DETECTION OF MISBEHAVING NODES IN WIRELESS ADHOC NETWORKS

Patan Mohammad Muzammil¹, T. J. Naga Lakshmi²
UG Student¹
Assistant Professor²
Department of Electronics
and Communication Engineering,
Saveetha School of Engineering, Chennai
muzu786143@gmail.com
t.j.nagalakshmi@gmail.com

June 25, 2018

Abstract

Now a days the communication is playing a major role in every one’s life. This has become the basic need to all kind of works that are taking place. But the way of communication is also playing a vital role in the current situations. As of the previous days the wired communication has been the most common one but now a days the most common way of communication has shifted to the wireless communication instead of the wired one. This has developed to such extent such that the data transmission is also taking place via wireless networks. This has made the need for security and safety to the networks which are used to make all these data transmissions. This security needs to be in such a way that there should be no data manipulation in any form by the nodes present in the specified network. In this paper
we are representing the way of node misbehavior which took place in the wireless ad hoc networks

Keywords: Ad hoc Networks, MANET, AODV, Watch Dog, Network Simulator.

1 INTRODUCTION

Wireless ad hoc networks are also called as the Mobile ad hoc networks (MANET). These networks which are independent type of networks which doesn’t have any administered network controller. These will configure themselves and are called as the self-configuring type of networks. These networks are most common type of networks now a days since from the development of mobile phone. These networks will have the intermediate devices which are capable of receive and transmit data from one to other. These devices are called as the nodes in the network. These nodes are the vital part of the wireless ad hoc networks. These nodes should have the capacity of self-configuration. Since these are free to move in any direction from one place to another place and are capable of changing to the other network base due to the capacity of self-configuration. Other than MANET there are several other type of networks which come under the category of ad hoc networks. Some of them are Vehicular ad hoc network, FANET, Smart phone ad hoc network and so on. These ad hoc networks are very convenient way of the network for the data transmission and it is as efficient as the wired technology. Since it is easy to setup and the maintenance to setup and look after is very low when compared to the wired LAN networks. This makes it the very suitable network type which can be spread to at any extent of the world. This network will use the air as a propagation medium. That too the infrastructure for this type of network is very less compare to the wired network. This popularity has made this network to be the most common network type to have the intrusions, malwares and node misbehaviors and so on. Due to these reasons the wireless ad hoc networks has become the most vulnerable and sometimes unsecure. To get these problems rectified in the effective way one should need to detect the source and gateway of the problem where the problem has arisen. Unless the detection of the source of the problem we cant able to rectify
these vulnerabilities. Since the major content of the wireless ad hoc networks are nodes, so the main aim of our work is to get the node detected which is misbehaving in the network. To get this work done one should use the different kind of available protocols which help to detect those misbehaving nodes. Misbehaving of the node includes the slow transmission of the data packets, heavy throughput, sending the data to the other nodes instead of the neighbor node, packet drop or packet loss and so on.

1.1 Elaboration

Most of the scholars has proposed many kind of methods to detect these misbehaving nodes in the ad hoc networks. These methods are having the different kind of protocols which are most popular with their efficient way of detections. These includes the DSR which stands for dynamic source routing protocol, DSDV which stands for Destination Sequenced Distance Vector Routing protocol, 2ACK (acknowledgement) protocol, EAACK which stands for Enhanced Adaptive Acknowledgement Protocol, AODV which stands for Ad hoc On Demand Distance Vector routing protocol. These protocols are used to find the misbehaving nodes in the ad hoc network most efficiently.

1.2 Methodology

1.2.1 AODV

Ad hoc On Demand distance Vector routing protocol is one of the routing protocols which are most popular to its efficiency and adaptability. This protocol is mainly developed by the University American State California, university of Santa Barbara and university of Cincinnati along with the co-operation of Nokia research Centre. This protocol has many combination of applications with different methods which is due to its easy way of usage, adaptability with other resources. This protocol will stand a part in the efficiency when compare with the other protocols. Ad Hoc On-Demand Distance Vector, a routing protocol for ad hoc mobile networks with large numbers of mobile nodes. The algorithm of the protocol will create the path between nodes only
when the routes are as per the request of the source nodes which provides the network the flexibleness which makes the nodes to enter and leave the network.

An ad hoc routing protocol is a protocol that controls how nodes decide which way to route packets between computing devices in a mobile ad hoc network. In ad hoc networks, nodes will not able to understand the topology which is designed for their networks. Instead, they have to discover it typically, a new node announces its presence and listens for announcements from the neighbors.

1.2.2 Watch Dog

The Watch dog is the method of detection for the misbehavior node detection in the wireless ad hoc network. It is the method in which the nodes in the networks will individually behave as the watch dogs. This is an independent way of approach but interlinked with each other node in the network. Through this method the network containing all nodes will have that much number of watch dogs which are capable of continuous surveillance on other nodes. This helps in the detection of misbehaving nodes. If a node has been misbehaving by any means the neighboring node which is acting as a watch dog will inform about this misbehaving node to the other neighboring nodes. This way the watch dog scheme will work along.

1.2.3 Network Simulator

The whole process for the misbehaving node detection will be carried on the network simulator tool for the real time observation of the procedures. This is the simulation tool which will allow the users to create the nodes, creating the network by accumulation the nodes, making the nodes to send or receive the packets, applying the desired routing protocols which we want to use for the routing of data in the network and so on. This makes the network simulator the most popular tool for the simulation of the network related real time observations. There are nearly three versions of the network simulator of which the network simulator 2 is the most popular one.
1.2.4 Problem
Mobile ad-hoc networks (MANETs) are contains of nodes which are connected wirelessly without using any pre-existent infrastructure. MANET nodes rely on network cooperation schemes to properly work, forwarding traffic unrelated to its own use. However, in the real world, most nodes may have a selfish behavior, being unwilling to forward packets for others in order to save resources. Therefore, detecting these nodes is needed for network performance. Watchdogs are used to detect selfish nodes in ad hoc networks which will reduce the time usage and is most effective way of approach.

1.2.5 Implementation
The implementation of the project is done on the basis of the network simulator.
- Linux CentOS 6.5/ Ubuntu 14.04
- NS2
- OTCL
- NAM
- X-Graph
- Trace Graph
- C++
- AWK
2 BLOCK DIAGRAM

2.1 Method

This paper proposes a watchdog based method alongside of the AODV algorithm which makes the effective way for the detection of selfish nodes. The dependence of the routing in ad hoc networks relies on the basis of node behavior. In order to support multihop operation in the network, most ad hoc routing algorithms assume well-behaving nodes. However, in reality there may exist constrained, selfish or malicious nodes.
2.2 TCL Script

The name TCL is defined as the Tool Command Language. TCL is a radically simple open-source interpreted programming language that provides common facilities such as variables, procedures, and control structures as well as many useful features that are not found in any other major language. Node configuration consists of the different node characteristics before creating them. They might consist of the type of addressing structure used in the simulation. After the node creation the implementation of the protocol is done in the network simulator alongside of the watch dog method. This is done with the help of the tool command language script which helps to implement these in the network simulator tool. The complete implementation of the process will results the misbehavior node detection in the simulator and it can be shown in the network animator tool.

3 RESULTS

Initial Nodes
4 ADVANTAGES

This method will be very easiest method for the implementation. This uses the low cost for the implementation and the energy usage for the whole setup to run is also low compared with others.

5 CONCLUSION

Thus with the help of the AODV protocol alongside of the watchdog method of detection of misbehaving node, we conclude that this method is the most efficient way for the detection of misbehaving nodes in the wireless ad hoc networks or mobile ad hoc networks. This method will approach directly by using the watchdog scheme by collaborating with the other nodes which is most effective and easy way. Thus there will be the possibilities to overcome the misbehavior of the nodes in the network which we can prevent them from the data manipulation and other harmful, unsecured consequences occurs in the network.

References

of Misbehaving Nodes Using an Enhanced Acknowledgment Based Intrusion Detection Technique in MANETs


