*2011 International Conference on Information and Network Technology*
*IPCSIT vol.4 (2011) © (2011) IACSIT Press, Singapore*

# Secure and Reliable Ad-Hoc on Demand Multipath Distance Vector Routing Protocol for Mobile Ad Hoc Networks

Mr. Bhushan M. Manjre [1], Mrs.Veena A. Gulhane [2]

[1]Dept. of Computer Science & Eng., G.H. Raisoni College of Eng., Nagpur 440002, India.
bhushan.manjre@gmail.com

[2]Asst. Professor, Dept. of Computer Science & Eng,G.H. Raisoni College of Eng., Nagpur 440002, India.
vinagulhane@gmail.com

**Abstract.** In a MANET, Node misbehavior is any such behavior that proves harmful to co-operative environment of MANET. Many schemes have been recently proposed for the detection and avoidance of misbehavior nodes, but still there are many issues like false detection due to network layer factors, packet dropping and packet delaying misbehavior which are yet to be addressed completely. The aim of the proposed approach is to mitigate the above mentioned problems of network layer misbehavior shown by mobile nodes in MANET. Based on AOMDV protocol, the proposed approach achieves this by finding reliable and secure paths for data packets before transmitting them. Since paths are verified for security and reliability at the beginning of data transmission, hence probability of packet loss/delay misbehavior is minimum. If any node in any path shows misbehavior, then that path is avoided and behavior check mechanism is triggered over that path so as to detect and check misbehaving nodes for misbehavior reasons. If misbehavior is due congestion, collision, transmitted power level or buffer overflow then the node is temporarily avoided but not blacklisted as 'misbehaving node' and thus avoiding false detection. In the proposed approach, two types of control packets viz. TPI and PFI control packets are used to detect and avoid misbehaving nodes. Also it eliminates reputation based system and promiscuous overhearing. Hence, the network throughput can be optimized in terms of security, reliability, processor and energy consumption as well as end to end delay.

**Keywords:** Co-operative multi hop forwarding capability, behavior check mechanism, misbehavior etc.

## 1. Introduction

A mobile Ad-Hoc Network (MANET) is a set of mobile nodes that form a wireless network without any fixed infrastructure. Each node pays role of both, a host i.e. an end system that executes applications and acts as source or destination and a secondly a router that relays data traffic for other nodes. Since these are mobile nodes and free to move randomly, hence network topology alters frequently. The network topology depends upon the current location and transmitting power of nodes. When node acts as router, its main task is to forward data packets for other nodes plus discovery and maintenance of routes to the destination.

Mobile ad hoc networks are a wireless network in which paths between sources to destination are formed on ad hoc basis. In such self-organized networks, each node has to forward data traffic unrelated to its own use. But being a router for other nodes leads to consumption of battery, processing and bandwidth resources of the router node. So, in order to achieve maximum throughput with the available resources, a node may not be willing to contribute their resources to maintain network connectivity. Such selfish behaviour may result into damages like denial of service which in turns degrades the performance of the network in terms of network throughput and packet delivery ratio because most existing routing protocols in MANET are aiming at finding most efficient path.

### 1.1 Misbehavior of Nodes

Misbehaviour of Node is any such behaviour that goes in total conflict of cooperative working environment of an ad hoc network. A misbehaviour threat can be defined as an unauthorized behaviour of an internal node that can result unintentionally in damage to other nodes, i.e., the aim of the node may not to launch an attack, but it may have other aims such as obtaining an unfair advantage compared with the other nodes [10]. Nodes will misbehave if controlled or programmed to do so by their owners or users with distinct dimensions of misbehaviour as follows [10]:

- Accidental or deliberate.
- Selfish or malicious
- Individual or collusion

Hence if we can identify and avoid misbehaving nodes before or during communication session, we can prevent the overall operation of ad hoc networks from getting hampered from various perspectives. In this paper, a novel multi path routing scheme is proposed to address the above mentioned routing layer misbehaviour.

### 1.2 Organization

The rest of the paper is organized as follows:

Section 2 describes the proposed work. Section 3 concludes this paper and outlines the future work. Section 4 points out references.

## 2. Proposed Work

In MANET, Ad-hoc On-Demand Multi path Distance Vector Routing (AOMDV) protocol is reactive routing protocol, uses multiple paths between source and destination. AOMDV, being multi path routing protocol, has more message overhead during route discovery and load balancing and hence traffic load increases, which consume both channel bandwidth as well as the battery power of nodes for communication and processing. This increased traffic load consumes more CPU cycles, battery and other resources of node which leads to increased misbehaving tendency of node since a node may try to save its battery and other resources especially when it is intermediate node in communication. The proposed mechanism is divided into three modules. Module I comprises of detection of misbehaving nodes in AOMDV protocol. Module II will remove the threats imposed by misbehaving nodes. Module III will be dedicated to optimization of network performance.

### 2.1 Detection of Misbehaving Nodes

In this module, the first step is the route discovery so as to obtain the set of node disjoint paths. One path is used as primary path and rest are kept as backup paths. Backup paths are used when primary path fails to transfer data. We give ID to each node disjoint path in the route cache from 0 to n. Here two types of control packets viz. TPI (Total path information) Packet and PFI (Path failure information) Packet are used. TPI packet is consisting of five field's viz. Source ID, Destination ID, Timeout value, Total number of paths i.e. n and the ID of the path over which that TPI packet is sent. PFI Packet contains attack identifier (value 0 for packet delay and 1 for packet dropping), and ID of failure paths.

| Source ID | Destination ID | Timeout Value | Total no. of Paths | Path ID |
|---|---|---|---|---|

Fig 1. TPI Packet format

| Attack identifier | Failure Path ID |
|---|---|

Fig 2. PFI Packet format

Initially the TPI packets are broadcasted over all paths in route cache. Each TPI packet contains the ID of the path over which it is broadcasted. This broadcasting guaranties that destination has obtained total number of all node disjoint paths obtained during route discovery, between source and destination, over which it is supposed to get TPI packets. Now destination keeps track of the Path IDs reported by received TPI packets. If any TPI control packet is lost or received after timeout value mentioned in TPI Packet, in middle of its

path, then corresponding ID for the path will not be reported to the destination, or reported with delay which means that the path over which that TPI packet is suppose to arrive, has dropped or delayed it. It immediately sends PFI packet over the primary path, back to source containing the ID of failure paths and attack identifier. Thus the source will avoid failure paths for data transmission and triggers the Behavior Check mechanism over failure paths, one by one. Behavior check mechanism will check each node in the path to trace culprit node and to point out the reasons behind the misbehavior and will inform source about the culprit node if any. This process is summarized in steps as follows:

Step 1) Route Discovery for Node-Disjoint Path Set.

Step 2) Broadcast TPI packets over all paths in route cache.

Step 3) Destination checks for missing or delayed TPI packets and the ID of their paths.

Step 4) Sends PFI packet back to source containing the ID of failure paths and attack identifier.

Step 5) Source will avoid failure paths and triggers Behavior Check mechanism over failure paths, detect misbehaving nodes, and checks whether the node is really misbehaving or it is dropping or delaying packets due to some other reasons like congestion, transmitted power level, collision, and buffer overflow. If it is really misbehaving with ill intention and not because of congestion, transmitted power level, collision, and buffer overflow, then only the node is declared as 'misbehaving node', otherwise not.

## 2.2 Removal of Misbehaving Nodes

Behavior check mechanism will point out packet dropper/delaying node and will inform source. Source will remove path from route cache and will put misbehaving node in the blacklist maintained at source. Those blacklisted nodes are avoided in next route discovery. By doing this, we eliminate future threats imposed by misbehaving nodes. Now the route cache has reliable paths. But it is also possible that any node in the reliable path may starts misbehaving at any point of time. In such cases, source won't be getting acknowledgement (ACK) for dropped packet within RTO. Here source will point out missing/delayed packet path from routing table, stops further data transmission over the same, redirect the traffic over next available shortest backup path and triggers Behavior Checking mechanism over failure path so as to check this path for misbehaving reasons and to blacklist the misbehaving nodes if any. The packet that was dropped over this failure path is retransmitted over new path which was recently selected for data transmission so as to avoid packet loss. This process is summarized in steps as follows:

Step 1) Source will remove failure path informed by PFI packet, from route cache, blacklisting misbehaving nodes and will exclude those in next route discovery.

Step 2) If node in reliable path starts misbehaving in the middle, then source won't be getting its ACK within RTO. Source will check its RT table, point's outs missing packet path and triggers Behavior Checking mechanism over it and once the misbehaving node is detected, it is added in blacklist.

Step 3) The missing packet is sent over another reliable shortest path chosen for further data transmission.

## 2.3 Network Optimization

There may be packet dropping because of several reasons like Congestion, transmitted power level, collision, and buffer overflow, because of which even though the node is not misbehaving intentionally still it is declared as packet dropping/delaying node and this leads to false detection. Due to false detection, reliable nodes are ignored and thus may degrade the overall performance of the system. Our module 1 avoids this degradation due to false detection.

Secondly, the paths are getting checked at the beginning of the data transmission by dispersing TPI packets and then data packets are sent over it. Thus, there is no need to employ reputation base system for checking reliability of paths .This avoids computational complexity, reduces control overhead, minimizes consumption of processing power, and eliminates excessive latency. This process is summarized in steps as follows:

Step 1) Avoidance of False Detection: False detection due to congestion, transmitted power level, collision, buffer overflow is avoided. Hence it gives chance of reintroduction into the network to those loyal nodes which are not currently able to forward the packets due to network layer factors.

Step 2) Avoidance of Reputation Based System: This decreases computational complexity and reduces processing power, delay etc.

Step 3) Promiscuous overhearing avoidance: Robustness increases and control overhead decreases.

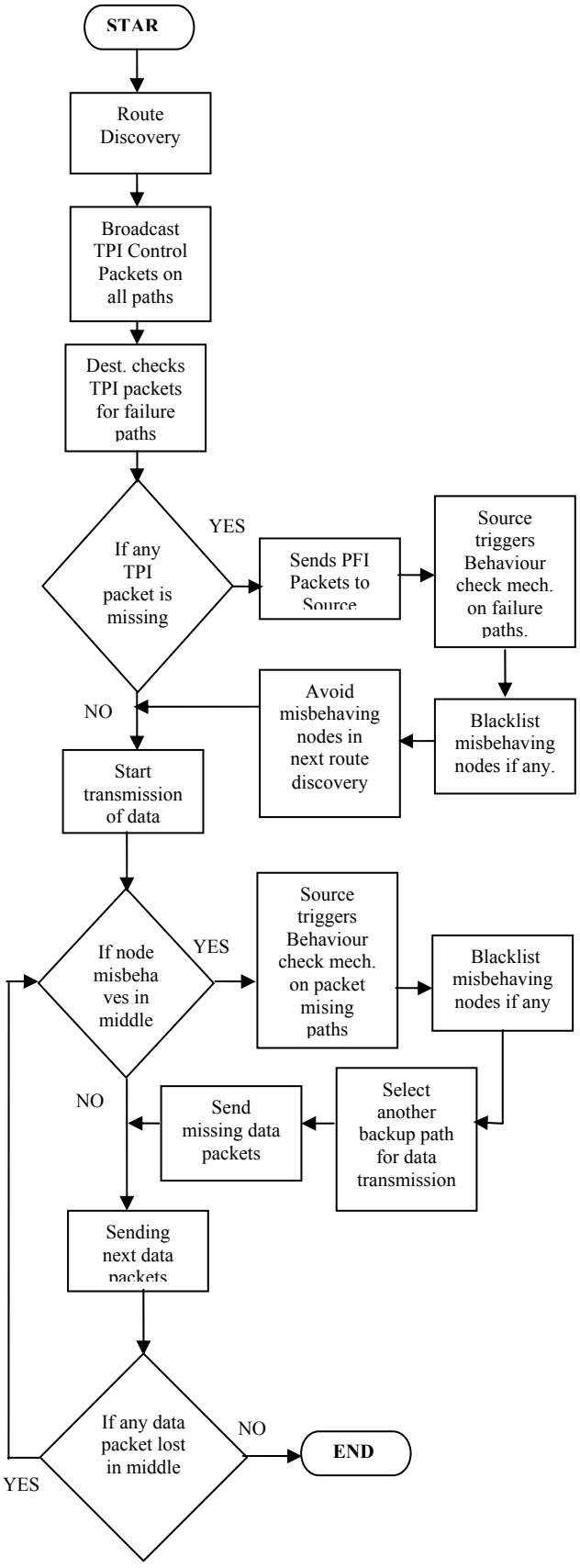


Fig. 3: Proposed Approach Flowchart

## 3. Conclusion

In this paper, a novel multi path routing scheme is proposed that facilitates the identification and removal of misbehaving nodes in mobile ad hoc network (MANET). This mechanism is implemented in conjunction with AOMDV (ad hoc on demand multi path distance vector routing protocol).A concept of pilot engine in railways is imitated here i.e. checking the path before actual data transfer and hence packet loss is kept minimum. It also avoids the implementation of reputation based mechanism, unnecessary promiscuous overhearing and false detection. Hence it helps in reducing data traffic, control overhead, processing power consumption, and computational complexity, latency. Minimizing all above factors yields better network optimization in terms of average packet delivery ratio, average end to end delay, network throughput and overhead transmission. Future work includes implementation of encryption and authentication mechanism so as to deal with packet altering misbehaviour.

## 4. References


[1] Sintayehu Dehnie and Stefano Tomasin "Detection of Selfish Nodes in Networks Using CoopMAC Protocol with ARQ", IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, VOL. 9, NO. 7, JULY 2010.

[2] Fahad T. Bin Muhaya , Fazl-e-Hadi, AtifNaseer "Selfish Node Detection in Wireless Mesh Networks", International Conference on Networking and Information Technology 2010.

[3] Mrs.Sujata V.Mallapur, Prof. Sujata .Terdal "Enhanced Ad-Hoc on Demand Multipath Distance Vector Routing Potocol (EAOMDV)", (IJCSIS) International Journal of Computer Science and Information Security, Vol. 07 No. 03 March 2010.

[4] Soufiene Djahel, Farid Nait-abdesselam, and Zonghua Zhang," Mitigating Packet Dropping Problem in Mobile AdHoc Networks: Proposals and Challenges", IEEE COMMUNICATIONS SURVEYS & TUTORIALS, ACCEPTED FOR PUBLICATION, IEEE 2010.

[5] Sintayehu Dehnie, Stefano Tomasin , Reza Ghanadan, "Sequential Detection ofMisbehaving Nodes in Cooperative Networks with HARQ", 2009 IEEE .

[6] Nastooh Taheri Javan, Reza Kiaeifar, Bahram Hakhamaneshi, Mehdi Dehghan," ZD-AOMDV: A New Routing Algorithm for Mobile Ad-Hoc Networks", 2009 Eigth IEEE/ACIS International Conference on Computer and Information Science.

[7] Wenjia Li, Anupam Joshi, and Tim Finin," Policy-based Malicious Peer Detection in Ad Hoc Networks ",2009 International Conference on Computational Science and Engineering .

[8] Dinesh Mishra, Yogendra Kumar Jain, Sudhir Agrawal," Behavior Analysis of Malicious Node in the Different Routing Algorithms in Mobile Ad Hoc Network (MANET).", 2009 International Conference on Advances in Computing, Control, and Telecommunication Technologies.

[9] Dhanalakshmi Somasundaram and Dr. Rajaram Marimuthu, "A Multipath Reliable Routing for Detection and Isolation of Malicious Nodes in MANET", 2008 International Conference on Computing, Communication and Networking (ICCCN 2008).

[10] A. Dadhich, Dr. A. K. Sarje, Dr. (Mrs.) K. Garg ," Distributed Cooperative Approach to improve detection and removal of misbehaving MANET Nodes", IEEE 2008.

[11] Jyotirmoy Karjee, Sudipta Banerjee," Tracing the Abnormal Behavior of Malicious Nodes in MANET", IEEE 2008.