iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 3 **Issue:** Issue II **Month of publication:** June 2015

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Proactive Source Routing With Attacker Detection and Filtering For Mobile Ad Hoc Networks

Trupthi B T
P G Student, Dept of Electronics and communication,
SEA College of Engineering and Technology, Bangalore, India.

Abstract*—Source routing protocol has been in use since ages and is found to be one of the most efficient ways for data forwarding.The paper proposes a source routing protocol named proactive source protocol (PSR) for mobile adhoc networks. The transmitter picks the best forwarder from multiple receivers, after receiving the data successfully the transmitter explicitly requests the selected node to forward the data. The nodes are checked for any malicious content. On the presence of malicious data, the attacker is detected and the node is filtered using kalman filtering. PSR protocol maintains a better network topology than the other source routing protocols such as dynamic source routing protocol, Adhoc on demand distance vector protocol. The analysis and the results indicate that the overhead required for PSR is comparatively less when compared to the other source routing protocols. The proposed system yields better data transportation performance.

Keywords*—Source Routing, Mobile Ad Hoc Networks, Dynamic source routing , Adhoc on demand distance vector protocol,Kalman Filtering

I. INTRODUCTION

Source routing allows a sender of a packet to partially or completely specify the route the packet takes through the network. In the case of non source routing protocols ,routers in the network determine the route the path based on the path's destination. A mobile ad hoc network (MANET) is a wireless communication network, where nodes that are not within the direct transmission range of each other require other nodes to forward data. It can operate without existing infrastructure and support mobile users, and it falls under the general scope of multihop wireless networking. Proactive source routing protocol (PSR) is a lightweight protocol designed to facilitate opportunistic data forwarding in MANETs. In PSR, each node maintains a breadth-first search spanning tree of the network rooted at it. This information is periodically exchanged among neighbouring nodes for updated network topology information. Thus, PSR allows a node to have full-path information to all other nodes in the network, although the communication cost is only linear to the number of the nodes. This allows it to support source routing.

II. LITERATURE SURVEY

Researchers have emphasised on network layer as it favours functioning of various routing protocols. The most salient research challenges in areas include end-to-end data transfer, link access control, security, and providing support for real-time multimedia streaming [1]. Reference [2] proposes abundant routing protocols in the network with differing objectives and for various specific needs. Opportunistic data forwarding represents the solutions to utilize the broadcast nature of wireless communication links [3]. The initial works on opportunistic data forwarding are carried out and contribute tremendously to the development of the data forwarding techniques [4]. Reference [5] proposes optimization techniques such as multihop relaying in optimized link state routing (OSLR) protocol. The support of opportunistic data forwarding in a MANET with constantly active data communication between many node pairs, the reactive nature of dynamic source routing (DSR) protocol renders it unsuitable [6]. The examples of proactive routing protocols include destination sequenced distance vector (DSDV) [7]. The development and the methodology of an as on demand protocol named ad-hoc on demand distance vector (AODV) protocol is .prescribed in [8].

III. DESIGN OF PROACTIVE SOURCE ROUTING PROTOCOL

Reactive protocols on receiving the routing information from upper layers, the mode finds out the way to reach the destination. The proactive protocols are table driven. PSR protocol is designed using the concept of tree based routing. To make the protocol compatible to MANET's the advantage of both "event driven" and "timer driven" is taken into account for route update strategy.

The links are checked for affected nodes to avoid duplicate nodes in the network. The design and the analysis of the protocol is carried out using JAVA and the database of the nodes is maintained using Microsoft Access.

A. Tree based Routing

The nodes in the PSR protocol are arranged in a tree structure. The update operation of PSR is iterative and distributed among all the networks. The base station node is first activated and the type of service to provide is browsed and selected by the users. Once the service is selected the sender and the receiver are selected. By utilizing the contention feature of the medium access control (MAC) sublayer, the forwarder closer to the destination will access the medium more aggressively. Therefore, the MAC sublayer can determine the actual next-hop forwarder to better utilize the long-haul transmissions. The fig 1 shows the arrangement of the base station and the receivers. The internet protocol (IP) address of each node is update in the routing table.

B. Differential Update

PSR provides every node with a breadth-first spanning tree (BFST) of the entire network rooted at it. The nodes periodically broadcast the tree structure. Based on the information collected from neighbours during the most recent iteration,

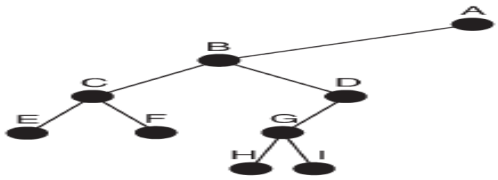


Fig 1: Binary tree representation of nodes

a node can expand and refresh its knowledge about the network topology by constructing a deeper and more recent BFST.

To achieve streamline differential routing updates, the two features are used: compact tree representation and an attempt of the nodes to maintain an updated BFST as the network topology changes. The following can be explained using mathematical equations. Consider node v and its BFST T_v. When it receives an update from neighbour u which is denoted by T_u, it first removes the sub tree of T_v rooted at u. Then, it incorporates the edges of T_u for a new BFST. The BFST of $(T_v - u) \cup T_u$ may not contain all necessary edges for v to reach every other node. The difference between two BFSTs can be represented by the set of nodes that have changed parents, which are essentially a set of edges connecting to the new parents

C. Attacker detection

The process of attacker detection and filtering comprises of many modules.

1) *Service Provider:* The service provider will browse for the data files and initialize the MAC address to the nodes. After initializing the nodes, a particular nose is destined as the receiver and the data file is forwarded in router less cost. Simultaneously, the router is updated with the MAC address and the data files. On receiving the data successfully the router acknowledges the service provider.
2) *Router:* The router consists of n-number of nodes to offer service. The router will receive the data file from the service provider and select a less cost or less sleep node to send data files to the particular end user. If any attacker is found in the router, then the router will select alternate less cost node and forward the data to the destination. In a router we can assign node cost, view node details and view attackers.
3) *Intrusion Detection System Manager:* An Intrusion Detection System (IDS) is a device or a software application that monitors network for malicious activities. Using IDS manager the user can view an attacker details with their tags such as attacker name, node name, Mac address, time and date.
4) *Kalman Filter:* The kalman filter keeps track of the estimated state of the system and the variance or uncertainty of the estimate. It is also known as linear quadratic estimation (LQE), is an algorithm that uses series of measurements observed over time containing noise and other inaccuracies. It is applied in trajectory optimization which refers to the process of designing a trajectory that minimizes or maximizes some measure of performance within the constrained boundaries.
5) *MAC Address:* A media access control (MAC) address is a unique identifier assigned to network interfaces for communications on the physical network segment. It is used as a network address for most IEEE 802 network technologies. Logically, MAC addresses are used in the media access control protocol sublayer of the open system interconnect (OSI) reference model.

Fig 2 represents the process of attacker detection and filtering. The process depicts the functionality of each module. The data files can be considered as the type of service chosen by the user.

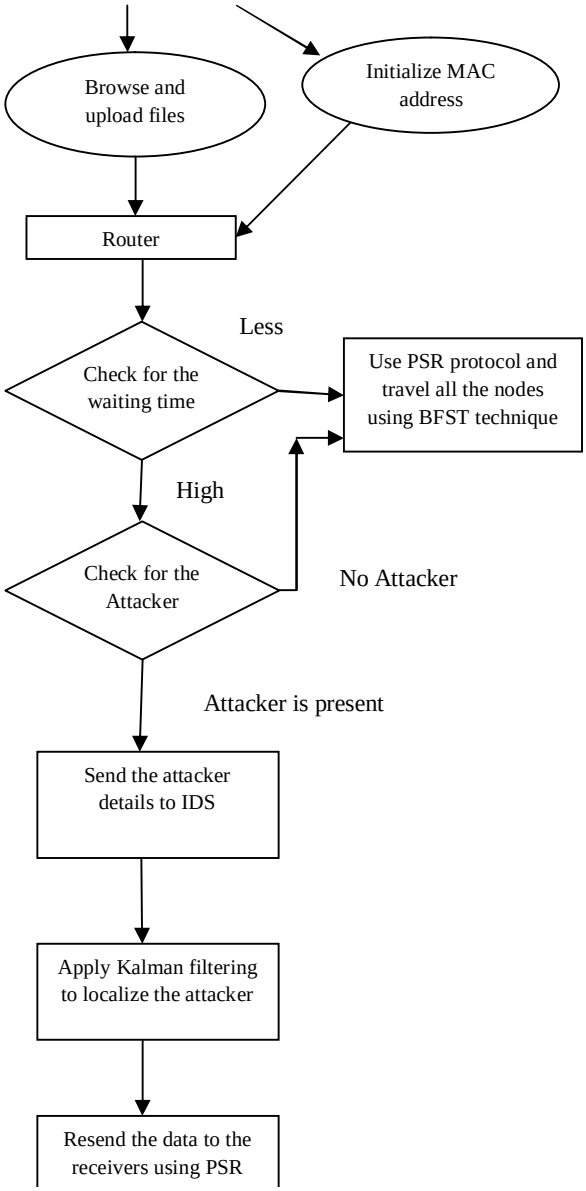


Fig 2: Flow chart for Attacker detection and filtering

IV. RESULTS

The protocol is designed efficiently using the coding language Java-Swings. It can be concluded that the experimental results prove that the routing protocol maintains a better network topology compared to other source routing protocols. Fig 3 represents the service provider module. It is used to initialize nodes and select the type of service required.

The module consists of various buttons where each button performs specific functions.

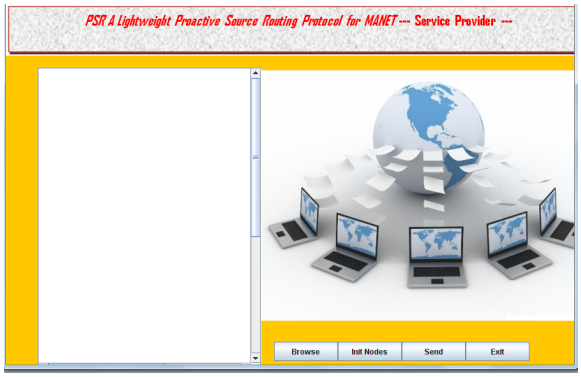


Fig 3: Service Provider Module

The data forwarding is efficient using less hop limit. Fig 4 shows the module working of the PSR protocol where the nodes are arranged in a tree structure.

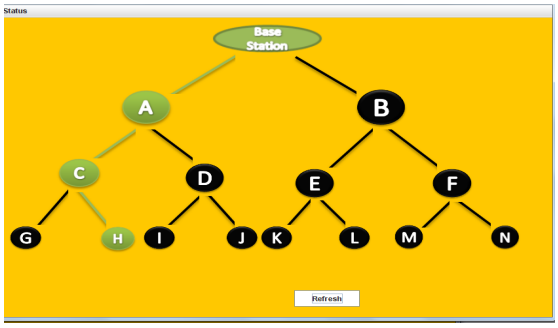
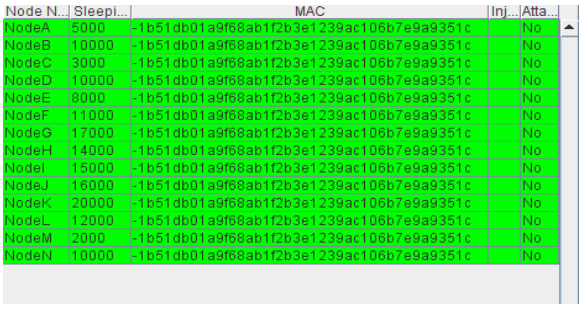


Fig 4: Data forwarding between the nodes.

The status of the MAC table can be viewed to detect the malicious message. The MAC address is proved to be same for the nodes as the transmitter picks its best forwarder from the receiver list. The table also gives the sleeping time for each node. Fig 5 depicts the MAC table comprising of the unique IP addresses.



Node N...	Sleepi...	MAC	Inj...	Atta...
NodeA	5000	-1b51db01a9f68ab1f2b3e1239ac106b7e9a9351c		No
NodeB	10000	-1b51db01a9f68ab1f2b3e1239ac106b7e9a9351c		No
NodeC	3000	-1b51db01a9f68ab1f2b3e1239ac106b7e9a9351c		No
NodeD	10000	-1b51db01a9f68ab1f2b3e1239ac106b7e9a9351c		No
NodeE	8000	-1b51db01a9f68ab1f2b3e1239ac106b7e9a9351c		No
NodeF	11000	-1b51db01a9f68ab1f2b3e1239ac106b7e9a9351c		No
NodeG	17000	-1b51db01a9f68ab1f2b3e1239ac106b7e9a9351c		No
NodeH	14000	-1b51db01a9f68ab1f2b3e1239ac106b7e9a9351c		No
NodeI	15000	-1b51db01a9f68ab1f2b3e1239ac106b7e9a9351c		No
NodeJ	16000	-1b51db01a9f68ab1f2b3e1239ac106b7e9a9351c		No
NodeK	20000	-1b51db01a9f68ab1f2b3e1239ac106b7e9a9351c		No
NodeL	12000	-1b51db01a9f68ab1f2b3e1239ac106b7e9a9351c		No
NodeM	2000	-1b51db01a9f68ab1f2b3e1239ac106b7e9a9351c		No
NodeN	10000	-1b51db01a9f68ab1f2b3e1239ac106b7e9a9351c		No

Fig 5: MAC table

In the presence of malicious data it can be detected that the MAC address table is injected with the attacker's message at the particular node. The malicious data can be detected and filtered Fig 6 emphasises on the presence of attacker in the network.

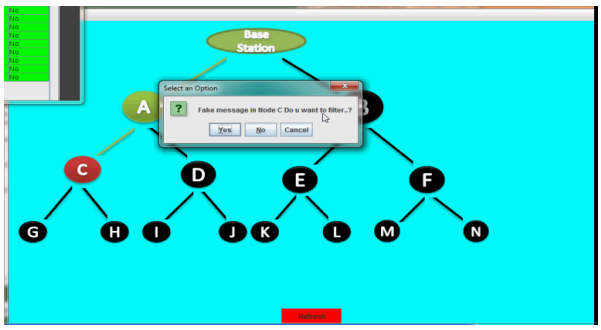


Fig 6: Presence of the attacker in the network

V. CONCLUSION

This paper presents the source routing protocol for data forwarding in MANETs. The protocol provides more topology information compared than the baseline source routing protocols. The overhead is significantly smaller than the other link state routing protocols. We put forward a tree-based routing protocol with its routing overhead per time unit per node is on the order of the number of the nodes in the network but each node has the full-path information to reach all other nodes. The MAC addresses are periodically updated before broadcasting. The attacker details can be traced out using IDS manager and filtered using Kalman filtering technique.

The protocol is efficient and yields better data transportation performance than the other source routing protocols.

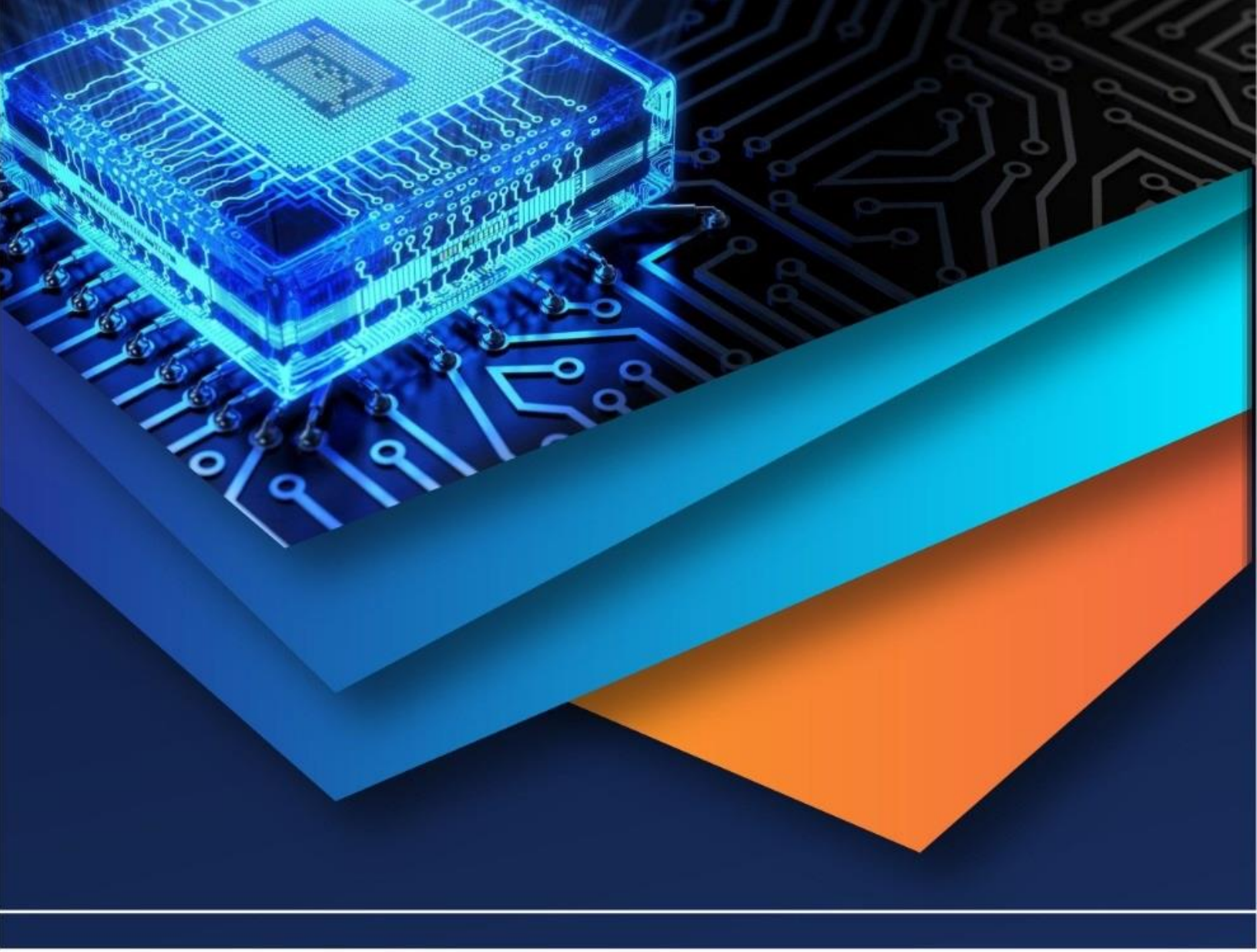
VI. FUTURE WORKS

As with many protocol designs, in many situations working on PSR faced tradeoffs. During forwarding the data in source routing protocols the user defines the path for the data to reach the destination. In this case if the allocated path has much traffic or if the link has experienced failure the data has no other alternate path as it's not defined by the user. In such situations the routing table at the nodes come handy.

When a data packet is forwarded to a neighbour that no longer exists, it causes link layer retrial, backlogging of subsequent packets, and TCP congestion avoidance and retransmission. Multiple trees can be incorporated at one time which makes it computationally more efficient.

REFERENCES

[1] M. Al-Rabayah and R. Malaney, "A new scalable hybrid routing protocol for VANETs," IEEE Trans Veh Technology, vol 61, no 6, pp 2625-2635, July 2012.
[2] R. Rajaraman, "Topology control and routing in ad hoc networks: A survey," ACM SIGACT News, vol. 33, no. 2, pp. 60–73, June. 2002.
[3] Y. P. Chen, J. Zhang, and I. Marsic, "Link-layer-and-above diversity in multi-hop wireless networks," IEEE Commun. Mag., vol. 47, no. 2, pp. 118 124, Feb. 2009.
[4] P. Larsson, "Selection diversity forwarding in a multihop packet radio network with fading channel and capture," ACM Mobile Comput Commun Rev, vol 5, no 4, pp 47-54, Oct 2001.
[5] T. Clausen and P. Jacquet, "Optimized Link State Routing Protocol (OSLR)," RFC 3626, Oct 2003.
[6] D. B. Johnson, Y.-C. Hu, and D. A. Maltz, "On the Dynamic Source
Routing Protocol (DSR) for mobile ad hoc networks for IPv4," RFC 4728,
Feb. 2007.
[7] C. E. Perkins and P. Bhagwat, "Highly dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for mobile computers," Comput. Commun. Rev., vol. 24, pp. 234–244, Oct. 1994.
[8] C. E. Perkins and E. M. Royer, "Ad hoc On-Demand Distance Vector (AODV) routing," RFC 3561, Jul. 2003.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY