International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

# AET: Implementing Anonymity Enhancing Techniques for MANETs Using Statistical Traffic Analysis

**Mrs. Maheswari V[1], Mr. Prasanth S[2]**

[1,2]Assistant Professor, Department of Computer Sience and Engineering Unnamalai Institute of Technology, Kovil Patti, Tamil Nadu, India.

**Abstract:**
Anonymous communication is the main issue in case of MANETs. It is difficult to find the source and destination of the communication link and the other nodes involved in it. Many anonymity enhancing techniques have been proposed based on packet encryption to protect the communication anonymity of mobile ad hoc networks (MANETs). However, MANETs are vulnerable under certain circumstances like passive attacks and traffic analysis attacks. Here we describe the traffic analysis problem, expose some of the methods and attacks that could infer MANETs are still weak under the passive attacks. To show how to discover the communication patterns without decrypting the captured packets, we present the paper AET using statistical traffic analysis. In order to discover the packet patterns MTPD works passively and does the traffic analysis based on the statistical characteristics of the captured raw traffic. Here we can determine the source node, destination node and the end-to-end communication path in case of mobile ad hoc networks.

**Keywords:** Anonymous Communication, Mobile ad hoc network, Passive attack, Statistical traffic analysis.

## 1. INTRODUCTION

MANET places that can configure itself for a change and is a type of temporary network. MANET's nodes are mobile because they use wireless connections to connect different networks. Such as a cellular or satellite to a standard Wi-Fi connection. For example, a VANET (Vehicular Ad Hoc Networks) , that allows vehicles to communicate with roadside equipment is a type of MANET. Each device in a MANET is free to move freely in any direction, and therefore change its links to other devices frequently. Each forward traffic unrelated to its own use, and should therefore be a router. MANET continued right through the building of a primary challenge is to transport the necessary tools for each device to maintain the information. Such networks or the Internet connection will work themselves. This includes vehicle and tricks Networks (VANETs) are used to communicate between vehicles in the roadside S. equipment. Internet -based mobile ad hoc networks (i-MANET), that connect the nodes and edges are fixed internet portals. It cannot apply directly to ordinary individuals, such as networks, routing algorithms. many researchers in an effort to increase security protocols for MANETs and some new regulations to implement the advice and counsel of the new improvements. The attacks on MANETs routing nodes can join and easy to go on a fixed route requests to the dynamics of the mobile

infrastructure, which can be challenging. Following are the attacks which are occur in layers of the OSI Model. Application layer: Malicious code, Transport Layer: Session traffic hijacking, flooding the network. Network layer : Sybil, floods , Black Hole , Worm Hole , link spoofing , unauthorized connection was made , Data link / MAC layer: malicious behavior , self-interested behavior , active attack , passive attack, internal and external attack ,Physical layer : interference , traffic collision . Proactive and Reactive are basically two approaches to protecting approach by the various encryption techniques, trying to prevent an attack from launching attacks in the first place. In contrast, reactive approach to detect security threats and react accordingly like posterior. MANET is a complete security solution to integrate approaches to include three elements: prevention, detection, and reaction. For example, when a packet functions can be used to protect by means of reactive approach, proactive approach can be used to ensure proper routing states. As argued in, security is a chain based, and it is only as protect as the simple weakest link. Missing an each single component may significantly degrade the overall security solutions. The protocol can be classified into two types. The proactive protocols are extensions of the wired network routing protocols.

approach by the various encryption techniques, trying to prevent an attack from launching attacks in the first place. In contrast, reactive approach to detect security threats and react accordingly like posterior. MANET is a complete security solution to integrate approaches to include three elements: prevention, detection, and reaction. For example, when a packet functions can be used to protect by means of reactive approach, proactive approach can be used to ensure proper routing states. As argued in, security is a chain based, and it is only as protect as the simple weakest link. Missing an each single component may significantly degrade the overall security solutions. The protocol can be classified into two types. The proactive protocols are extensions of the wired network routing protocols.

They are maintaining the global such as common topology information in the form of tables at every node. This type of protocols maintains fresh lists of destinations and their routes by periodically distributing routing tables throughout the network. These tables are updated frequently in order to maintain consistent and accurate network state information. Routing information is generally flooded in the whole network, whenever a node requires a path to the destination node, it runs like an appropriate correct path finding algorithm on the topology information it already maintains. The Destination sequence Distance-vector routing protocol(DSDV), Source tree adaptive routing protocol(STAR), Wireless routing protocol(WRP) and Cluster head gateway routing protocol(CSGR) are some examples for the proactive routing protocol[3]. Unlike the Table driven routing protocols, Reactive routing protocols execute the path finding process and exchange routing information only when a path is required by a node to communicate with a destination. The protocol fall under this category do not maintain the network information. They obtain the required path when it is necessary, by using a connection establishment process. The Dynamic source routing protocol (DSR), Temporally Ordered Routing algorithm (TORA), Adhoc On-Demand Distance vector routing protocol etc. A good routing protocol for this network environment has to dynamically adapt to the changing network topology. This Hybrid type of protocol combines the advantages of proactive and reactive routing protocol functions. The routing is initially started with some proactively prospected routes and then serves the demand from additionally activated nodes through reactive flooding. Nodes within a certain distance from the node concerned .or within a particular geographical region are said to be within this zone, a table driven protocol is used. For nodes which are located beyond that zone, an on-demand approach is used. The Zone Routing protocol (ZRP), Zone based Hierarchical Link State routing protocol (ZHLS). The main

disadvantages of such algorithms are: Advantage depends on number of other nodes activated; Reaction to traffic demand depends on gradient of traffic volume [2]. The DSR protocol is composed of two mechanisms that work together to allow the discovery and maintenance of source routes in the ad hoc network [5]. **Route Discovery** is the mechanism by which a node Swishing to send a packet to a destination node D Obtains a source path to D. Route Discovery mechanism is used only when S attempts to send a packet to D and does not already know a path to D. **Route Maintenance** is the mechanism by which node S is able to find, while using a source path to D, if the network topology has changed such that it can no longer use its path to D because a link along the path no longer works. When path Maintenance indicates a source route is broken, Source can attempt to use any other route it happens to know to Destination, or it can invoke Route finding mechanism again to search a new path. Route Maintenance is used only when Source is actually sending packets to Destination. DSR does not use any periodic routing advertisement, like link status sensing, or neighbor node detection and does not relies on these functions from any underlying protocols in the network.

### A. Objective:

The objective of the paper described in the abstract is to address the issue of anonymous communication in Mobile Ad hoc Networks (MANETs) and the vulnerabilities they face, particularly under passive attacks and traffic analysis attacks. The paper aims to propose solutions to enhance the anonymity of communication in MANETs by introducing techniques such as AET (Anonymous End-to-End Traffic) and MTPD (Mobile Traffic Pattern Discovery).

Specifically, the objectives of the paper can be summarized as follows:

1. To highlight the challenges of anonymous communication in MANETs.
2. To discuss the vulnerabilities of MANETs under passive attacks and traffic analysis attacks.
3. To propose the AET technique for discovering communication patterns without decrypting captured packets.
4. To introduce the MTPD method for analyzing the statistical characteristics of captured raw traffic to determine source nodes, destination nodes, and end-to-end communication paths in MANETs.

Overall, the paper aims to contribute to the field of secure communication in MANETs by addressing the anonymity and security concerns associated with mobile ad hoc networks.

### B. Contribution:

The contribution of the paper described in the abstract lies in its proposed techniques and methods to enhance the anonymity and security of communication in Mobile Ad hoc Networks (MANETs). Here are the key contributions of the paper:

1. **Introduction of AET (Anonymous End-to-End Traffic):** The paper introduces the AET technique, which allows for the discovery of communication patterns in MANETs without the need to decrypt captured packets. This technique aims to enhance the anonymity of communication in MANETs by providing a method to analyze traffic patterns.
2. **Presentation of MTPD (Mobile Traffic Pattern Discovery):** The paper presents the MTPD method, which works passively to analyze the statistical characteristics of captured raw traffic in MANETs. This method helps in determining the source node, destination node, and the end-to-end communication path in mobile ad hoc networks.
3. **Addressing Passive Attacks and Traffic Analysis Attacks:** By discussing the vulnerabilities of

MANETs under passive attacks and traffic analysis attacks, the paper sheds light on the potential weaknesses in current anonymity-enhancing techniques and proposes solutions to mitigate these vulnerabilities.

4. **Enhancing Communication Security in MANETs:** Overall, the paper contributes to the field of secure communication in MANETs by providing insights into traffic analysis issues, introducing novel techniques for anonymity preservation, and offering a method for discovering communication patterns in a secure manner without compromising privacy.

These contributions aim to advance the understanding and development of secure communication protocols in MANETs, addressing the challenges associated with anonymity and security in mobile ad hoc networks.

## 2. RELATED WORKS

### A. Acknowledgement Scheme

An end-to- end acknowledgment scheme based on nominal Acknowledgement. It aims to reduce the network load on the network and when misconduct is detected [1]. Nodes S and T between the way all intermediate nodes cooperative and node successfully transmits the packet Pad1, node D is receiving that packet. Now , the tip of the destination node D is a building to demolish the data packet Pad1 sends out the same way but in a reverse order of a building Pak1 to send an acknowledgment packet back down. If that Pak1 (Acknowledgement) is not received by the sender means it establishes the Secure Acknowledgement mode.

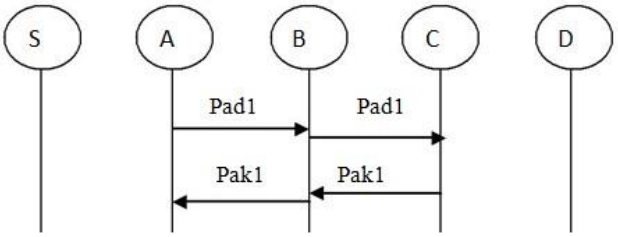



Fig 1: Acknowledgement Scheme

### B. *Secure Acknowledgement Scheme*

S- Acknowledgement scheme is an improved version of the Acknowledgement program [1]. Each of the three nodes continues to work as a team to identify faulty nodes. In each of these three fronts, the third node to the first node to send an acknowledgment packet. S- Acknowledgement receiver with the intention of introducing the conflict or faulty nodes to detect even with the presence of limited transmission power.

### C. *Misbehavior Report Authentication*

The plan is to escape the presence of misconduct could not be found on the wrong end of the weakness of the monitoring is designed to solve. Report misconduct can be created by a malicious attack by malicious nodes were innocent. For a network whose nodes are sufficient to cause the attackers to break down the entire network when the attack can be lethal. The main goal of the project is to escape through a different path to the node that contains the information of the missing packet, acknowledge it. He escapes from the start, from the source node and the destination node searches its local knowledge base and search for alternatives [6][7] .The source node is to find another route with a request of the DSR routing . Due to the nature of MANETs, it is common to find many ways between the two nodes. By

adopting alternative target node, we pass the point of reporting misconduct. When the node receives a packet depends on its local knowledge base searches and compares the data packet is received. Otherwise, reliable and accepted the report of misconduct. Since the adoption of the escape plan, EAACK misconduct, despite the existence of the report is the ability to detect malicious nodes. As discussed before, EAACK is an acknowledgment - based IDS. EAACK in three areas, ie, Acknowledgement S-ACK Acknowledgement, Misbehavior Report Authentication, Will be executed based detection schemes. All of them depend on an acknowledgment packet network to detect misbehaviors . Therefore, it is important to make sure that is true all acknowledgment packets.

## 3. PROPOSED SCHEME

In order to provide more security to mobile adhoc network than existing system, we are proposing a new technique known as hashing technique i.e. node verification technique for intrusion detection system and calculating energy level for each node.

### A. Hash Technique

The hashing technique is an generation of hash id to mobile nodes H(n) = public key/identity. If any node in the network wants to verify neighbour node or any other node , the particular node X request a neighbour node Y to generate a hash id using hash function. The Y node generates hash id using a public key of X and identity of Y. in the same X node also generates a hash id using public key of Y and identity of X. if both the hash id are equal then the nodes are authenticated and not a malicious node. If Y node hash id is not equal to X node hash id then the corresponding Y node is malicious node. Then the detected malicious node is eliminated from the network. In this way our proposed technique detects and eliminate malicious node. Any node can verify any other at any time, by this intrusion detection system all nodes in the network can be verified and we can form a securable network. Hashing techniques are available based on the concept of a hash function that it transforms a given input value of arbitrary length to a value of a stable length, called the hash value. The transformation is done in a manner; it is computationally infeasible to transform the hashing value to the true value. . Hash functions are most efficient as they don’t involve heavy calculations. Hence they are applied in the area of security for information authentication and value of integrity checks

### B. Data collection:

Data collection module is included for every anomaly detection system to collect the information of nodes and values of features for the corresponding layer in a system. Normal profile is created during the normal collection scenario. Attack related data is collected during the attack scenario.

### C. Data collection:

The audit data is collected and record in a file format, so that it can be used for any type of anomaly detection. Data preprocess collection is a technique to process the information with some test train data. In the entire layer misuse detection systems, the previous mentioned preprocessing technique was used.

## 4. METHODOLOGY

Based on the abstract provided, the methodology for the paper on enhancing communication anonymity in Mobile Ad hoc Networks (MANETs) using the AET and MTPD techniques may involve the following steps:

1. **Problem Identification:** Identify the challenges and vulnerabilities associated with anonymous communication in MANETs, particularly under passive attacks and traffic analysis attacks.

2. **Literature Review:** Review existing anonymity-enhancing techniques in MANETs and analyze their effectiveness in addressing the identified issues.
3. **Development of AET Technique:**
   Design the AET technique for discovering communication patterns without decrypting captured packets.
   Define the methodology for implementing AET and how it enhances communication anonymity in MANETs.
4. **Development of MTPD Method:**
   Design the MTPD method for analyzing statistical characteristics of captured raw traffic to determine source nodes, destination nodes, and end-to-end communication paths.
   Define the methodology for implementing MTPD and its role in enhancing communication security in MANETs.
5. **Simulation and Evaluation:**
   Set up simulation environments to test the AET and MTPD techniques.
   Evaluate the performance of the techniques in terms of anonymity preservation, communication pattern discovery, and resistance against passive attacks and traffic analysis attacks.
6. **Data Collection and Analysis:**
   Collect data from simulated MANET scenarios with varying network sizes and traffic patterns.
   Analyze the data to assess the effectiveness of AET and MTPD in discovering communication patterns and enhancing anonymity in MANETs.
7. **Comparison with Existing Techniques:**
   Compare the performance of AET and MTPD with existing anonymity-enhancing techniques in MANETs.
   Highlight the advantages and limitations of the proposed techniques in addressing the identified vulnerabilities.
8. **Discussion and Conclusion:**
   Discuss the findings from the simulation and analysis.
   Draw conclusions on the effectiveness of the AET and MTPD techniques in enhancing communication anonymity and security in MANETs.

By following these steps in the methodology, the paper can provide a structured approach to developing and evaluating the proposed techniques for enhancing communication anonymity in MANETs.

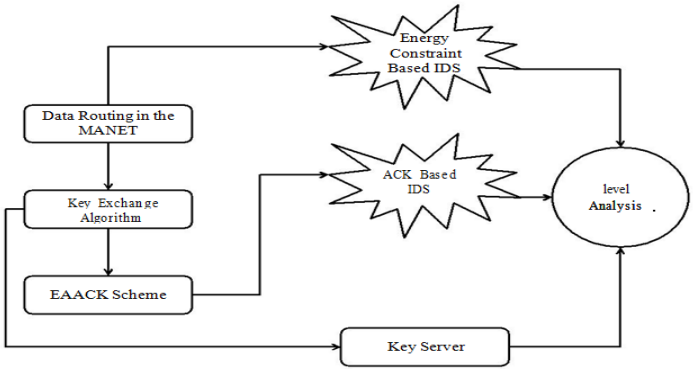



Fig 2: System Overview

**Fig: Evaluation of Result**

Using the determined IP address of the source and destination nodes we can discover the physical location of the mobile devices. It could be upgraded for military uses for the defense purpose by traffic monitoring. Use of the sensors in the routers, will improve the attack as we can find the exact location of the source and the destination devices.

**B. Energy Level**

In this system the intrusion detection system detects the malicious node by calculating energy level for each node. This can be done through trust level analysis algorithm. In this technique we are going to calculate the energy level for each node , generally the malicious nodes have three times more energy value compared to normal nodes. By analyzing the energy level of all nodes we can easily detect and eliminate the malicious nodes from network. For example maximum nodes will have energy level as 23 joules.

**A. Modules Description**

**1. Home agent:**

The present in each network and it gathers information about its system from application layer to routing layer in OSI model.

**2. Neighboring node:**

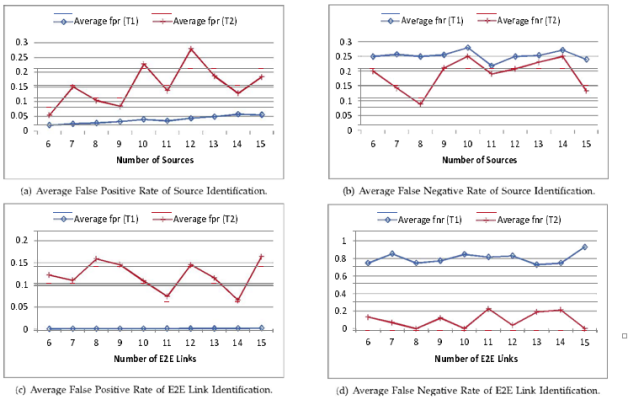
Any system in the network transfer any type of information to other network system, it will broadcast through some intermediate nodes. Before it transfer the information, it can send mobile node to the neighboring agent and it collect all the information atlast it return back to the network and it calls classifier rule to check out the hackers. If any suspicious activity was found, then it will not forward the message to neighboring node.

**RESULT ANALYSIS**

The simulation results were conducted with the help of the Network Simulator. The network is running on a laptop with intel3 core, Processor CPU and memory 3-GB RAM. The intention is to provide simulation results and make it easier to compare the results. In NS 2, the nominal configuration has 40 nodes in a flat space. The physical layer and the MAC layer are included in NS2 for providing a platform and make communication with neighbor nodes. The moving speed of mobile node is up to 30 m/s and a pause time of 1000 seconds. User Datagram Protocol with constant bit rate is implemented with a 512 B packet size of.

With the restricted capabilities, the attacker can take advantage of STARS to perform traffic analysis as follows:

1. divide the entire network into multiple regions geographically;
2. deploy sensors along the boundaries of each region to monitor the cross-component traffic;
3. treat each region as a super node and use STARS to figure out the sources, destinations, and end-to-end communication relations; and
4. analyze the traffic even when nodes are close to each other by treating the close nodes as a super node.




(a) Average False Positive Rate of Source Identification.
(b) Average False Negative Rate of Source Identification.
(c) Average False Positive Rate of E2E Link Identification.
(d) Average False Negative Rate of E2E Link Identification.

## CONCLUSION AND FUTURE ENHANCEMENT

In this paper, we propose an idea of attacking mobile ad hoc networks. MTPD is basically an attacking system for MANETs which works passively for identifying the traffic patterns. It captures the packets from the MAC layer or the physical layer of the network and need not look into the contents of the captured traffic. Here we use the heuristic approach for analyzing the captured packets and to discover the hidden traffic patterns.

Using the determined IP address of the source and destination nodes we can discover the physical location of the mobile devices. It could be upgraded for military uses for the defense purpose by traffic monitoring. Use of the sensors in the routers, will improve the attack as we can find the exact location of the source and the destination devices.

## References

1. 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.
2. 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.
3. 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.
4. M. Blaze, J. Ioannidis, A. Keromytis, T. Malkin, and A. Rubin, “WAR: Wireless Anonymous Routing,” Proc. Int’l Conf. Security Protocols, pp. 218-232, 2005.
5. R. Song, L. Korba, and G. Yee, “AnonDSR: 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.
6. M. Reed, P. Syverson, and D. Goldschlag, “Anonymous Connec-tions and Onion Routing,” IEEE J. Selected Areas in Comm., vol. 16, no. 4, pp. 482-494, May 2002.
7. D. Chaum, “Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms,” Comm. ACM, vol. 24, no. 2, pp. 84-88, 1981.
8. Yang Qin, Dijiang Huang, *Senior Member, IEEE,* and Bing Li“STARS: A Statistical Traffic Pattern DiscoverySystem for MANETs”, 2013.
9. Boukerche, K. El-Khatib, L. Xu, and L. Korba, “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.
10. 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.