RESEARCH ARTICLE OPEN ACCESS

E-APSAR:Enhanced Anonymous Position Based Security Aware Routing Protocol For Manets

Priyanka Malgi∗, Ulka Padwalkar∗
St. Francis Institute of Technology, Mumbai-400103, India,
St. Francis Institute of Technology, Mumbai-400103, India

Abstract
In the past few years, we have seen a rapid expansion in the field of mobile computing due to the pro- liferation of inexpensive, widely available wireless devices or networks.However, all these networks are conventional wireless networks as they require a fixed network infrastructure with centralised administration for their operation, potentially consuming a lot of time and money for set-up and maintenance.Drawbacks of conventional wireless networks are driving a new alternative way for mobile communication, in which mobile devices form a selfcreating, self-organising and self-administering wireless network, called a mobile ad hoc network.In mobile ad-hoc networking (MANETs), nodes communicate to each other based on public identities. In this paper,for a position based routing[22] an innovative packet forwarding mechanism is proposed in which source node generates route request packet and broadcast packet to other neighbor nodes to locate destination by implementing black hole attack[8]. Proposed E-APSAR (Enhanced Anonymous Position Based security aware routing protocol) is implemented on NS-2 and results shown significant improvement over original DSR in terms of various performance metrics. It has been found that on dense network certain numbers of malicious nodes are supportive to reducing communication overhead and because of density negative effect of malicious attacks which is proposed E-APSAR that is able to reduce. Hence result shows proposed E-APSAR will be helpful to decrease communication overhead.
Index Terms—Ad-hoc, Anonymity, Geographic routing, Secu- rity,Black hole attack,DSR.

I. INTRODUCTION

The field of wireless and mobile communications has expe- rienced an unprecedented growth during the past decade.The new age of Information Technology is a drastic change from traditional regular desktop computing, where there is a need for isolated workstations communicate to each other through shared servers in a fixed network, to an environment where a large number of different platforms communicate over multiple network platforms. In this environment the devices adapt and reconfigure themselves individually and collectively, to support the requirements of mobile users. MANETs are a kind of wireless ad-hoc networks that usually has a routable networking environment on top of a Link Layer ad hoc network. Opposed to infrastructured wireless networks, where each user directly communicates with an access point or base station, a mobile ad hoc network, or MANET, does not rely on a fixed infrastructure for its operation. The growth of laptops and 802.11/Wi-Fi wireless networking has made MANETs a popular research topic since the mid 1990s.[2]

Mobile ad hoc networks (MANETs) are autonomous col- lection of mobile nodes which communicate over relatively bandwidth constrained wireless links. MANETs exhibit very interesting properties: they are self-organizing, decentralized and support mobility. Hence, they are very good candidates for tactical networks in military applications. Nodes that lie within each others send range can communicate directly and are responsible for dynamically discovering each other. In order to enable communication between nodes that are not directly within each others range, intermediate nodes act as routers that relay packets generated by other nodes to their destination

The specific characteristics of MANETs impose many challenges to network protocol designs on all layers of the protocol stack . All network protocol developments need to integrate smoothly with traditional networks and take into account possible security problems[21].There are many challenging security issues which need to be addressed before MANETs are ready for widespread commercial or military deployment. Major security problem is the issue of secure routing in the presence of selfish or malicious nodes, which selectively drop packets they are required to forward and in so doing, these selfish or malicious entities can cause various communication problems.

A. DSR:Dynamic Source Routing

The Dynamic Source Routing protocol (DSR) is a simple and efficient routing protocol designed specifically for use in multihop wireless ad hoc networks of mobile nodes. DSR allows the network to be completely self-organizing and self-configuring, without the need for any existing network infras- tructure or administration. The protocol is composed of the two mechanisms of Route Discovery and Route Maintenance, which work together to allow nodes to discover and maintain source routes to arbitrary destinations in the ad hoc network [3]

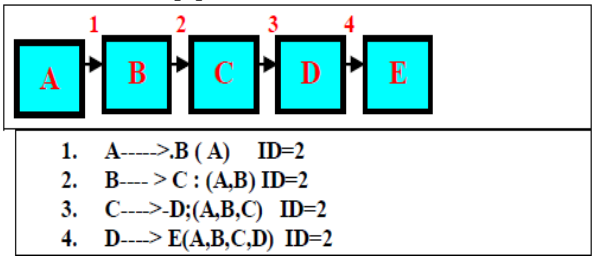

Fig. 1. Examples of different zone partitions

B. Black Hole Attack in DSR

A black hole attack [4] is a kind of denial of service attack where a malicious node can attract all packets by falsely claiming a fresh route to the destination and absorb them without forwarding them to the destination. MANETS are vulnerable to various types of attacks. On the basis of different characteristics the attack on mobile ad hoc network is classified as passive and active attacks. One such active attack is Black hole attack. A black hole is a node that has the characteristics that it always responds with a RREP message to every RREQ, even though it does not really have a legitimate route to the target node. A Black Hole attack [5] [7] is a kind of denial of service where a malicious node can absorb all data packets by fallaciously claiming a new and fresh route to the destination and then drops them without delivering them to the destination. Cooperative Black hole means the malicious nodes act in a group. In black hole attack [6][4], the malicious node waits for the neighbours to initiate a RREQ packet. As the black hole node receives the RREQ packet, it will immediately send a forged RREP packet to the source node advertising itself as having the shortest and optimum route path to the target destination. On receiving of RREP the source node thinks discovery of route process is over, discards other RREP messages from other nodes and choose the path through the malicious node to route the data packets and starts to transmit the data packets over malicious node as shown in figure 2. When the data packets reach the black hole node that malicious node absorbs the entire packet and dropped them instead of forwarding them to the intended destination which results in denial of communication.

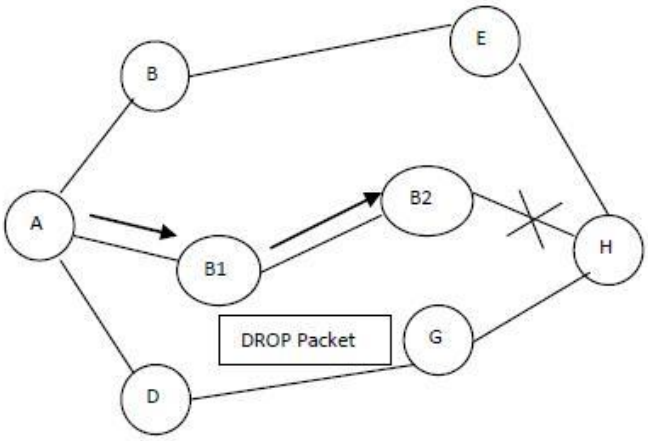

Fig. 2. Black Hole Attack

C. Problem Statement

MANET characteristic possess many security challenges. From literature can conclude that there are certain attacks and found that malicious nodes have harmful effect on net- work.When thinking for remedy on these attacks, Density play important role. Cooperation based network works with coop- eration of participate nodes. As number of nodes is increasing cooperation gets better. Basic characteristic of adhoc network suggest cooperation from participating nodes and DSR works with only cooperation. It has been found that DSR protocol works with source routing mechanism in which source node generates route request packet and broadcast packet to other neighbor nodes to find destination which increases routing overhead and collision in network [8].

II. IMPLEMENTATION OF PROPOSED ALGORITHM E-APSAR

A. Implementation

DSR and Proposed E-APSAR are tested on NS-2 which is a discrete event simulator targeted at networking research. It provides substantial support for simulation of TCP, routing and multicast protocols over wired and wireless networks. It consists of two simulation tools. The network simulator (ns) contains all commonly used IP protocols. The network animator (nam) is use to visualize. Ns-2 fully simulates a layered network from the physical radio transmission channel to high-level applications. The ns-2 simulator has several features that make it suitable for experimental result.
Ns-2 is an object-oriented simulator written in C++ and OTcl. The simulator supports a class hierarchy in C++ and a similar class hierarchy within the OTcl interpreter. There is a one-to-one correspondence between a class in the interpreted hierarchy and one

in the compile hierarchy. The reason to use two different programming languages is that OTcl is suitable for the programs and configurations that demand frequent and fast change while C++ is suitable for the programs that have high demand in speed. Ns-2 is highly extensible. It not only supports most commonly used IP protocols but also allows the users to extend or implement their own protocols. It also provides powerful trace functionalities, which are very important in our research since various information need to be logged for analysis [9].

B. Algorithm for Proposed E-APSAR PROTOCOL

1. Node Initialization:Node environment is created.
2. Zone Creation wherein the network area is divided into zones.
3. Zone Discovery Process wherein each node discovers its zonal head and exchanges routing related information.
4. Read Malicious Nodes information from file.
5. Key Generation for transmitting data securely
6. Source node starts data transmission to destination
7. It selects first neighbor in zone and transmits data securely using encryption to first neighbor
8. Check whether current node is malicious or not
9. If Malicious then forward all route request and route reply packets and drop data packets else forward route request and route reply as well as data packets.
10. The neighbour then forwards packet to next zone till it is received by destination zone.
11. Finally the destination node retrieves all data received successfully using decryption.

III. EXPERIMENTAL SETUP

The performance is analyzed against parameters such as mobility, no. of nodes. For the performance analysis of the protocol extensions, DSR network is used as a base reference. The experimental results are being studied under NS-2 Simu- lator. Experiments have been carried out in order to evaluate performance of MANETs under various routing attacks with the effect of density of network.

The aim is to reduce no. of routing request packets. DSR and Proposed E-APSAR are simulated in same settings of parameters and scenarios. Experiments are run on 4 different mobility and also on different no. of nodes. The mobility model is Random Waypoint model of 1000 * 1000 metres. It has focused more attention on the evaluation of network performance in terms of routing overhead, throughput, and packet delivery ratio and normalized routing load of a mobile adhoc network where a number of nodes and numbers of malicious nodes both are varying[28]. Following parameters are set for experiments on network simulator ns2.

TABLE I
SI M U L AT I O N SC E NA R I O SE T U P [?]

Parameter	Value
Number of Nodes	10,20,30,40,50
Topology	Mobile
Mobility model	Random Way Point
Simulation Time	1000
Simulation Area	1000 x 1000
Routing Protocol	DSR , AODV
Traffic Model	Constant Bit Rate
Packet Size	1000 Bytes
Interval	1 Sec

IV. RESULT ANALYSIS OF MOBILITY BASED DSR AND E-APSAR

• Throughput: Network throughput is the average rate of successful message delivery over a communication channel. This data may be delivered over a physical or logical link, or pass through a certain network node. The throughput is usually measured in bits per second (bit/s or bps), and sometimes in data packets per second or data packets per time slot.

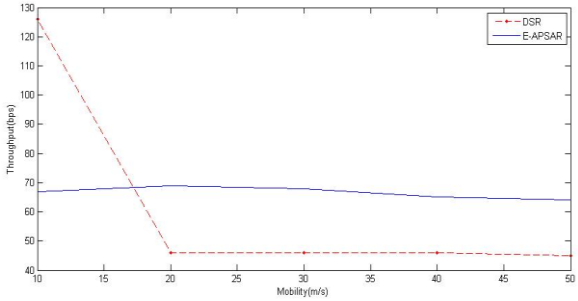

Fig. 3. Mobility Vs Throughput

Figure 3 shows Mobility Vs Throughput in DSR and E- APSAR. It is analyzed that as mobility increases in network throughput is decreasing as speed increases due to breaking of connection between nodes and packets are being discarded in DSR but in E-APSAR throughput is increasing for some specific mobility after that it is also decreasing as breaking of routes and connection between nodes.

• Routing Overhead Nodes often change their location within network. So, some musty routes are generated in the routing table which leads to unnecessary routing overhead

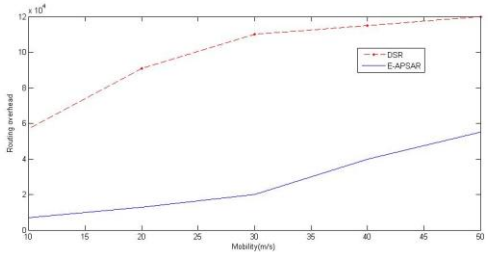

Fig. 4. Mobility Vs Routing Overhead

Figure 4 shows Mobility Vs Routing Overhead in DSR and E-APSAR. The experimental results of dynamic topology where nodes tend to move from one place to another place at different time frame. So links may break and re-route discovery required. It is required to establish lots of connection because of this movement. Line Graph clearly suggests that as mobility increasing in network overall routing overhead will increase.

• Average end-to-end delay of data packets There are possible delays caused by buffering during route discov- ery latency, queuing at the interface queue, retransmission delays at the MAC, and propagation and transfer times. Once the time difference between every CBR packet sent and received was recorded, dividing the total time difference over the total number of CBR packets re- ceived gave the average end-to-end delay for the received packets. This metric describes the packet delivery time: the lower the end-to-end delay the better the application performance

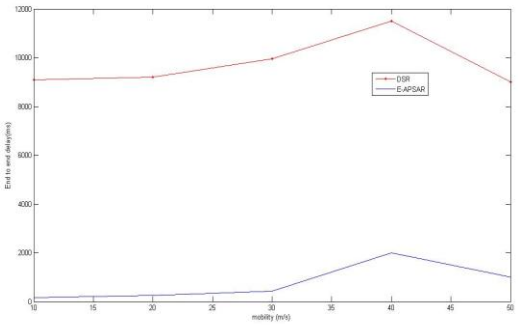

Fig. 5. Mobility Vs E2E Delay

Figure 5 shows Mobility Vs E2E Delay in DSR and E- APSAR. From this, it is analyzed that as mobility increases in network the delay time between deliveries of packets between nodes is also increasing due to more breaking of connection between nodes but as mobility increases highly the delay decreases thus E-APSAR is also acting beneficially as mobility increases to some extent.

• Packet Delivery Ratio Packet delivery ratio is defined as the ratio of data packets received by the destinations to those generated by the sources. This performance metric gives us an idea of how well the protocol is performing in terms of packet delivery at different speeds using different mobility.

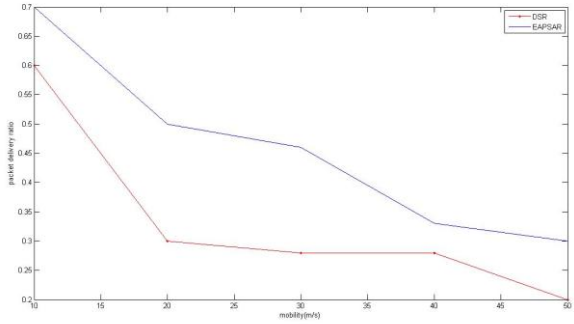

Fig. 6. Mobility Vs Packet Delivery Ratio

Figure 6 shows Mobility Vs Packet Delivery Ratio in DSR and E-APSAR. It shows the impact of changing the speed, with which nodes move in an ad hoc network, on the packet delivery ratio. In general, packet delivery ratio decreases with increase in average node speed. E-APSAR also shows that packet delivery ratio increases as speed increases s from 5 to
10 but then it continually decreases as mobility increases.

V. CONCLUSION AND FUTURE WORK

The performance of routing protocols in MANET is very much affected by different kind of attacks. The results of simulation show that this attack has high effect on DSR protocol. In black-hole attack case, based on the number of attacker, the throughput is high or low. As the number of ma- licious nodes increases, the throughput will go on decreasing, because actually data packets are dropped rather than routing packets[28]. Similarly for all four parameters, the performance of E-APSAR is better than baseline DSR protocol.

Future work lies in modifying E-APSAR in an attempt to fight stronger, active attackers as Grey hole and other types of Attacks and selfish behavior of nodes and to be proved by related theoretical and simulation results.

REFERENCES

[1] Jeroen Hoebeke, Ingrid Moerman, Bart Dhoedt and Piet Demeester,“ An Overview of Mobile Ad Hoc Networks: Applications and Challenges”.

[2] Priyanka Malgi, D.D. Ambawade,“ Anonymous Position Based security aware routing protocol”, Proc. of ICCT,2013.

[3] D B. Johnson, D A. Maltz, and Y. Hu. The dynamic source routing protocol for mobile ad hoc network, IETF, pp 43-53, April 2003.

[4] Dow CR, Lin PJ, Chen SC, Lin JH, Hwang SF, A Study of Recent Research Trends and Experimental Guidelines in Mobile Ad-hoc Net- works. IEEE 19th International Conference on Advanced Information Networking and Applications, Tamkang University, Taiwan pp 72-77, 28-30 March 2005.

[5] Ashish T. Bhole, Prachee N. Patil, Study Of Black hole Attack in MANET, International Journal of Engineering and Innovative Technology (IJEIT) Volume 2, Issue 4 pp 99-102, October 2012.

[6] N.Bhalaji, Dr.A.Shanmugam,Association between nodes to combat black hole attack in DSR based MANET, 978-1-4244-3474-9/09/ pp 403-407, IEEE 2009.

[7] Samba Sesay, Zongkai Yang and Jianhua He,"A Survey on Mobile AdHoc Wireless Network, Information Technology Journal 3 (2): 168-175, 2004, ISSN 1682-6027 2004 Asian Network for Scientific Information, pp 169-175.

[8] Rooshabh Kothari, Deepak Dembla," Implementation of Black Hole Security Attack using Malicious Node for Enhanced - DSR Routing Protocol of MANET", International Journal of Computer Applications (0975 8887) Volume 64 No.18, February 2013.

[9] http://www.isi.edu/nsnam/ns/