponding sequence number greater than or equal to that contained in the RREQ packet. If this is the case, then it uses a RREP packet back to the source. Otherwise, it rebroadcast the RREQ packet. All nodes keep track of the RREQ's source IP address and broadcast ID. If they receive a RREQ packet, which they

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 4, Special Issue 11, September 2015

National Conference on Emerging Trends in Computing, Communication & Control Engineering [NCET 2K15]

On 4th September, 2015

Organized by

Department of CSE, ECE & EEE, Magna College of Engineering, Chennai-600055, India.

have already processed, then it discards a RREQ packet and does not forward it. The RREP packet propagates back to the source, nodes set up forward pointers to the destination. Once the source node receives the RREP packet, it may begin to forward data packets to the destination.

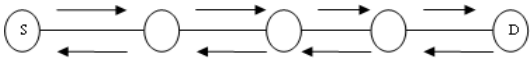


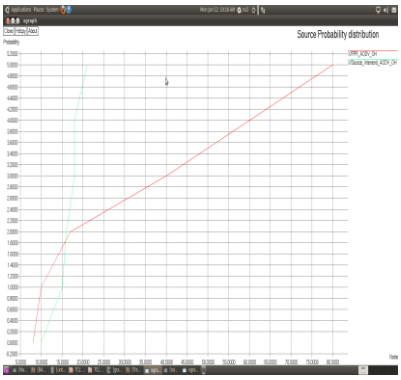
Fig. Propagation of RREQ.

The AODVM is based on AODV. The propagation of RREQ packet follows the same rule as the basic AODV except the intermediate nodes are disallowed to send route replies back to the source. Although not further propagated, duplicate RREQ packet received at an intermediate node are processed for possible alternate path back to the source. Every node maintains a RREQ table which keeps track of all the neighbours from which a RREQ packet is received and the corresponding cost (hop-count) back to the source. When a RREQ packet reaches the destination, a RREP packet is generated and sent back to the last hop node from which the destination receives the RREQ packet. The RREP packet contains an additional field last hop ID to indicate the last hop node (i.e., the neighbour of the destination). The RREP packet may not follow the exact reverse path. Instead, an intermediate node determines which next hop node the RREP packet should be sent based on the information saved in the RREQ table. When an intermediate node receives a RREP packet, it finds from its RREQ table using a shortest path back to the source and sends the RREP packet to the corresponding next node.

3.1.4 Star: STAR is the technique; it will create source/destination probability distribution for each and every node to be a message source and destination and the end-to-end link probability distribution (the probability for each node to be an end-to-end communication pair).

3.1.4.1 Traffic Protector: In this module, first it uses the captured traffic to construct a sequence of point-to-point traffic matrices and then derives the end-to-end traffic matrix. Second, further analyzing the end-to-end traffic matrix, it calculates the probability for each node to be a source/destination (the source/destination probability distribution) and that for each pair of node to be an end-to-end communication link (the end-to-end link probability distribution). Finally it will hide the traffic pattern between actual source and destination from disclosure nodes.

4.1. Routing Overhead: It is equal to the number of routing packets transmitted per data packet delivered at destination. Each hop-wise transmission of a routing packet is counted as one transmission. It is also known as Normalized Routing Load (NRL). It is also defined as



NRL =Number of control packets generated /number of received data packets

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 4, Special Issue 11, September 2015

National Conference on Emerging Trends in Computing, Communication & Control Engineering [NCET 2K15]

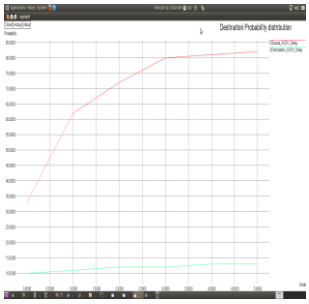
On 4th September, 2015

Organized by

Department of CSE, ECE & EEE, Magna College of Engineering, Chennai-600055, India.

The routing overhead is an important metric to compare the performance of different protocols since it gives a measure of the efficiency of protocols, especially in a low bandwidth with congested wireless environments. Protocols that transmit a large number of packets can also increase the probability of packet collisions and waiting time of data packets in transmission buffer queues.

4.2. End -To-End Delay: The delay of data propagation, transfer and the delays caused by buffering, queuing and retransmitting data packets. The delay of each packet is computed as the time of received data packets minus the time of sent this data packet. The average end to end delay is then computed as:



Average delay =Total delay of each data packets /total data packets received.

Generally, there are three factors affecting end-to-end delay of a packet: (i) Route discovery time, which causes packets to wait in the queue before a route path is found. (ii) Buffering waiting time, which causes packets to wait in the queue before they can be transmitted. (iii) The length of routing path. The more number of hops a data packet has to go through, the more time it takes to reach its destination node. In real time communications, since packets which arrive late could be useless although they reach the destination successfully. Real time traffic is delay sensitive.

IV. CONCLUSIONS AND FUTURE WORK

In our work we concentrated on a statistical traffic pattern discovery system for mobile adhoc networks. These systems are mainly depending on an attacking system that's help to capture raw traffic based on Mac layer condition without the knowledge of intermediate packets. Here we done an end to end and point to point traffic analyze to find hidden traffic to make communication in manet as restricted communication.

REFERENCES

[1] Lee, S.E., and Gerla ,M., 2001, "Split Multipath Routing with Maximally Disjoint Paths in Adhoc Networks", *In Proceedings of IEEE ICC*, pp. 3201-3205.
[2] X. Wang, S. Chen, and S. Jajodia, "Network Flow Watermarking Attack on Low-Latency Anonymous Communication Systems," Proc. IEEE Symp. Security and Privacy, pp. 116-130, 2007.
[3] Y. Zhang, W. Liu, W. Lou, and Y. Fang, "MASK: Anonymous On Demand Routing in Mobile Ad Hoc Networks," IEEE Trans. Wireless Comm., vol. 5, no. 9, pp. 2376-2385, Sept. 2006.
[4] M. Wright, M. Adler, B. Levine, and C. Shields, "The Predecessor Attack: An Analysis of a Threat to Anonymous Communications Systems," ACM Trans. Information and System Security, vol. 7, no. 4, pp. 489-522, 2004.
[5] G. Danezis, C. Diaz, and C. Troncoso, "Two-Sided Statistical Disclosure Attack," Proc. Seventh Int'l Conf. Privacy Enhancing Technologies, pp. 30-44, 2007.
[6] D. Chaum, "The Dining Cryptographers Problem: Unconditional Sender and Recipient Untraceability," J. Cryptology, vol. 1, no. 1, pp. 65-75, 1988.
[7] Y. Liu, R. Zhang, J. Shi, and Y. Zhang, "Traffic Inference in Anonymous MANETs," Proc. IEEE Seventh Ann. Comm. Soc. Conf. Sensor Mesh and Ad Hoc Comm. and Networks (SECON '10), pp. 1-9,
2010.
[8] Y. Zhang, W. Liu, W. Lou, and Y. Fang, "MASK: Anonymous On-Demand Routing in Mobile Ad Hoc Networks," IEEE Trans. Wireless Comm., vol. 5, no. 9, pp. 2376-2385, Sept. 2006.

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 4, Special Issue 11, September 2015

National Conference on Emerging Trends in Computing, Communication & Control Engineering [NCET 2K15]

On 4th September, 2015

Organized by

Department of CSE, ECE & EEE, Magna College of Engineering, Chennai-600055, India.

[9] S. Seys and B. Preneel, "ARM: Anonymous Routing Protocol for Mobile Ad Hoc Networks," Proc. IEEE 20th Int'l Conf. Advanced Information Networking and Applications Workshops (AINA Work- shops '06), pp. 133-137, 2006.
[10] J. Kong, X. Hong, and M. Gerla, "An Identity-Free and On-Demand Routing Scheme against Anonymity Threats in Mobile Ad Hoc Networks," IEEE Trans. Mobile Computing, vol. 6, no. 8,pp. 888-902, Aug. 2007.
[11] Zhenqiang, Y., Krishnamurthy S. V and Tripathi S. K., 2003, "A Framework for Reliable Routing in Mobile Adhoc Networks", *In Proceedings of IEEE INFOCOM*, Vol. 1, pp. 270 -280.
[12] G. Danezis, "Statistical Disclosure Attacks: Traffic Confirmation in Open Environments," Proc. Security and Privacy in the Age of Uncertainty (SEC '03), vol. 122, pp. 421-426, 2003.
[13] W. Dai, "Two Attacks against a PipeNet-Like Protocol Once Used by the Freedom Service," http://weidai.com/freedom-attacks.txt, 2013.
[14] Y. Qin and D. Huang, "OLAR: On-Demand Lightweight Anonymous Routing in MANETs," Proc. Fourth Int'l Conf. Mobile Computing and Ubiquitous Networking (ICMU '08), pp. 72-79, 2008.
[15] D. Chaum, "Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms," Comm. ACM, vol. 24, no. 2, pp. 84-88, 1981.