A Novel, Secure and Reliable Routing Scheme to Alleviate Bad Nodes in Mobile Ad Hoc Networks

Ms.Mitali Ingle[1], Mr. R. S. Thakur[2], Mr. D. S. Gawande[3]

[1]*Assistant Professor Dept. of CSE, D.B.A.C.E.R.,Nagpur.*
[2]*Assistant Professor Dept. of CSE, D.B.A.C.E.R.,Nagpur*
[3]Assistant Professor Dept. of CSE, D.B.A.C.E.R.,Nagpur

ABSTRACT

In a MANET, Node misbehavior is any such behaviour that proves harmful to co-operative environment of MANET. Many schemes have been recently proposed for the detection and avoidance of misbehavior nodes, but these suffer from many problems like false detection due to network layer factors, receiver collision, power controlled misbehavior and collusion. To mitigate this problem of routing layer misbehavior, various existing misbehavior detection schemes have been analyzed and a novel routing scheme is proposed herewith that aims at finding secure and reliable paths for data packets before transmitting them over the same. Since paths are verified for security and reliability at the beginning of data transmission, hence probability of packet loss misbehavior is minimum. In the proposed multi path routing scheme, two types of control packets viz. TPI and PFI control packets are used to detect and avoid misbehaving nodes. Here, false detection due to congestion, transmitted power level, collision, and buffer overflow is avoided. Also it eliminates reliability index mechanism, unnecessary promiscuous overhearing, and redundancy. Hence network throughput is optimized in terms of reliability, security, processor and energy consumption as well as end to end delay.

Keyword: - *Co-operative multi hop forwarding capability, receiver collision, path efficiency, 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. There

are two types of routing protocols: Proactive routing protocol and Reactive routing protocol.

Proactive routing protocol: It stores and maintains route to destination by periodically updating with the help of control overhead.

Reactive routing protocol: In this type, route computation is made only when it is needed.

One of the biggest challenges in ad-hoc networking is the efficient delivery of data packets from source to destination especially in the situation where each device in a MANET is free to move independently in any direction with any speed, and will therefore frequently changing its links to other devices and breaking current paths. Hence, due to the wireless and distributed nature of MANETS, routing in ad-hoc networks can be viewed as a challenge. In such dynamic network, it is important to get route in time, perform the routing that gives maximal throughput with minimal control overhead since control messages consume both channel bandwidth as well as the battery power of nodes for Communication/processing.

Mobile ad hoc networks are a wireless network in which paths between sources to destination are formed on ad hoc basis and each intermediate node in the path has to act as router and forward packets between source and destination. 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 to save its resources. Such selfish behavior 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.

There are two main security issues with ad hoc networks [17]. The first is the need for privacy of communication in network where communication transmission is being performed by nodes owned by many different people/organizations. The other is that the network is vulnerable to a number of attacks (not necessarily deliberately) that can degrade the performance of the network or give unfair advantage to some of the participants. Due to lack of preexisting infrastructure, it is easier for attackers to enter or leave network, perform eavesdropping and gain access to confidential information since no physical connection is needed for it. Hence to mitigate attacks, cryptographic tools such as authentication, key distribution, digital signatures, hashing and encryption techniques can be used to achieve service availability, integrity, confidentiality, proper authentication, and non-repudiation of communication in mobile ad hoc networks. As there can be no online certification authority or trusted third party and hence security concerns are more complicated in MANETS as compare to conventional networks. The other main issue is that the functions of the network are provided by the user devices themselves rather than an independent network operator [17]. It means there is no governing body that can compel nodes to co-operate each other. Also the user devices can be programmed like mobile phones, hence they can be easily made to behave in any desirable way. In future, ill minded users may program there own devices to achieve desirable ill effects.

A. Misbehaviour of Nodes

Misbehavior of Node is any such behavior that goes in total conflict of cooperative working environment of an ad hoc network. A misbehavior threat can be defined as an unauthorized behavior 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 [17]. Nodes will misbehave if controlled or programmed to do so by their owners or users with distinct dimensions of misbehavior as follows [15]:

a) Accidental or deliberate.

b) Selfish or malicious.

c) Individual or collusion.

Hence if we can identify and avoid misbehaving nodes 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 misbehavior

B. Organization:

The rest of the paper is organized as follows: Section 2 describes the related work. Section 3 describes proposed work. Section 4 concludes this paper and outlines the future work. Section 5 points out references.

2. RELATED WORK

Security in MANET has been an active research area. Many solutions for detection and avoidance of misbehaving nodes have been suggested in the literature.A Distributed Cooperative Approach [15] is proposed to improve

detection and removal of misbehaving MANET Nodes in which issue of misbehaving nodes is addressed by providing a distributed cooperative system, in which every node participates in identifying the misbehaving node. Every node exchanges its monitored information both cooperative as well as non-cooperative and giving chance of node's reintroduction into the network in case of false detection. Multi path Reliable Routing (MRR) algorithm [14] determines reliable paths based on node reliability index parameter and adds redundancy in transmitted data to reduce data loss.Enhanced Ad-Hoc on Demand Multi path Distance Vector Routing Protocol (EAOMDV) [4] was proposed to address route failure problem in AOMDV by pre-emptively predicting the link failure by the signal power received by the receiver. Policy-based Malicious Peer Detection in Ad Hoc Networks [9] is scheme in which context information, such as communication channel status, buffer status, and transmission power level, is collected and then used to determine whether the misbehaviour is likely a result of malicious activity or not. Efficient Monitoring Mechanisms for Cooperative Storage in Mobile Ad-Hoc Network [6] is one approach that considers MANET's various constraints and overcome the limitations of the existing monitors. ZD-AOMDV protocol is new routing algorithm [8] that modifies the AODV protocol which results in selection of zone-disjoint paths, to the extent feasible, to achieve less end to end delay. Sequential Detection of Misbehaving Nodes in Cooperative Networks with HARQ [7] was suggested which is based on Sequential Probability Ratio Test (SPRT) for cooperative networks using automatic repeat request (ARQ). Detection of Selfish Nodes in Networks Using CoopMAC Protocol with ARQ [1] is based on the uniformly most powerful (UMP) test or on the sequential probability ratio test (SPRT). The two techniques are characterized and compared in terms of their average detection delay and resulting network performance.In various misbehaving node detection and avoidance mechanisms, there is promiscuous overhearing, false detection, reliability index mechanism and redundancy in transmitted data. These not only consume considerable amount of bandwidth but also battery and processor power and lowers down networks overall throughput. So if these can be avoided, then that may improve the network performance considerably.

3. 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 /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.

A. Detection of Misbehaving Nodes:

In this module, the first step is the route discovery so as to obtain the set of node disjoint paths. Here two types of control packets viz. TPI (Total path information) Packet and PFI (Path failure information) Packet. TPI packet is used to convey information like Data transmission path information, including the path length and nodes along the path, Timeout value, Source ID and cryptographic key. PFI Packet conveys information about alert identifier and failure path lengths and nodes along them. To identify misbehaving paths, destination has destination path table which is shown in figure 1.

Source ID	RTO value	Data Info.	Routes Info.	Key

fig.1: Destination path table

Initially the TPI packets are broadcasted with an effective dispersion algorithm. This broadcasting guaranties that destination has obtained information about all node disjoint paths obtained during route discovery, between source

and destination since every TPI packet contains this information. Now the destination will check whether any TPI control packet is lost in middle of its path. If any of the TPI packet is missing, then it means that the path over which that TPI packet is suppose to arrive, has dropped or delayed it. It immediately sends PFI packet back to source containing the information of failure path. Thus the source will avoid failure path and triggers Watchdog over failure path. Watchdog will point out packet dropper node and will inform source. This process is summarized in steps as follows:

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

Step 2) Broadcast TPI packets with Dispersion Algorithm.

Step 3) Destination checks for missing control packets and their paths.

Step 4) Sends PFI packet back to source containing the information of failure paths.

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

B. Removal of Misbehaving Nodes:

Watchdog will point out packet dropper node and will inform source. Source will remove path from route cache and will avoid misbehaving node in next route discovery. 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 its acknowledgement (ACK) within retransmission time out (RTO). Here source will checks its RT table, points out missing packet path and triggers watchdog over it so as to remove this path from the route cache. The packet that was sent over this failure path is retransmitted over some another shortest reliable path so as to avoid packet loss. Since only missing packets are retransmitted, hence no need to add redundancy in transmitted information. This process is summarized in steps as follows:

Step 1) Source will remove failure path informed by FPI packet, from route cache.

Step 2) Source maintains black list of misbehaving nodes and will exclude those in next route discovery.

Step 3) If node in reliable path starts misbehaving in the middle, then source won't be getting its ACK within RTO.

Step 4) Source will check its RT table, point's outs missing packet path and triggers watchdog over it and once the misbehaving node is detected, it is added in blacklist and step 2 will be executed.

Step 5) The missing packet is sent over another reliable shortest path chosen from route cache.

C. Network Optimization:

There may be packet dropping because of several reasons like Congestion, transmitted power level, collision, and buffer overflow. Hence even though the node is not misbehaving still it is declared as packet dropping 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 we are checking the paths at the beginning of the data transmission by dispersing TPI packets and then sending packets over it. Thus, there is no need to give reliability index to every node. This avoids computational complexity since it reduces control overhead, minimizes consumption of processing power, and eliminates excessive latency. Since we do not employ reputation based system and hence promiscuous overhearing is needed only when

packet dropper node is found which hence prominently reduces control overhead. 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 able to forward the packets due to network layer factors.

Step 2) Avoidance of Reliability index mechanism: Since it increases computational complexity, takes processing power and induces delay, hence it is avoided.

Step 3) Redundancy Avoidance: Only sending missing packets, thus reducing flooding and avoiding congestion.

Step 4) Promiscuous overhearing and reputation based system avoidance: Robustness increases and control overhead decreases.

4. CONCLUSION

In this paper, a novel secure and reliable multi path routing mechanism is proposed that enhances the identification and removal of misbehaving nodes in mobile ad hoc network (MANET). This mechanism is implemented 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. Above stated mechanism also avoids the implementation of reliability index mechanism, unnecessary promiscuous overhearing and reputation based system, redundancy in transmitted data. Hence it helps in reducing data traffic, control overhead, processing power, and computational complexity, latency, flooding. 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 misbehavior and simulation in different environments

5. 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] S. R. Biradar,Koushik Majumder, Subir Kumar Sarkar," Performance Evaluation and Comparison of AODV and AOMDV", S.R.Biradar et al. / (IJCSE) International Journal on Computer Science and Engineering , Vol. 02, No. 02, 2010, 373-377.

[4] 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 .

[5] 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.

[6] Mustapha Reda Senouci, Abdelouahid Derhab, Nadjib Badache ," EfficientMonitoring Mechanisms for Cooperative Storage in Mobile Ad-Hoc Networks: Detection Time and Accuracy Tradeoffs", 2009 29th IEEE International Conference on Distributed Computing Systems Workshops.

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

[8] 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.

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

[10] Wei Gong, Zhiyang You,, Danning Chen, Xibin Zhao, Ming Gu, Kwok-Yan Lam," Trust Based Malicious Nodes Detection in MANET", IEEE 2009.

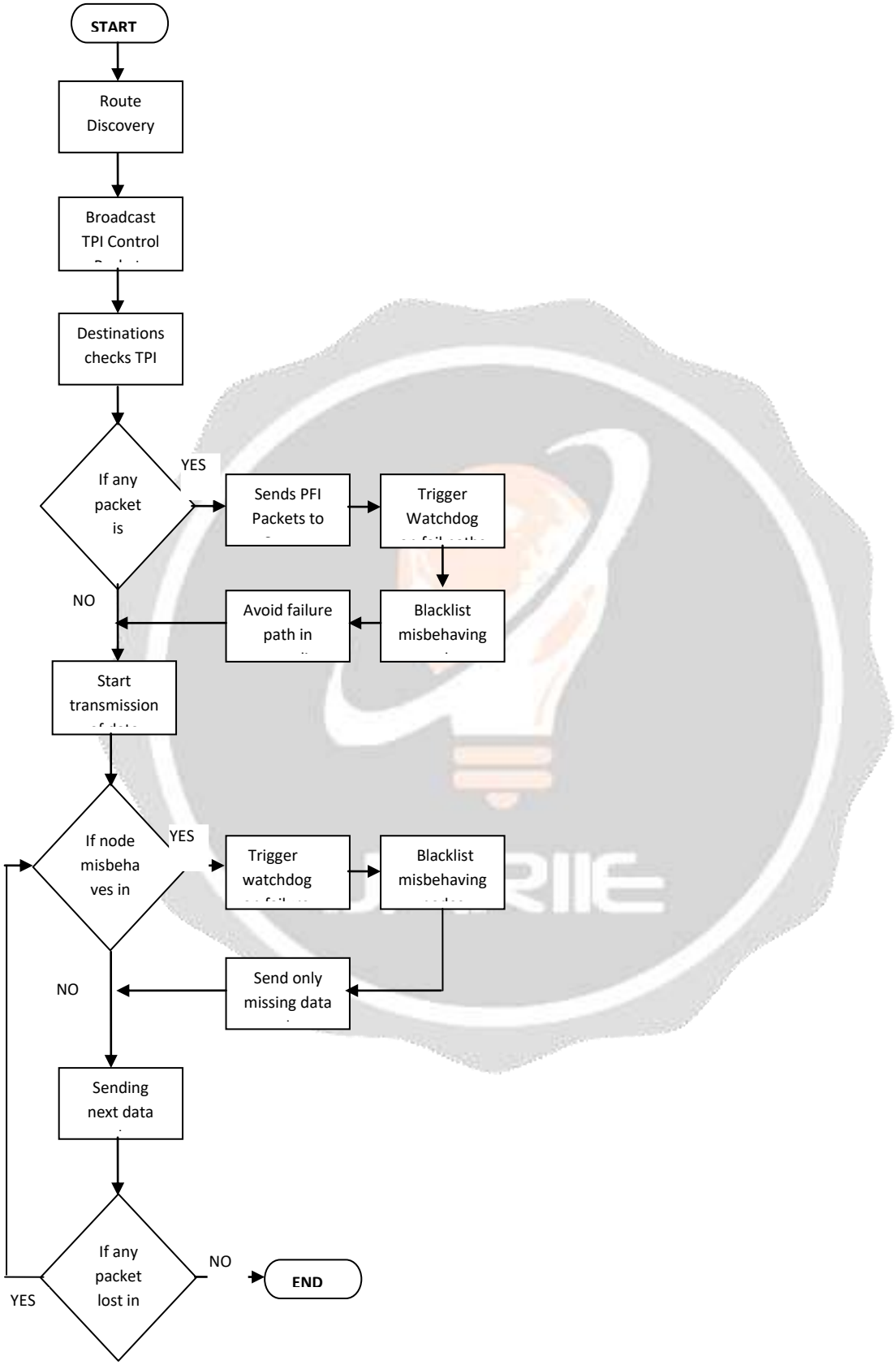

fig.2: Flowchart of proposed scheme