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

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 6, June 2016

GSTAR: Generalized Statistical Traffic Pattern Analysis System in MANETs for Anonymous Communication

Prabhu K [1], Sangeetha S [2]

Assistant Professor, Department of Computer Science and Engineering, VSB College of Engineering Technical Campus, Coimbatore, TamilNadu, India[1]

Associate Professor, Department of Computer Science and Engineering, VSB College of Engineering Technical Campus, Coimbatore, TamilNadu, India[2]

ABSTRACT: Anonymous Communication is the main issue in case of MANETs (Mobile Ad hoc Networks). Many anonymity enhancing techniques have been proposed based on packet encryption to protect the communication anonymity of mobile ad hoc networks. It is difficult to find the source and destination of the communication link and the other nodes involved in it. MANETs are still vulnerable under passive statistical traffic analysis attacks due to the open communication environment. Communication anonymity [1] is a critical issue in MANETs, which generally consists of the following aspects: i) Source/destination anonymity ii) End-to-end relationship anonymity. The scheme fails to address several important constrains when deriving the end-to-end traffic from the one hop evidences. In the proposed system GSTAR (Generalized Source Tree Adaptive Routing) using Statistical method are capable of discovering the sources, the destinations, and the end-to-end communication relations. It provides anonymous connections that are strongly resistant to both eavesdropping and traffic analysis. To disclose the hidden traffic patterns in a MANET communication system, the proposed system involves the statistical parameters to calculate the probability values of source and destination nodes. It uses the captured traffic to construct a sequence of point-to-point traffic matrices and then derives the end to end traffic matrix [1].

KEYWORDS: Anonymous communication, MANET, GSTAR, Routing, Traffic analysis.

I. INTRODUCTION

MANETs consist of a peer-to-peer self forming, self-healing network in contrast to a mesh network has a central controller. Each device in a MANET is free to move independently in any direction, and change its links to other devices frequently. The primary challenge in building a MANET is equipping each device to continuously maintain the information required to properly route traffic. Such networks may operate by themselves or may be connected to the larger Internet. They may contain one or multiple and different transceivers between nodes.

MANET is comprised of mobile hosts that can communicate with each other using wireless links. It is also possible to have access to some hosts in a fixed infrastructure depending on the kind of mobile ad hoc network available.Different protocols are then evaluated based on measures such as the packet drop rate, the overhead introduced by the routing protocol, end-to-end packet delays, network throughput etc. Each device in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently. Each must forward traffic unrelated to its own use, and therefore be a router. The primary challenge in building a MANET is equipping each device to continuously maintain the information required to properly route traffic. Such networks may operate by themselves or may be connected to the larger Internet.

The statistical traffic analysis attack defines the network information from its statistical characteristics which are different from above mentioned passive attacks. In these attacks the adversary does not modify the traffic behaviour

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

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 6, June 2016

either by modifying or deleting the data packets. They just gather the packets, then do the statistical analysis. Predecessor attack, disclosure attack are some of the examples of statistical traffic analysis.

Anonymity is a property of network security. An entity in a system has anonymity if no other entity can identify the first entity, nor is there any link back to the first entity that can be used, nor any way to verify that any two anonymous acts are performed by the same entity. It includes,

1. Unlinkability of sender and receiver
2. Route discovery
3. Data delivery
4. Modifying control functions
5. Trust management

The main objective of this project is to achieve anonymous communication and discover the traffic patterns in MANET. The Enhanced work is based on GSTAR protocol using the statistical method it works passively and does the traffic analysis based on the statistical characteristics of the captured raw traffic. It is used to determine the source node, destination node, end-to-end communication relation and the hidden traffic pattern in a MANET communication system based on the probability values. It discovers the communication patterns without decrypting the captured packet.

II. LITERATURE SURVEY

In[4] Huang devised an evidence-based statistical traffic analysis model specially for MANETs. In this model, every captured packet is treated as evidence supporting a point to point (one-hop) transmission between the sender and the receiver. A sequence of point to point traffic matrices is created, and then they are used to derive end to end relations. This approach provides a practical attacking framework against MANETs but still leaves substantial information about the communication patterns undiscovered. First, the scheme fails to address several important constrains (e.g., maximum hop-count of a packet) when deriving the end-to-end traffic from the one hop evidences. Second, it does not provide a method to identify the actual source and destination nodes. Moreover, it only uses a naive accumulative traffic ratio to infer the end-to-end communication relations (e.g., the probability for node j to be the intended destination of node i is computed as the ratio of the traffic from i to j to all traffic coming out from node i), which incurs a lot of inaccuracy in the derived probability distributions. To measure the unlinkability, Huang proposed a solution include the following components: (i) the transmission model and channel model for IEEE 802.11b protocols, (ii) an unlinkability evaluation model using evidence theory, and (iii) a simulation study to validate the proposed models based on a fixed wireless communication system. Due to the unique characteristics of MANETs, very limited investigation has been conducted on traffic analysis in the context of MANETs.

In 2008 H.wong et al. proposed a timing-based approach in to trace down the potential destinations given a known source. In this approach, assuming the transmission delays are bounded at each relay node, they estimate the flow rates of communication paths using packet matching. Then based on the estimated flow rates, a set of nodes that partition the network into two parts, one part to which the source can communicate in sufficient rate and the other to which it cannot, are identified to estimate the potential destinations.

In 2013 Haiying et al. presented Anonymous Location-based and Efficient Routing protocol (ALERT) for traffic analysis in MANET. ALERT forms a non traceable anonymous route by dynamically splitting a network range into zones and arbitrarily decides nodes in zones as intermediate relay nodes. Particularly, in each step of routing, a data sender divides the network environment so as to split themselves and the destination into two zones. After that it randomly picks a node in the rest zone as the subsequent relay node and employs the GPSR algorithm to forward the data to the relay node. Finally, the data is transmitted to k nodes in the zone of destination by offering k-anonymity to the destination node. Additionally, ALERT has a scheme to conceal the data originator between a amount of initiators to reinforce the anonymity defence of the source node. Furthermore ALERT is resilient to timing attacks and intersection attacks.

In 2010 Yunzhong et al. presented Traffic Inference Algorithm known as TIA, which permits a universal adversary to correctly infer the MANET traffic pattern regardless of the need of present anonymous on-demand routing protocols. TIA initially explores the frames of overheard routing for recognition of flow and then maps each flow in rounds according to the inter arrival times of data-frame. Given consecutive frames of a flow exceed, and then the consequent vectors of frame inter arrival times on some link is extremely correlated with that of the subsequent link by the side of

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

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 6, June 2016

the flow path. This makes the adversary to repeatedly obtain the unknown flows and therefore the traffic pattern from overheard frames of MAC includes no prior ideas of the inter arrival time distribution of each flow in a network. Even though traffic analysis based on inters arrival time has been generally carried out on low latency mix networks and its likelihood in anonymous MANETs still unaffected. The TIA achieves good accuracy in traffic inference, while the mechanism is tightly tied to particular anonymous routing protocols but not a general approach. It identifies the end to end flows by tracing the routing frames, and then infer the actual traffic pattern using the data frames.

In 2003 J.M.Chang et al. proposed a detection scheme called the cooperative bait detection scheme (CBDS), which aims at detecting and preventing malicious nodes launching gray hole collaborative black hole attacks in MANETs. In this approach, the source node stochastically selects an adjacent node with which to cooperate, in the sense that the address of this node is used as bait destination address to bait malicious nodes to send a reply RREP message. Malicious nodes are thereby detected and prevented from participating in the routing operation, using a reverse tracing technique. In this setting, it is assumed that when a significant drop occurs in the packet delivery ratio, an alarm is sent by the destination node back to the source node to trigger the detection mechanism again. It takes the advantage of proactive detection in the initial step and the superiority of reactive response at the subsequent steps in order to reduce the resource wastage. As such, it can identify all the addresses of nodes in the selected routing path from a source to destination after the source has received the RREP message. However, the source node may not necessary be able to identify which of the intermediate nodes has the routing information to the destination or which has the reply RREP message or the malicious node â reply forged RREP. This scenario may result in having the source node sending its packets through the fake shortest path chosen by the malicious node, which may then lead to a black hole attack.

In 2002 Michael et al. presented onion routing prototype which can be employed to protect an Internet services against both traffic analysis attacks and eavesdropping from both the outside observers and network. They split the connection anonymity from the communication anonymity over that connection. For instance, when two parties operating onion routers which is able to recognize themselves to each other by without disclosing the existence of a connection between them. This work examines the adaptability of anonymous connections by extending their use in a various Internet applications. These applications comprise standard Internet services such as electronic mail, Web browsing and remote login. In addition Anonymous connections have also been used to hold virtual private networks (VPN) with connections that are opposing to traffic analysis which holds connectionless traffic. For supporting anonymous connections the configuration of onion routing network can be handled in different ways which includes customer-ISP configuration and firewall configuration, shifts privacy to the user's computer and may ease the carrier of responsibility for the user's connections.

In 2006 Yanchao et al. presented framework of a new anonymous on-demand routing protocol, known as MASK, which can concurrently attain anonymous MAC-layer and network-layer communications. The originality of MASK relies in the exploitation of dynamic pseudonyms quite rather than network addresses and static MAC. MASK suggests anonymity of sender and receiver plus relationship anonymity of sender-receiver. Particularly, even if adversaries might examine a transmission of packets in which they neither establish real network IDs of its sender and receiver, nor they choose when some two nodes are communicating in the network. Additionally, MASK guarantees node as intracablity that, even though adversaries might identify some real network IDs or its group memberships, they are not capable to make a decision whom and where the related nodes are in the network. Furthermore, MASK warranties end-to-end flow untraceability, sense that forwarded packets are not traced by adversaries to its ending destination or backward to its new source, In addition it cannot identify packets corresponding to a original communication flow.

In 2007 Chao-Chin et al. presented MANET Anonymous Peer-to-peer Communication Protocol (MAPCP), for peer to peer applications over mobile ad-hoc networks. This protocol is considered to be a flexible middleware connecting the MANET routing protocols and peer to peer applications. MAPCP utilizes a broadcast based method jointly with a probabilistic-based flooding control algorithm to launch anonymous paths among peers, which involves no hop-by-hop encryption or decryption, therefore entails lower power consumption and computational complexity. This protocol launches several anonymous paths among communication peers exist in a single phase of query, and is extremely resilient to node failure, mobility and malicious attacks. Moreover, MAPCP offers plans for communication peers to manage the trade off involving bandwidth efficiency and anonymity degree.

In 2006 Stefaan Seys and Bart Preneel proposed the ARM protocol. It requires no cryptographic operations in order for nodes to be able to recognize a message as being targeted at them or not. Nodes that only participate in the hiding process only need to decrypt and encrypt the short message header using their broadcast keys. Assume that every node

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

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 6, June 2016

in the network has a permanent identity that is known by the other nodes in the network that wish to communicate with this node. Assume that the source S and the targeted destination D share a secret key kSD and a secret pseudonym. The source will include this pseudonym in RREQ messages targeted at this specific destination. Once the source of a RREQ message receives a RREP message with the same identifier NymSD, it can start sending DATA messages to the destination. Similar to sending RREQ messages, DATA messages will have a onetime identifier attached to them. It allows a node on the route to recognize the fact that it is the next hop and that it should forward the message. Forwarding DATA messages is similar to forwarding RREP messages, using the same TTL scheme, but no padding is required. ARM protocol Anonymity is an important part of the overall security architecture for mobile ad hoc networks as it allows users to hide their activities. It enables private communications between users while making it harder for adversaries to focus their attacks.

In 2007 Jiejun Kong et al. proposed a new anonymous routing protocol ANODR (ANonymous On-Demand Routing) as the countermeasure. ANODR is a purely on-demand routing scheme that just sets up anonymous routes as needed in real time. This limits the chance of eavesdropping and traffic analysing to a time-critical on-demand window. In a mobile environment, the adversary is left with few options, it must launch the attack in the time-critical window or its information about the guarded mobile nodes is out-of-date. Another distinction of ANODR is that it is the first identity-free ad hoc routing scheme, which is contrary to all existing ad hoc routing schemes based on node identities. Instead of using node identities, ANODR relies on one-time cryptographic trapdoors in routing. Without node identities, the adversary has no means to break a mobile node's identity anonymity except via a node intrusion.

In 2012 Sunil et al. presented Energy Efficient, Secure and Stable Routing Protocol, ad hoc network holds the hosts communicating between themselves with moveable radios. Due to the limited radio propagation range of this network which can be organized by without considering any infrastructure support or wired base station where routes are primarily considered as multi-hop. The ad hoc network nodes are limited by battery power for their function. A sufficient number of intermediate nodes are used to route a packet from a source to a destination. An efficient resource is said to be Battery power of a node which need to be employed proficiently so as to keep away from early termination of a network or a node. One unique characteristic of Energy Efficient ad hoc routing protocol is its exploitation of Power for each entry of route. For a certain option to reach a destination by means of two routes, a demanding node is essential to choose one with improved power status.

In 2009 SunhoLim et al. proposed an Random Cast protocol to improve energy performance by controlling the level of overhearing and forwarding without a significant impact on network performance The Random Cast protocol enables a transmitter to choose no, unconditional, or randomized overhearing for its neighbours. It is specified in the ATIM frame and is available to its neighbouring nodes during the ATIM window. Random Cast, when a node sends an ATIM for a broadcast packet, all of its neighbours receive the packet in the following data transmission period but probabilistically rebroadcast it. The difference between the randomized overhearing of a unicast packet and the randomized rebroadcast of a broadcast packet. The performance of Random Cast is evaluated using ns-2 which simulates node mobility, a realistic physical layer, radio network interfaces, and the DCF protocol.

III. PROPOSED METHODOLOGY AND DISCUSSION

In [4] the Existing system D. Huang, proposed the Evidence-based statistical traffic analysis model, in which every captured packet is treated as evidence supporting a point-to-point (one-hop) transmission between the sender and the receiver. A sequence of point-to-point traffic matrices is created, and then they are used to derive end- to-end (multi hop) relations. It provides a practical attacking framework against MANETs but still leaves substantial information about the communication patterns undiscovered. MANET systems can achieve very restricted communication anonymity under the attack of STARS.

Statistical traffic analysis attacks have attracted broad interests due to their passive nature i.e., attackers only need to collect information and perform analysis quietly without changing the network behaviour (such as injecting or modifying packets). The predecessor attacks and disclosure attacks are two representatives. However, all these previous approaches do not work well to analyse MANET traffic because of the following three natures of MANETs,

1. The broadcasting nature
2. The ad hoc nature

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

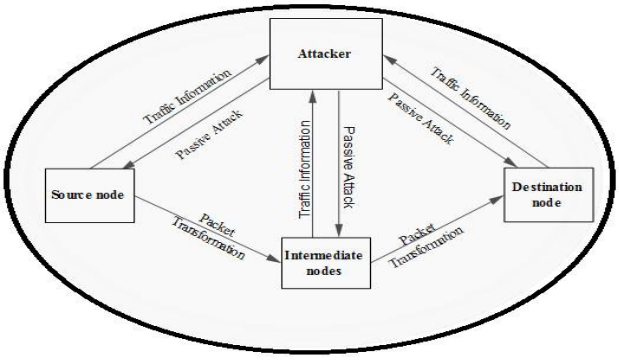
International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 6, June 2016

3. The mobile nature

In [1] the proposed system GSTAR protocol is used for MANETs. This approach is used to discover the hidden traffic pattern in MANETs. GSTAR is basically an attacking system, which only needs to capture the raw traffic from the PHY/MAC layer without looking into the contents of the intercepted packets. From the captured packets, table driven protocol constructs a sequence of point-to-point traffic matrices to derive the end-to-end traffic matrix, and then uses a heuristic data processing model to reveal the hidden traffic patterns from the end-to-end matrix. It is the statistical traffic analysis approach that takes the salient features of MANETs; the broadcast property, ad hoc property and mobile property.



(a)

The Fig.(a) Architecture of GSTAR. In the above figure the source and the destination nodes are identified in which how the packets are transferred has been shown and the possible attacks are listed on it.

It 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 [1].

To achieve its goals, the proposed system includes two major steps for calculating the probability values,

1. 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.
2. Apply a heuristic approach to identify the actual source and destination nodes, and then correlate the source nodes with their corresponding destinations.

The attacker can take advantage of GSTARS by using statistical method to perform traffic analysis as follows:

1. Treat each region as a super node and use Enhanced GSTAR to figure out the sources, destinations, and end-to-end communication relations.
2. Analyse the traffic even when nodes are close to each other by treating the close nodes as a super node.
3. Using this method the passive observer observes the actual source and destination nodes, and then correlates the source to their corresponding destination using heuristic approach.
4. It determines the source, destination and their relations effectively.
5. It infers the traffic pattern with an accuracy as high as 95%.
6. To monitor the cross component traffic.

IV. EXPERIMENTAL RESULTS

Different strategies can be used to speculate the actual traffic patterns from the probability distributions. The performance of GSTARS based on the following two basic strategies, T1 and T2.T1 is the number of actual sources, destinations, or end-to-end links is known to be k. simply select the top k items (nodes or links) with the highest probabilities[1].

T2 is the number k is unknown keep selecting the top items with the highest probabilities until both of the two criteria are satisfied:

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

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 6, June 2016

1. The sum of the probabilities of the selected items has reached u; and
2. The probability of the last selected item is v times larger than the current one.

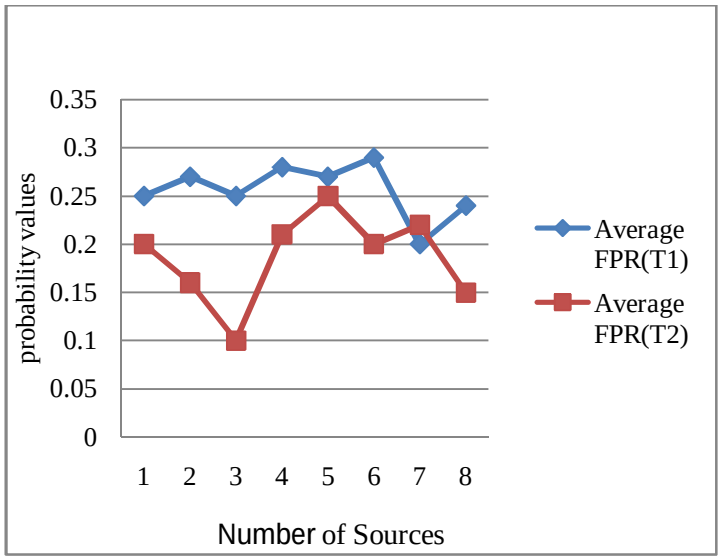
u and v are two adjustable thresholds, which are set to 0.8 and 4 in this approach. The simulated MANET is comprised of 42 mobile nodes deployed in a 1,000 x1,000 m2 area. The number of sources varies from 2 to 6 and each source node has a single destination. Both the sources and destinations are randomly selected. In each round, in STAR routing protocol use T1 and T2 to identify the sources and end-to-end links, and compare them with the actual traffic patterns to calculate the false-positive rate and false-negative rate based on the typical confusion matrix.

Identify k0 sources (end-to-end links) in which only c of them are actual sources (end-to-end links), the false-positive rate is defined as follows,

$$fpr = fp/fp + tn = k' - c/N - k'$$

and the false-negative rate is defined as follows:

$$fnr = fn/fn + tp = k - c/k$$



(a)

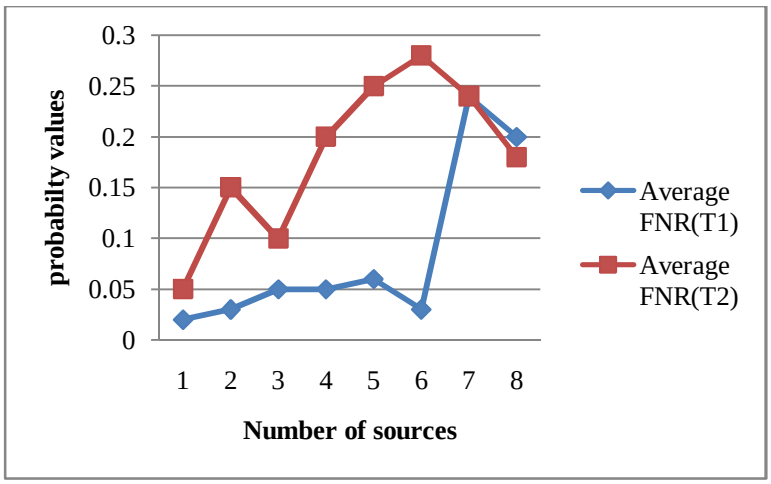
The Fig (a). False Positive Ratio for source identification. The above figure depicts the average values (over the 10 rounds for each case) of the false-positive rate shown in Fig.a evaluated that both T1 and T2 achieve reasonably good accuracy for source identification [1].

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

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 6, June 2016



(b)

The Fig (b). False Negative Ratio for source identification. The above figure depicts the average values (over the 10 rounds for each case) of the false-positive rate shown in Fig.b evaluated that both T1 and T2 achieve reasonably good accuracy for source identification [1]. From Fig.b evaluated that both T1 and T2 achieve reasonably good accuracy for source identification.

Using T1, the false-positive rate is almost always less than 0.5, although it increases slightly as the number of sources goes up and the peak of the false-negative rate is lower than 0.3. T2 tends to select more nodes as source nodes, which inevitably increases the false-positive rate. However, the false-negative rate is decreased at the same time. A valuable observation is that, T2 is not necessarily better than T1 by knowing the number of items to be selected.
The above graph shows the average false Negative rate of source identification. From Fig.3 evaluated that both T1 and T2 achieve reasonably good accuracy for source identification. Using T1, the false-negative rate is almost always less than 0.3, although it increases slightly as the number of sources goes up and the peak of the false-negative rate is lower than 0.3. T2 tends to select more nodes as source nodes, which inevitably increases the false-negative rate. However, the false-negative rate is decreased at the same time. A valuable observation is that, T2 is not necessarily better than T1 by knowing the number of items to be selected.

V. CONCLUSION

The proposed system GSTAR using statistical method is the first method to calculate statistical values of the source and destination nodes. Compared to the existing system such as evidence theory, TIA algorithm it gives less average End to End Delay and average Jitter. It gives better results in throughput, PDR with exponential traffic pattern. It will scale well in large network since it has significantly reduced bandwidth consumption for the routing updates while at the same time reducing latency by using predetermined routes. The proposed method works well on on-demand anonymous MANET routing protocols. Detailed simulations show that it can infer the traffic pattern with an accuracy as high as 25%**.** Empirical studies demonstrate that GSTAR achieves good accuracy in disclosing the hidden traffic patterns. The neighbourhood noise reduction is reduced and the probability values of the source and destination are calculated, as 0.4 for both the source and destination node.

REFERENCES

[1] Yang Qin, Dijiang Huang, and Bing Li, " STARS: A Statistical Traffic Pattern Discovery System for MANETs". IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL. 11, NO. 2, MARCH/APRIL 2014.

[2] Zhang, Y., Liu, W., Lou, W., and Fang, Y., "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)

Vol. 5, Issue 6, June 2016

[3] Qin, Y., and Huang, D., "OLAR: On-Demand Light weight Anonymous Routing in MANETs", Proc. Fourth Int'l Conf. Mobile Computing and Ubiquitous Networking (ICMU '08), pp. 72-79, 2008.
[4] Blaze, M., Ioannidis, J., Keromytis, A., Malkin, T., and Rubin, A., "WAR: Wireless Anonymous Routing", Proc. Int'l Conf. Security Protocols, pp. 218-232, 2005.
[5] Boukerche, A. El-Khatib, K., Xu, L., and Korba, L., "SDAR: A Secure Distributed Anonymous Routing Protocol for Wireless and Mobile Ad Hoc Networks", Proc. IEEE 29th Ann. Int'l Conf. Local Computer Networks (LCN '04), pp. 618-624, 2004.
[6] Seys, S., and Preneel, B., "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.
[7] Shokri, R., Yabandeh, M., and Yazdani, N., "Anonymous Routing in MANET Using Random Identifiers", Proc. Sixth Int'l Conf .Networking (ICN '07), p.2, 2007.
[8] Song, R., Korba, L., and Yee, G., "Anon DSR: Efficient Anonymous Dynamic Source Routing for Mobile Ad-Hoc Networks", Proc.Third ACM Workshop Security of Ad Hoc and Sensor Networks (SASN '05), pp. 33-42, 2005.
[9] Reed, M., Syverson, P., and Goldschlag, D., "Anonymous Connections and Onion Routing", IEEE J. Selected Areas in Comm., vol. 16,no. 4, pp. 482-494, May 2002.
[10] Chaum, D., "Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms", Comm. ACM, vol. 24, no. 2, pp. 84-88, 1981.
[11] Raymond, J., "Traffic Analysis: Protocols, Attacks, Design Issues, and Open Problems," Proc. Int'l Workshop Designing Privacy Enhancing Technologies: Design Issues in Anonymity and Unobserva-bility, pp. 10-29, 2001.
[12] Dai,W."Two Attacks against a Pipe Net-Like Protocol Once Used by the Freedom Service," http://weidai.com/freedom-attacks.txt, 2013.
[13] Wang, X., Chen, S., and Jajodia, S., "Network Flow Watermarking Attack on Low-Latency Anonymous Communication Systems", Proc. IEEE Symp. Security and Privacy, pp. 116-130, 2007.
[14] Reiter, M., and Rubin, A., "Crowds: Anonymity for Web Transactions", ACM Trans. Information and System Security, vol. 1, no. 1,pp. 66-92, 1998.
[15] Wright, M., Adler, M., Levine, B., and Shields, C., "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.
[16] Figueiredo, D., Nain, P., and Towsley, D., "On the Analysis of the Predecessor Attack on Anonymity Systems," technical report, Computer Science, pp. 04-65, 2004.
[17] Danezis, G., "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.
[18] Danezis, G., and Serjantov, A., "Statistical Disclosure or Intersection Attacks on Anonymity Systems," Proc. Sixth Information Hiding Workshop (IH '04), pp. 293-308, 2004.
[19] G. Danezis, C. Diaz, and C. Troncoso, "Two-Sided Statistical Disclosure Attack," Proc. Seventh Int'l Conf. Privacy Enhancing Technologies, pp. 30-44, 2007.
[20] Troncoso, C., Gierlichs, B., Preneel, B., and Verbauwhede, I., "Perfect Matching Disclosure Attacks," Proc. Eighth Int'l Symp. Privacy Enhancing Technologies, pp. 2-23, 2008.
[21] Huang, D., "Unlinkability Measure for IEEE 802.11 Based MANETs" , IEEE Trans. Wireless Comm., vol. 7, no. 3, pp. 1025-1034, Mar. 2008.
[22] Chaum, D.,"The Dining Cryptographers Problem: UnconditionalSender and Recipient Untraceability", J. Cryptology, vol. 1, no. 1,pp. 65-75, 1988.
[23] He, T., Wong, H., and Lee, K., "Traffic Analysis in Anonymous MANETs", Proc. Military Comm. Conf. (MILCOM '08), pp. 1-7, 2008.
[24] Liu, Y., Zhang, R., Shi, J., and Zhang, Y., "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.
[25] Wexler, J.,"All About Wi-Fi Location Tracking", Network World,http://features.techworld.com/mobile-wireless/2374/all-about-wi-fi-location-tracking/, 2004.
[26] Scalable Network Technologies, "QualNet Simulator", http://www.qualnetcomm.com/, 2008.