Mitigating the Problem of Packet Dropping & Energy Management in AD-HOC Wireless Network

Mr. Umesh Samarth
ME in Wireless Communication and Computing
JDCOEM, Nagpur
RTMNU, Nagpur, India
kamble.rucha3@gmail.com

Prof. S. V. Sonekar
ME in Wireless Communication and Computing
JDCOEM, Nagpur
RTMNU, Nagpur, India
srikantsonekar@rediffmail.com

Abstract—A mobile ad-hoc network (MANET) is a self-arranged network that consists of mobile routers connected by wireless channels. Anonymity communication is a great challenge in MANET. Though there are many anonymity enhancing techniques that have been introduced. These techniques are based on packet encryption to secure the communication anonymity. Still MANET is vulnerable to passive statistical traffic analysis attacks. There are two features of communication anonymity: end-to-end anonymity and source or destination anonymity.

This proposed system is designed to discover the communication pattern without decoding the captured packets. First phase of the proposed system is to search the required node. The search is performed by using a heuristic approach. Second phase is to perform statistical traffic analysis. The purpose of this phase is to discover the data transmission of the searched node to its adjoining nodes. After implementing the statistical traffic analysis whether the searched node plays the role of source or destination is estimated. With the help of this estimation the traffic pattern is discovered.

The utility of this proposed system is basically in military environment. In order to track the adversaries attack this system is utilized. The adversaries are not able to know that they have been tracked. This proposed system works passively and perform traffic analysis based on statistical characteristic of captured raw packets.

*****

I. INTRODUCTION

Mobile Ad-hoc Network (MANET) is one of random network whose nodes are self-constructed, self-established, infrastructure less and connected by wireless links. The basic structure of MANET is illustrated in Fig. 1. In mobile ad-hoc network (MANET) nodes are mobile in nature. This makes the topology dynamic. The wireless medium used has limited resource and also lack of centralized administration. Due to above characteristics, anonymous communication becomes a challenge in MANET. There are two aspects of communication anonymity: End-to-End Anonymity and Source or Destination Anonymity. Source or Destination Anonymity: There is difficulty in identification of source and destination nodes in the network. End-to-End Anonymity: There is difficulty in identification of end-to-end communication relation. Many anonymous routing protocols such as Anonymous On-Demand Routing (ANODR) and On-demand Lightweight Anonymous Routing (OLAR) have been proposed for anonymity of nodes in network. Still adversary can intercept the information through passive attack.

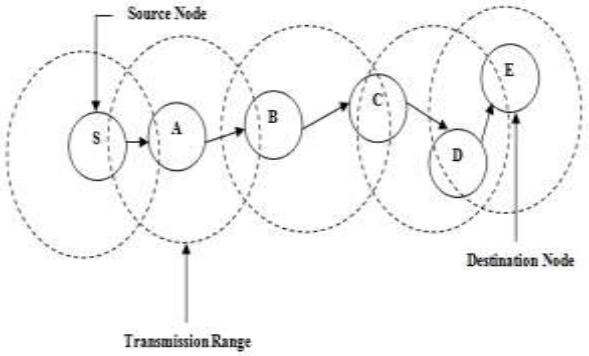

Fig.1 Basic structure of Mobile Ad-hoc Network

MANET can be attacked in two ways: Active and Passive. An active attack seeks to change system resource or affect their operation. While a passive attack try to gain or arrange data from the system but does not disturb system resources. Passive attack is more harmful than active attack as the user is unaware of collecting information performed by an adversary without disturbing the operation. However, MANET is vulnerable to traffic analysis that is one of the types of passive attack. Traffic Analysis is the process of monitoring and analyzing the activities of traffic patterns during delivery of packets in MANET. Traffic analysis can be useful to carry out an investigation on their adversary in a military operation. The nodes that are within the transmission range can communicate directly, while communication between more

than two nodes can take place through intermediate nodes. As centralized administration is absent in MANET, each node maintain their own routing and resource management in distributed manner. This makes MANET vulnerable to traffic analysis.

Problem Definition

The predecessor attack and disclosure attack are types of traffic analysis. In traffic analysis information is neither leaked nor modified it is analyzed and monitored. The enemy could determine the identity and location of communication hosts and could observe length and frequency of messages being exchanged. This report might be useful in assuming the nature of the communication. However, predecessor and disclosure attacks cannot analyze MANET traffic due to the following reasons:

1) Broadcasting nature: In wired networks, mostly point-to-point message transmission takes place. In such cases there is only one possible receiver. While in wireless network the messages are broadcasted. So they can have multiple possible receivers. This results in uncertainty to trace a particular path.

2) Ad hoc nature: One of the characteristic of MANET is infrastructure less. Due to this nature the mobile node can deliver as both a router and a host. Thus it is difficult to determine the role of mobile node to be a source, destination, or just a relay.

3) Mobile nature: The existing traffic analysis models do not consider the mobility of communication peers. This makes communication relations among mobile nodes more complex.

1.5 Objectives

In order to accomplish the aim of reducing anonymous communication and to disclose the hidden traffic pattern in mobile ad hoc network (MANET) the objectives of Traffic Pattern Discovery System (TPDS) are mentioned below:

1) To discover the traffic pattern in MANET.

The traffic pattern in MANET can be discovered by first searching the required node using a heuristic approach. Statistical traffic analysis is carried out to analyze the transmission of data. Probability distribution deduces the possibility of nodes being source and destination.

2) To identify point to point transmission among receivers.

Point-to-Point transmission can be analyzed by calculating the number of data received by the receivers. Traffic matrix is calculated to find out transmission among receivers.

II. PROPOSED SYSTEM

The flow of the proposed system is illustrated in Fig. 4. The first step of the system is to form a network. This network consists of nodes that are scanned to find a traffic free path. In order to search the node a heuristic searching algorithm is applied. Statistical traffic analysis is performed on the required node. Probability distribution is applied to discover the traffic pattern. This system works on one condition that if the required node is not found then the system stops and no further process is carried out.

Constraints

Traffic Pattern Discovery System (TPDS) consists of some of the constraints that are discussed below:

- Best-First Search is used to traverse the traffic pattern can detect the path until nodes can be scanned. If no nodes are free then path is not found. Hence, the algorithm stops working.
- The searching of path is restricted to specified range only. The searching cannot be performed away from that specified range.

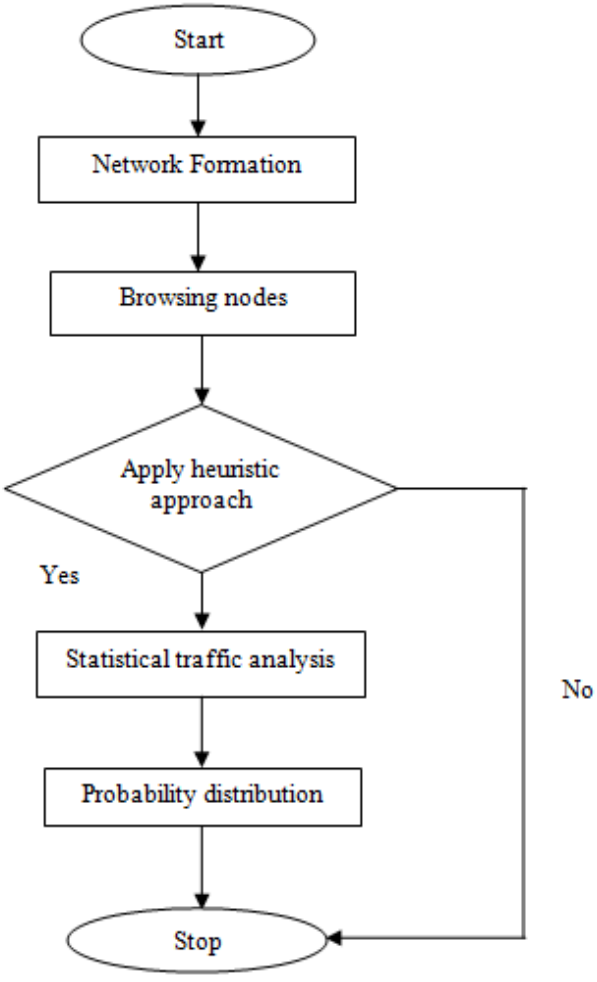

Fig. 2 System flow diagram

III. DESIGN AND IMPLEMENTATION

Outcomes

The research has been carried out with three different total numbers of nodes. They are 25, 45 and 65. However, here only outcomes of total numbers of nodes that are 45 nodes have been included. The following outcomes are obtained during each phase:

Topology Formation and Setup Phase

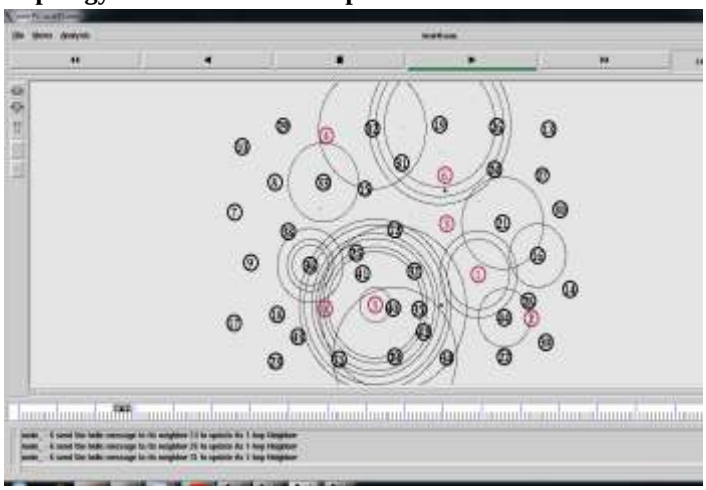

Fig.3 Topology formation for 1-hop neighbors

The topology formations among nodes for the nodes which are 1-hop distance away are displayed in Fig. 3. In this phase, hello packets are sending to all its neighbor nodes those are 1-hop distance away from sender node. The black coloured node indicates that the node is in state to start topology formation for 1-hop nodes. The omni-directional antennas are sending signals to neighbor nodes. One of the nodes becomes sender node and starts sending hello packets to nodes that are 1-hop distance away. The neighbor nodes become receiver and starts receiving hello packets. The pink coloured node indicates that the node has completed topology formation for 1-hop neighbor

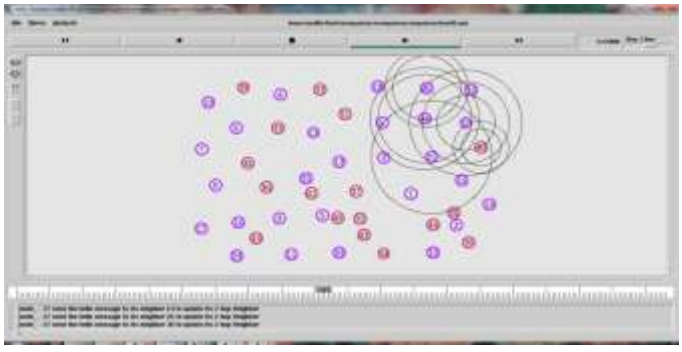

Fig.4 Topology formation for 2-hop neighbors

The topology formation for 2-hop neighbor is illustrated in Fig. 7. The pink coloured nodes indicate the node is in the state to start sending hello packets to its 2-hop neighbors. Node number 30 is performing topology formation for 2-hop neighbors. This node first send signal to nodes that are 2-hop distance away. After confirming the range the node number 30 acts as source and starts sending hello packets. Nodes that are 2-hop distance away acts as receivers. The violet coloured nodes indicate that node had already completed 2-hop topology formation

Data Routing

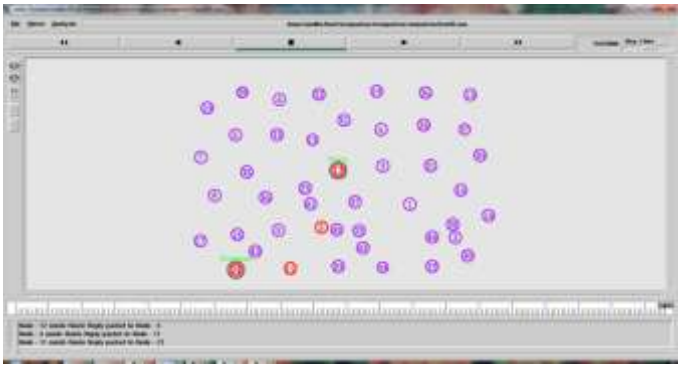

Fig.5 Discovery of source and destination nodes

The snapshot of last phase of the proposed system is displayed in Fig.11. After performing statistical traffic analysis and probability distribution, the node having the highest probability of being a sender and receiver is traced in the last phase. The outcome displays the source and destination node of the detected traffic pattern. These nodes are marked with red colour and labeled with green colour. The node number 12 is marked as source node, since it is having the highest probability of being sender. Similarly node number 23 is marked as destination node, as it is having the highest probability of being receiver

IV. RESULTS

Result Analysis

With the completion of simulation of the proposed system it is necessary to perform analysis of the system. This gives an assurance of the correct implementation of the proposed ideas. This analysis can be displayed through graphical analysis. The following are the outcomes of the analysis performed after simulation.

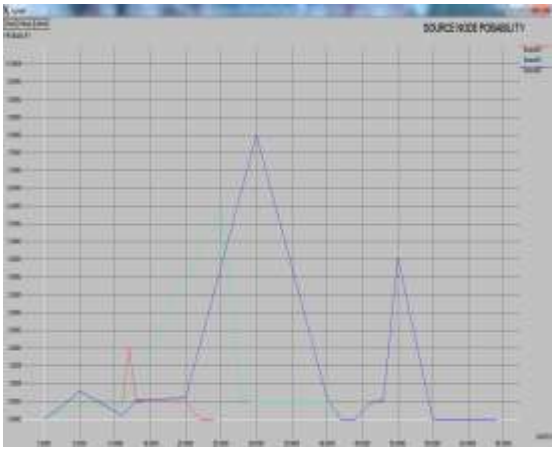

Fig.6 Source node probability analysis

 ISSN: 2321-8169
134 – 138

The analysis of source node probability is displayed in Fig. 12. The simulation is performed on three different total numbers of nodes. They are 25, 45 and 65. This graph shows the overall probability of being source node for each node in the network. The X-axis represents "Nodes", while Y-axis represents "Probability". The red colour line is used for 25 nodes, green for 45 nodes and blue for 65 nodes. For 25 nodes, the highest probability value as 2 is present between node numbers 10 to 15. For 45 nodes, the highest probability value as 6 is present between node numbers 10 to 30. While, for 65 nodes the highest probability value as 8 is present between node numbers 20 to 40

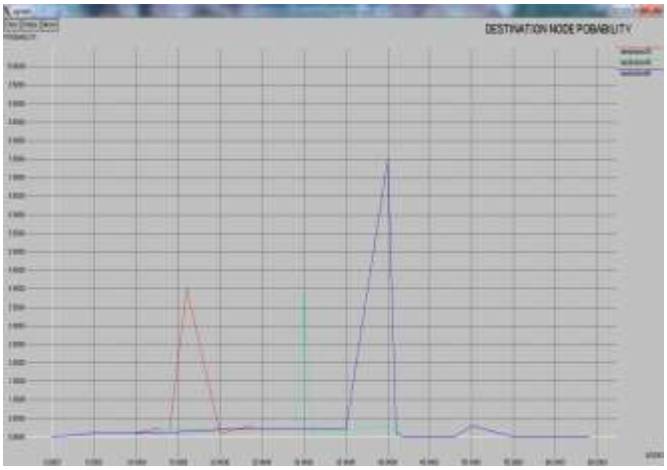

Fig.7 Destination node probability analysis

The analysis of destination node probability is displayed in Fig. 13. The simulation is performed on three different total numbers of nodes. They are 25, 45 and 65. This graph shows the overall probability of being destination node for each node in the network. The X-axis represents "Nodes", while Y-axis represents "Probability". The red colour line is used for 25 nodes, green for 45 nodes and blue for 65 nodes. For 25 nodes, the highest probability value as 4 is present between node numbers 10 to 20. For 45 nodes, the highest probability value as 4 is present between node numbers 25 to 35. While, for 65 nodes the highest probability value as 7.5 is present between node numbers 35 to 45.

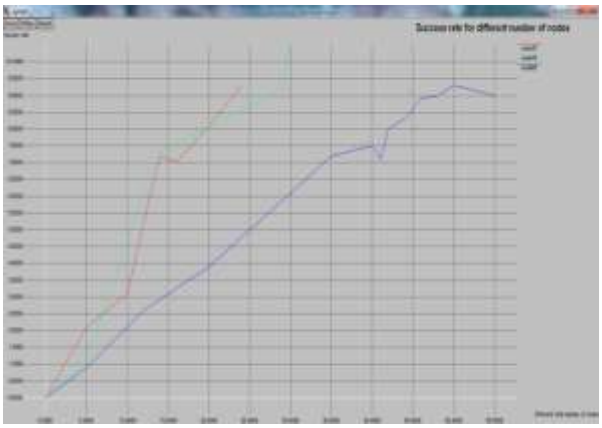

Fig.14 Success rate for probability distribution

The success rate for probability distribution is illustrated in Fig. 14. Success rate is calculated to find out the correctness of working of the proposed system. Success rate can be defined as percentage of success among a number of attempts. Here, graphical analysis is displayed for different number of nodes. The graphical analysis shows that how successfully simulation is carried out for three different numbers of nodes i.e. 25, 45 and 65. The X-axis represents "Different total number of nodes". While Y-axis represents "Success rate". The red line is used for 25 nodes, green for 45 nodes and blue for 65 nodes. From the graph it can be concluded that 45 nodes have the most successful success rate followed by 25 nodes and 65 nodes. The overall success rate obtained from this graph is 93.67%. In the graph some lines are in downfall position. This downfall can be seen in the simulation carried with total number of nodes as 65.

The reason for this downfall is due to increase in number of nodes. As the number of nodes in the network increases the system has to analyze more number of nodes. This result in increment in the number of packets transferred in the network. With increment in the number of nodes, there is increase in performing analysis. This definitely increase the time required to perform the traffic analysis. The success rate is inversely proportional to number of nodes. With increase in number of nodes the success rate falls down.

For example, consider a network having 10 nodes, all nodes are communicating with each other. So the number of packets transferred can be considered as 100 at any given point of time. The success rate can be considered as a probability value which cannot be more than 1. So the success rate for these 10 nodes will be 1/10=0.1. Now increase the number of nodes to 20, the packets will get increased to 200 and success rate will fall to 1/20=0.05.

From above example it is proved that success rate decreases with increase in number of nodes. The formula for success rate used in this proposed system is:

$$\text{Success rate} = \frac{\text{Sucsess}}{\text{No. of attempts}}$$

Where "Success" refers to the success of getting same node number multiple times as source or destination and "No. of attempts" refers to the number of times the simulation has been executed.

V. CONCLUSION AND FUTURE SCOPE

The main purpose of the proposed system is to disclose the identity of source and destination nodes in the network. This can be fulfilled by discovery of communication pattern. The communication pattern is discovered without decrypting the packets. This has been satisfied by using best-first search (a heuristic approach) for traversing the path, statistical traffic analysis for analyzing and to identify point-to-point transmission among receivers. This is followed by calculating probability distribution to find out approximate source and destination nodes in the traced path. This reduces anonymous communication which is one of the characteristics in mobile

ad-hoc network (MANET).The overall success rate obtained from the graph of success rate for probability distribution is 93.67%, while overall success rate obtained from the graph of success rate for different traffic pattern is 78.33%.

Best-First Search is one of the heuristic search algorithms that have been utilized in this proposed system. However, this best-first search has a drawback. Best-First Search algorithm terminates when no optimal path is found. This drawback can create an obstacle to find out the communication path of the adversary. Thus, in future instead of best-first search A* or AO* can be used as a heuristic search approach.

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] Lei Liu, Xiaolong Jin, Geyong Min, and Li Xu, "Real-Time Diagnosis of Network Anomaly based on Statistical Traffic Analysis", IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications, 2012.

[3] 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, pp. 1-9, 2010.

[4] Benjie Lu and Zhingqing Liu,"Prolog with Best First Search", IEEE 25th Chinese Control and Descision Conference, 2013.

[5] Douglas Kelly, Richard Raines, Rusty Baldwin, Michael Grimaila, and Barry Mullins, "Exploring Extant and Emerging Issues in Anonymous Networks: A Taxonomy and Survey of Protocols and Metrics", IEEE Communications Surveys & Tutorials, Vol. 14, No. 2, Second Quarter 2012.

[6] Tehrani, A.H. and Shahnasser, H.," Anonymous communication in MANET's, solutions and challenges," IEEE International Conference on Wireless Information Technology and Systems (ICWITS), pp. 1-4, 2010.

[7] Y. Qin and D. Huang, "OLAR: On-Demand Lightweight Anonymous Routing in MANETs," Proc.Fourth Int'l Conf. Mobile Computing and Ubiquitous Networking, pp. 72-79, 2008.

[8] 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.