International Journal of Applied Engineering Research ISSN 0973-4562 Volume 13, Number 15 (2018) pp. 12084-12088
© Research India Publications. http://www.ripublication.com

Detection of Misbehaving Node in MANET using Aggressive Routing Scheme

Mr. Raja[1] and Dr. J. Thirumaran[2]

[1]Research Scholar, Department of Computer Science, Rathinam College of Arts and Science, Coimbatore, Tamil Nadu, India.
[2]Professor, Department of Computer Science, Rathinam College of Arts and Science, Coimbatore, Tamil Nadu, India.

Abstract

An Ad hoc network is a set of mobile nodes that generates a temporary network without the help of centralized management or fixed support devices that are usually available as regular networks. These terminals typically have a limited transponder limit, so each terminal helps in carrying packets of its neighbors, so the temporary network terminals operate as routers and hosts. Topology can be changed in a adhoc network due to the movement of nodes. When creating new connections in the ankles, some links are broken when one or more limits on the nodes are moved.

The logic logically contradicts the lack of possessions to safeguard their attributes in order not to interfere carefully. To ensure secure routing a technique is required to disappoint misbehaviour and conserve the collaboration in the network. The proposed scheme employs a Distributed aggressive model at each node for augmenting the security of the network. Accompanying information concerning misbehaviour in the network is moderately disseminated between the nodes during route establishment and it is used as a warning step to ensure safe ways. The offered outline considers the real world scenario where a node may demonstration dissimilar kinds of misbehaviour at different times. Thus, it provides an aggressive resolution construction technique to deal with nodes presenting fluctuating misbehaviours in accordance to their severity.

Keywords: MANET, Node Misbehave, Routing, Aggressive, Detection.

MANET – AN INTRODUCTION

A Ad hoc network is a set of mobile nodes, which generate a temporary network without the help of centralized administration or standard support devices that are usually available as regular networks. These terminals typically have a limited transponder limit, so each terminal helps in carrying packets of its neighbors, so the temporary network terminals operate as routers and hosts. This allows one node to carry packets between other edges, as well as run user applications. Networks do not have standard conditions in these categories by nature or are suitable for situations where the network can not be deployed. Advertising has been found in various sectors such as military, emergency, conferences and sensor networks. Each of these application areas have their specific requirements for ethical guidelines.

Since network nodes are mobile, an ad hoc network usually has a dynamic topology, which can have profound effects on network attributes. Network nodes are often run by the battery, which controls the CPU, memory, and bandwidth. This will require resource open network operations. Also, wireless (radio) media affects network behavior, resulting in relatively high error rates resulting in fluctuations.

These unique desirable features offer many new challenges in the design of wireless ad hoc networking protocols. Network functions such as routing, addressing, recognition and recognition should be designed to deal with a dynamic and dynamic network topology. It is more than a hip to set up paths between the ends, and well-built routing protocols.

The distinctive feature of these protocols is the ability to detect pathways, despite a dynamic topology. In simple situations, the edges can communicate directly with each other, for example, when they are on the wireless transmission range of each other. However, ad hoc networks are connected to terminal connections only from a series of wireless hops from other ends.

Features of Mobile Ad-Hoc Network

Mobile ad hoc networks have the following features-

- Autonomous terminal.
- Distributed function.
- Multihop routing.
- Dynamic Network Topology.
- Connection capacity changes.
- Light weight terminals.

In MANET, each mobile terminal is a auto-leading, which acts as a host and a router. The central control of the network function is no longer a background network and is distributed across the network's control and management terminals.

The basic types of ad hoc routing algorithms are based on single-hop and multihop, different link layer attributes and steering protocols. The simplest of single-hop manet multihop is the low cost and compatibility of the process, based on the structure and function.

Since the nodes are mobile, network analysis will change quickly and unexpectedly, and the connection on the terminals varies by time. MANET should change according to the traffic and surface conditions and the mobility of mobile network ends.

Mobile nodes on the network stop being redirected within themselves when they are operating, and fly their own network.

Wireless Connection the higher bit-error rates are deep in a MANET. An endless endpoint will be shared by several sessions. Any channel that communicates with terminals is subject to noise, fading and interference, and has a lower bandwidth than the wired network.

In most cases, MANET nodes are mobile devices with low CPU processing capacity, small memory size and low power storage. These devices require optimal algorithms and mechanisms that implement computer and functional functions.

Challenges of Mobile Ad-Hoc Network

In the past few years, advertising hoc networking is a popular step. Every aspect of the network is examined in a variety of issues, in one way or another. However, no final decision is reached or at least agreed to any problems. On the contrary, more questions arise. The issues to be resolved are as follows:

- Scalability
- Routing
- Quality of service
- Client server model shift
- Security
- Energy conservation
- Node cooperation
- Interoperation

The above approach to tackling features is recommended and possible upgrade solutions are discussed. In today's survey work, "rounding" has been reviewed for the appropriate protocol to suit the network's changing situation.

PROTOCOL – ANALYSIS

An algorithm security threat analysis has a systematic mechanism for analyzing security vulnerabilities in a given protocol and community environment.

Possible analysis is carried out in three lead lines. Within the first stage, the implementation of the algorithm is analyzed to spread the malicious information and look at the orientation of each type of steering message. At the second level, causal relationships among exclusive attack behaviours and the extents of disruption prompted are derived for all viable community conditions. in the end, based totally at the observations of the previous degree, contents of every kind of routing message inside the protocol are assessed for protection threat. We are able to use the famous DSR protocol to demonstrate the security analysis technique.

DSR Fundamentals

Dynamic Source Routing (DSR) is an optimized version of traditional connection state protocols such as OSPF. It uses the concept of multifunction relays (MPRs) to effectively disseminate link status updates across the network. Only the end of the selected MPRs by some node is allowed to create connection status updates. Furthermore, link status updates only contain connections between MPR nodes and their MPR-selectors. Thus, each analysis is available only in partial analysis information. However, this information is enough to calculate the short hip path to each other, as there are at least one MPR nodes in that path.

DSR only uses timely updates for connection status. Overall, when the total overhead is determined by the number of edges that make up updates, the number of leads for each update and the amount of each development, the higher the lower the comparison of the DSR base connection state protocol than the network. For the microcomputer network, the DSR distorts the traditional connection state protocol. Finally, the use of occasional updates, selecting a refresh gap, face topology changes.

PROBLEM STATEMENT

A self-paced node does not perform packet sharing functionality for unrelated data packets. However, the DSR protocol runs in Route Discovery and Route Maintenance Phases. These incorrect behavioral modes may be included in the chosen ways to advance data packets from the source, as they are part of the root discovery stage. Invalid behavioral methods refuse to carry out data packets from the source. This causes confusion.

In guarantee services such as TCP, the source code can either choose an alternative route from its path or start a new way of detection. The alternate route has the wrong behavior, and the data exchange may fail again. The new path innovation phase returns through similar routes, including misconduct methods. In the end, the source term may decide that no way to provide data packets is available.

As a result, although the network is not a source of reliable communication sources, these routes are available. In the best efforts like UDP, the field simply sends data packets to the next hip point, which goes forward. On the way there is the existence of wrong friendship and the flow of data traffic will be reduced. This cannot be supported without proof.

MISBEHAVING BODES MODEL

Routing protocols provide two main functions: the way function and data-sending function. The former guides were involved in the discovery and maintenance of pathways. The latter is related to the relaying data packets towards the target via the installed path. Routing and data transmission can be affected by the presence of both ends; misleading the contradictions does not lead to the wrong actions of the network and activates the padlets forward.

We consider two types of misconceptions: self nodes and malicious ends.

Selfish Nodes

Automatic edges attempt to save their own resources because resources on wireless devices are highly controlled. So self-nodes may have their source in carrying data packets to other rings: it can be achieved in two ways:

- *Selfish node1: -*
  The directional routes take part in routing functions, but not the predecessor of other packet data packets; So data packets can be dropped instead of being sent to their destination.

- *Selfish node type2: -*
  These nodes do not take correctly in the steady process by guiding guidelines, for example: in DSR selfish node may drop all RREQ they received or not forward a RREP to some destination. As a result, this self-promotion does not participate in the requested ways.

Misbehave Nodes

Unlike self-serving nodes, the malicious edges do not protect their evidence, but they try to participate in all the ends and ruin the other ends. As a result, other terminals may use a "dangerous" route under their control in malicious fronts. The malicious terminology depends on the maneuvers. In the context of the DSR routing protocol, a malicious term is said to have a way to some locations and to respond to the received RREQ with incorrect information. After being selected on the requested path, the dose can be attacked by dropping all the packets in the Black Hole attack, or selecting gray hole assault packets.

PROPOSED METHODOLOGY

The proposed architecture is given below, and it consists of three phases.

Initial Phase

It is the beginning module of the proposed methodology. The first rule, referred as Mobility Prediction (MP), uses a simple mobility prediction scheme to estimate when the location information broadcast in the previous beacon becomes inaccurate. The next beacon is broadcast only if the predicted error in the location estimate is greater than a certain threshold, thus tuning the update frequency to the dynamism inherent in the node's motion. (ODL), aims at improving the accuracy of the topology along the routing paths between the communicating nodes.

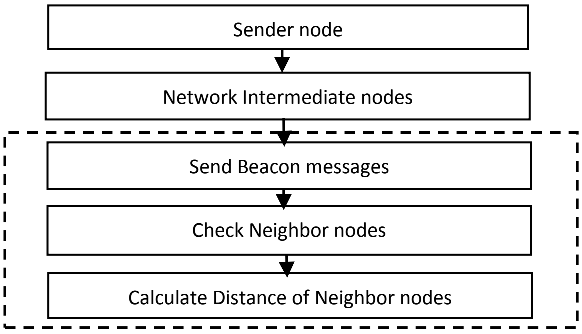
Sender node
Network Intermediate nodes
Send Beacon messages
Check Neighbor nodes
Calculate Distance of Neighbor nodes

Figure 1: Initial Phase

Distributed Aggressive Model

In this paper, a new type of node, with suspicious node, cooperative terminals and selfish initiatives, will carry some suspicious picks to encourage them to cooperate properly after further investigations. They are aware of the use of a state model to determine what to do in each state. Except for a period of time restricting the reputation, a period of time is introduced to each state.

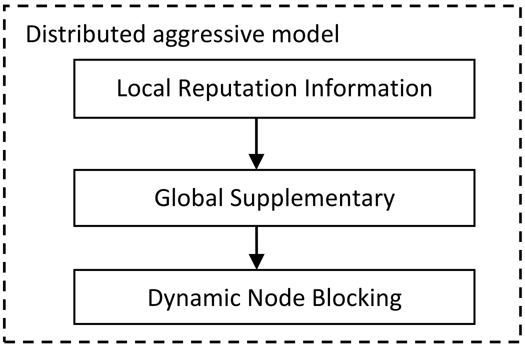

Figure 2: Distributed Aggressive Model

Decisive Routing

In wireless multi-network network, since it is the nature of wireless multi-network networks, recursive notes on nodes have the same interface as it came. It again makes every retransmit, a packet from each unbalanced neighbour's home and actually packet

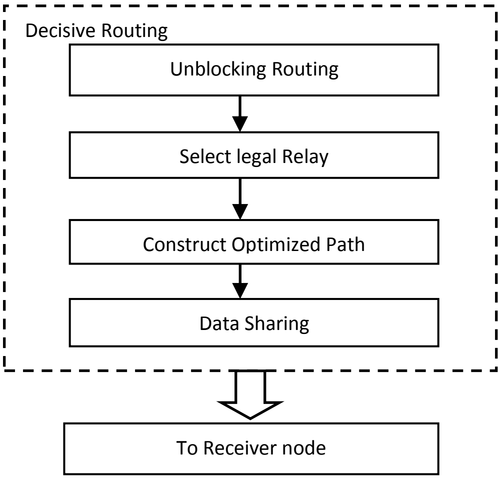

Figure 3: Decisive Routing

The key concept used in the protocol is that of multipoint relays (MPRs). MPRs are selected nodes which forward broadcast messages during the flooding process. This technique substantially reduces the message overhead as compared to a classical flooding mechanism, where every node retransmits each message when it receives the first copy of the message. Thus, a second optimization is adjacency selection by use smart peering selection to improve the routing efficiency. This paper also proposes other optimization such as link set, link state declaration and topology reduction. Except for these optimizations, this paper put forward substantial elements of the protocol and MANET interface type.

RESULTS & DISCUSSIONS

The detailed simulation model is based on network simulator-2 (ver-2.31), is used in the evaluation. The NS instructions can be used to define the topology structure of the network and the motion mode of the nodes, to configure the service source and the receiver to create the statistical data trace file and so on. Performance metrics are calculated from trace file (.tr) that has contained the all simulation information.

The simulation is done using ns-2, to analyze the performance of the network by varying the nodes mobility. The evaluated performances are given below. Note down selfish nodes are consider one in case of attack to visualized the effect of attack but after applying misbehaviour node scheme consider the selfish nodes to see the secure effect of misbehaving node in network.

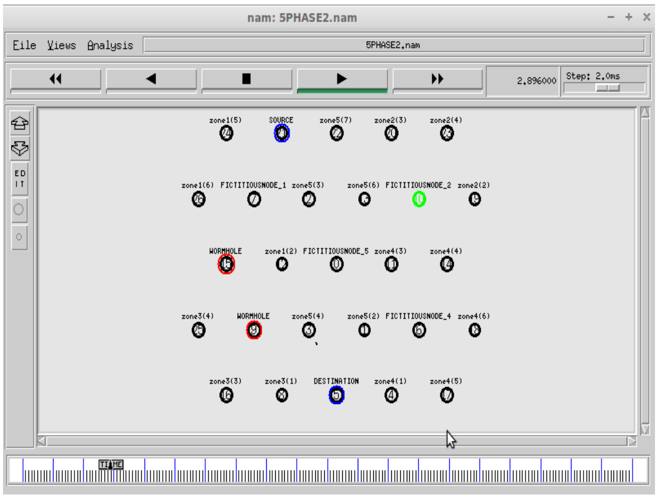

Figure 4: Node Detection

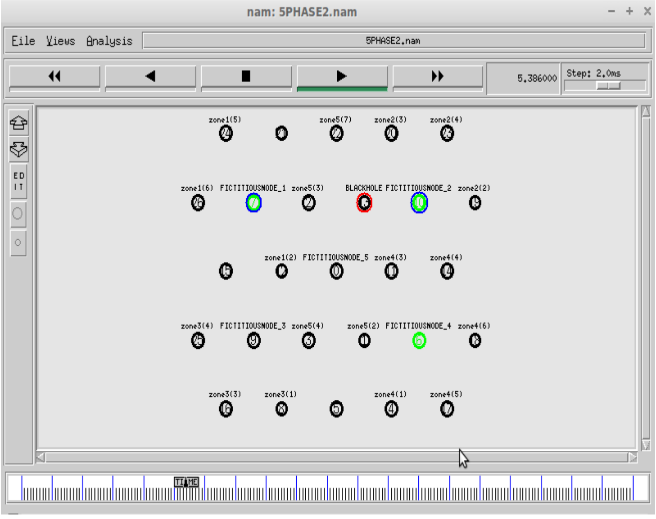

Figure 5: Misbehave Node

In this paper we focus on evaluating the protocols under Selfish node or malicious nodes attack and measure the network performance after applying intrusion detection system with following criteria

The performance evaluation metrics considered were:

Packet Delivery Ratio (PDR): = Total number of packets received / Total number of packets sent X 100 Average

End to End Delay: = Summation (time received – time sent)/number of packets The summation is over all received packets

Throughput (kbps): = Summation (received size)/(stop time – start time) X (8/1000).

Where stop time is stop time of packet sending and start time is start time of packet sending. Factor of (8/1000) is used to convert to kbps.

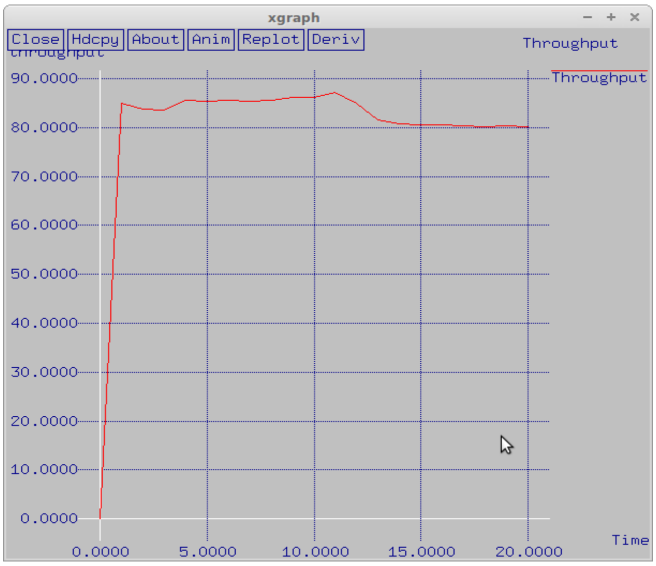

Figure 6: Throughput

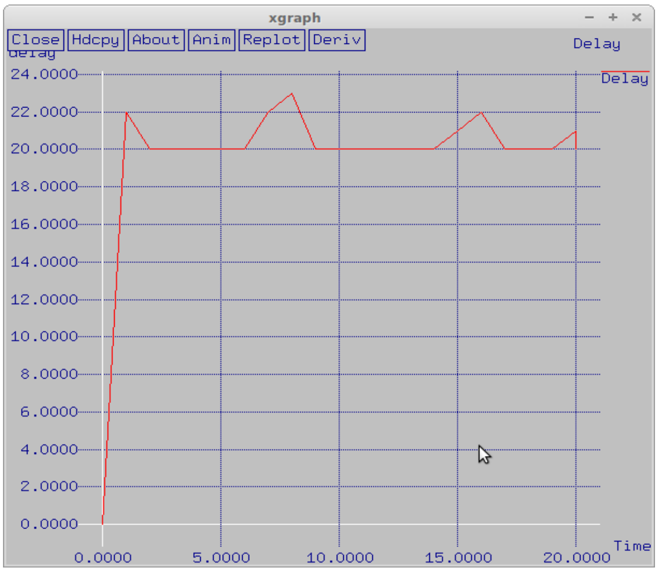

Figure 7: Delay Rate

This work has provided a study of MANET misbehaving node detection in combination with different mobility models for varying network areas.

CONCLUSION

In this work, we proposed a new routing scheme designated for MANETs. The motivation for our work is to develop an Routing scheme that is able to detect misbehaving node in case of collision, limited transmission power and false misbehaviour report. We demonstrated the performance of our proposed scheme through an evaluation in the network simulator environment. The results showed that the proposed scheme is effective in detecting misbehaving nodes in MANETs. Although the simulation result showed that our proposed scheme outputs higher throughput, it also has a lower delay with the increase of malicious nodes in the network. This makes our proposed scheme a better choice in the security sensitive environment than other schemes we have investigated.

REFERENCES

[1] Bing Wu, Jianmin Chen, Jie Wu, Mihaela Cardei (Department of Computer Science and Engineering) Florida Atlantic University, “A Survey on Attacks and Countermeasures in Mobile Ad Hoc Networks”, 2006 Springer.

[2] G.S. Mamatha and Dr. S.C. Sharma, “Network Layer Attacks and Defense Mechanisms in MANETS- A Survey”, International Journal of Computer Applications, Volume 9, No.9, November 2010, pp. 12-17.

[3] T.V.P.Sundararajan, Dr.A.Shanmugam, “Performance Analysis of Selfish Node Aware Routing Protocol for Mobile Ad Hoc Networks”, ICGST-CNIR Journal, Volume 9, Issue 1, July 2009.

[4] Anita Yadav, Y. N. Singh, R. R. Singh, Improving Routing Performance in AODV with Link Prediction in Mobile Adhoc Networks, Wireless Pers Commun, DOI 10.1007/s11277-015-2411-5, published online, 2015.

[5] P. C. Reddy, New Routing Metrics for ADHOC Network Routing Protocols, J. Inst. Eng. India Ser. B, DOI 10.1007/s40031-014-0116-x, 2014.

[6] Haitham Y. Adarbah, Shakeel Ahmad, Bassel Arafeh, and Alistair Duffy, Efficient Broadcasting for Route Discovery in Mobile Ad-hoc Networks, SummerSim-SPECTS, 2015, July 26-29, 2015, Chicago, IL, USA.

[7] J. Liu, X. Jiang and S. Member, Throughput Capacity of MANETs with Power Control and Packet Redundancy, IEEE Trans. Wirel. Commun., vol. 12, no. 6, pp. 3035–3047, 2013.

[8] Hawa M., Taifour S., Qasem M., Tu_aha W. A, dynamic cross-layer routing protocol for mobile ad hoc networks, International Journal of Electronics and Communications (AEU), 2012.

[9] Ahmed Al-hamadani, William H. Allen, RAAODV: a Reputation-Aware AODV for Mobile Ad hoc Networks, ACM SE ’14 March 28-29, 2014 Kennesaw, GA USA. Detection of Misbehaving Node using Secure Acknowledgement in MANET Rasika R. Mali and Sudhir T. Bagade, *2016 International Conference on Computing, Analytics and Security Trends (CAST), Dec 19-21, 2016.*

[10] M. Patel “Detection of malicious attack in MANET a behavioral approach” IEEE International Conference on Advance Computing Conference, 2013, pp. 388 – 393.

[11] Jian-Ming Chang, Po-Chun Tsou, Isaac Woungang, Han-Chieh Chao, and Chin-Feng Lai “Defending Against Collaborative Attacks by Malicious Nodes in MANETs: Cooperative Bait Detection Approach”, IEEE Conf. Malicious Attacks on 2015, pp 65-75.

[12] Baadache, Abderrahmane, and Ali Belmehdi. "Fighting against packet dropping misbehavior in multi-hop wireless ad hoc networks." Journal of Network and Computer Applications 35, no. 3 (2012): 1130-1139.

[13] Muthumalathi, N., and M. Mohamed Raseen. "Fully selfish node detection, deletion and secure replica allocation over MANET." In Current Trends in Engineering and Technology (ICCTET), 2013 International Conference on, pp. 413-415. IEEE, 2013.

[14] Rodriguez-Mayol, Alberto, and Javier Gozalvez. "Reputation based selfishness prevention techniques for mobile ad-hoc networks." Telecommunication Systems 57, no. 2 (2014): 181-195.

[15] Kumar, Jebakumar MSP Josh, Ayyaswamy Kathirvel, Namaskaram Kirubakaran, Perumal Sivaraman, and Muthusamy Subramaniam. "A unified approach for detecting and eliminating selfish nodes in MANETs using TBUT." EURASIP Journal on Wireless Communications and Networking 2015, no. 1 (2015): 143.

[16] Shao, Baohua. "Performance of Ad Hoc on Demand Distance Vector Routing Protocol." In 2010 International Conference of Information Science and Management Engineering, pp. 420-421. IEEE, 2010.