© 2016 IJSRSET | Volume 2 | Issue 1 | Print ISSN : 2395-1990 | Online ISSN : 2394-4099
Themed Section: Engineering and Technology

Detection and Prevention of Selfish Nodes in Mobile Adhoc Networks

Avni Verma*, Prof. Nitin Tiwari

Computer Science and Engineering Department, Gyan Ganga College of Technology, Jabalpur, Madhya Pradesh, India

ABSTRACT

A MANET is a remote system in which hubs can go about as sender/collector or even as delegates prefer switches. Hubs in a MANET may act up with an aim to preserve assets. This happens due to restricted assets accessible for every hub. This causes an incredible effect on the whole system execution. In this paper we examine about MANET as zones and groups with a Static Agent as a focal hub and a Zonal Agent for every zone. It is a change over Mobile Agent based building design which is made conceivable in light of the fact that by presenting Zonal Agents. In this way, the framework has the capacity distinguish Selfish and Malicious Nodes with lessened measure of data trade between the hubs furthermore talk about the approaches for better after-effects of self-cantered hubs and grouping approaches for hub classification.

Keywords: MANET, Misbehaviour, Zonal Agent, Misbehaving Nodes

I. INTRODUCTION

Portable Ad Hoc Networks (MANETs) is the most pertinent range of examination predominantly as a result of the different difficulties that it postures to the current conventions and architectures. Existing architectures and conventions are lacking to guarantee the administrations required by a MANET. Versatile Ad-Hoc systems are remote, framework less, self-arranging, self-sufficient systems. Hubs can work as sender/beneficiary or even as a switch [1]. This diminishes the requirement for extra framework for sending information parcels and performing directing capacities.

The correspondence between these portable/static hubs happen through remote connections. They may speak straightforwardly with one another or by Utilizing different hubs as switches. All the hubs in the system are allowed to move bringing about unusual changes to the system topology. This represents a gigantic test before the system overseers. All system exercises, for example, finding the topology and conveying information parcels, must be executed by the hubs themselves, either independently or all things considered. Contingent upon its application, the structure of a MANET may change from a little, static system that is exceptionally power-compelled to an extensive scale, portable, profoundly element system [2]. Therefore, Monitoring of a MANET occasionally empowers to recognize any bottlenecks in the system which may hamper the system execution or may bring about disavowal of administration to the current hubs. In this paper, we propose a novel framework to identify Selfish and Malicious hubs in a MANET. The framework depends on a voting based system to distinguish a possibly acting mischievously hub and after that utilizing the versatile specialists to recognize a conceivably getting out of misbehaving node as either selfish or a malicious node.

II. METHODS AND MATERIAL

A. Analysis of Approaches For Selfish Nodes

AODV Routing in MANET

Broadly MANET use two types of routing proactive and reactive, in this section we are going to discuss well known reactive routing protocol called AODV [6]. AODV is a reactive routing protocol [6] designed for

mobile ad hoc networks. Unicast, multicast and broadcast proclamation are applied in AODV method. AODV is federation of mutually DSR and DSDV. It adopts the basic on demand method of Route Discovery and Route preservation from DSR and the use of hop by hop steering sequence number and sporadic beacons from DSDV [7] is an on demand routing protocol, AODV only wishes to conserve the routing information about the active paths. In AODV, steering information is maintained in routing tables at nodes. Every mobile node maintains a next-hop routing table, which restrain the destinations to which it currently has a path. A routing table terminates, if it's not update its entry until reactivation has been in a certain specified time period.

Furthermore, AODV espouses the destination sequence number method used by DSDV in an on-demand technique.

Hello messages can be used to recognize and oversee links to neighbours. If Hello messages are used, all enthusiastic nodes intermittently broadcast a Hello message that all its neighbours amuse. Since nodes intermittently send Hello messages, if a node fails to amuse several Hello messages from a neighbour, a link break is detected.

B. **Flooding and its used in Attack**

Flooding (shown in figure 1) is a requisite message spreading technique for network-wide broadcast within mobile ad hoc networks (MANETs). Topological awareness is not essential for flooding in MANET [8]. Every the routing protocol is based on the on demand routing is established path via the flooding method. While aggressor used this flooding to interrupt the communication it's called flooding attacks.

In MANET Flooding is making use of discover the route from source to destination. But sometime this is severe difficulty for MANET. Some node using this flooding for disturbs the communication between the nodes. This node fire mass of route request message and tries to preserve the resources of the node. Once the resources of the node preserve, they does not give answer of the another node requested message.

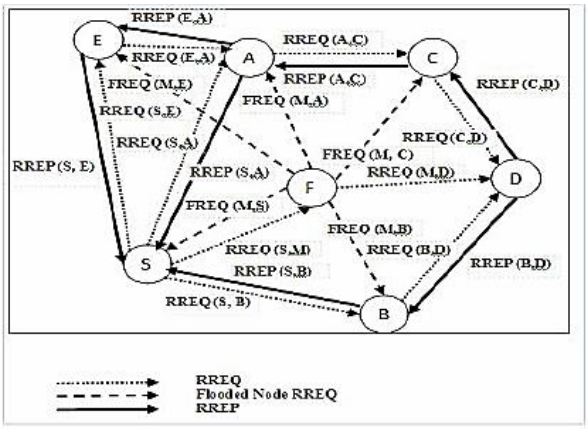

Figure 1: Flooding attack

B. Literature Survey

Author Alokparna Bandyopadhyay, Satyanarayana Vuppala and Prasenjit Choudhury [1] have suggested default value for the RREQ_RATELIMIT is 10 as proposed by RFC 3561. However, a malicious node can override the restriction put by RREQ_RATELIMIT by increasing it or disabling it, thus allowing it to send large number of RREQ packets per second. A node is able to do so because of its self-control over its parameters. This permits it to flood the network with false route requests, leading to a type of DoS attack due to the network-load forced by the false RREQs.

Author Humaira Ehsan and Farrukh Aslam Khan [10] has been suggested evaluation of network performance for AODV especially in terms of packet efficiency, routing overhead, and throughput.

Author Arpita Raverkar [11] has been define three parameter Route discovery, throughput and delay for detection of flooding attack.

Author S. Kannan, T. Kalaikumaran, S. Karthik and V.P. Arunachalam [9] has been used to detect malicious node who floods in the network using RREQ messages, has proposed a statistical approach to avoid the forwarding of such packets via the concept of RREQ counts. Author Abdur Rashid Sangi, Jianwei Liu and Likun Zou [12] has been discuss about attack has been done by the authorize node. Attacks have been initiated by authenticated nodes/devices in Ad Hoc Network to disrupt the network called Byzantine attack. Although these attacks can be initiated independently but are more distressing if start in a mutual way. They highlight the performance degradation of AODV routing protocol, when the Byzantine attack are initiated in a combination.

There are many misbehaviour detection systems [1], [3], [4], [2], [7], [8] proposed by various authors. [1] Uses Mobile Agent (MA) to gather data about the nodes in a cluster and decide whether a link is misbehaving. The system results in large amount of work being done by MA and data transmitted between nodes. It saves the amount of data to be polled to detect misbehaving nodes since MA gets the data from each node locally but the RERR packet being transmitted to each node in all the zones is a big overhead for the centralized Static Agent (SA).

Reference [4] proposes 2 schemes to detect selfish nodes in a MANET namely TWOACK and S-TWOACK. TWOACK sends back a special acknowledgement packet called as TWOACK along the route on which packet has been sent.

TWOACK travels in exactly reverse direction to the original packet. Each node in system computes the number of TWOACK packets received and number of data packets sent, which enables to identify misbehaving links. S-TWOACK is an optimization of TWOACK, since it transmits TWOACK packets only for selected data packets. This reduces the number of acknowledgments being transmitted across the network.

III. RESULTS AND DISCUSSION

NS-3 Network Simulators and Proposed Algorithm

1. Collect all the metrics using NS-3 test bed and save as XML file.
2. Extract XML file using DOM (Dynamic Object Module) and input in SVM.
3. Calculate PDR, CO and PMIR
4. If (PDER>0.9) and ((CO >= 70) and (PMIR > =0.3)
   Node is flooded
   Else
   No-operation

Network Simulator-3 - NS-3 is a discrete-event network simulator in which the implementation of simulation core and models is in C++. NS-3 is built as a library which can either be statically or dynamically linked to a C++ main program that defines the simulation topology and starts the simulator. NS-3 also exports almost its entire API to Python, allowing Python programs to import an "NS-3" module in much similar way as the ns-3 library is linked by executables in C++.

Primary function of NS-3 simulator is to simulate networks of communicating nodes and the traffic among them. To do this, NS-3 offers its primary abstractions of computing nodes by applications to spawn traffic and net devices and channels toward move the traffic. Support Vector Machine (SVM) - In machine learning, support vector machines (SVMs, or support vector networks) are supervised learning models with related learning algorithms that examine data and distinguish patterns, intended for categorization and deterioration analysis. The essential SVM takes a set of input data and predicts, for every given input, which of two feasible classes forms the input. SVM used to classify the node into two groups normal node and malicious node.

IV. CONCLUSION

In this paper investigation over the Mobile Agent Based Architecture and gives various favourable circumstances over other existing frameworks. Since it identifies Selfish and in addition malevolent hubs, it is superior to anything existing frameworks hypothetically. It utilizes less number of messages. Nonetheless, we haven't directed an experimental investigation of the proposed structural engineering however hypothetical writing demonstrates that the quantity of messages being transmitted and the quantity of occasions that happen for identification of acting up hubs is not exactly the Mobile Agent based methodology and we additionally examination the grouping methodologies like SVM for better after effect of arrangement of hubs concerning time.

V. REFERENCES

[1] Alokparna Bandyopadhyay, Satyanarayana Vuppala and Prasenjit Choudhury "A Simulation Analysis of Flooding Attack in MANET using NS-3", Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronics Syst,, Feb. 28 2011-March 3 2011.

[2] Wenjia Li and Anupam Joshi, "Security Issues in Mobile Ad Hoc Networks - A Survey", the 17 Th White House Papers Graduate Research2004 Cite Seer.

[3] Casimir & Roland, "The Performance Of Dynamic Source Routing Protocol For Mobile Ad Hoc Networks", Blekinge Institute of Technology September 2009.

[4] Luis Gironés Quesada, “A Routing Protocol for MANETs”, Norwegian University of Science and Technology, May 2007.
[5] Abedellatif Mohammed Hussein, "Flooding Control in Route Discovery for Reactive Routing in Mobile Ad Hoc Networks”, Kate Gleason College of Engineering Rochester Institute of Technology Rochester, NY May, 2007.
[6] C.E. Perkins, and E.M. Royer, “Ad-hoc On-demand Distance Vector Routing,” in: Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications, New Orleans, LA, February 1999, pp.90-100.
[7] Deepa.S and Dr. D.M Kadhar Nawaz,” A Study on the Behavior of MANET Routing Protocols with Varying Densities and Dynamic Mobility Patterns” IJCA Special Issue on “Mobile Ad-hoc Networks” MANETs, 2010.
[8] Yoav Sasson, David Cavin, and Andre Schiper, ”Probabilistic Broadcast for Flooding in Wireless Mobile Ad hoc Networks” Cite Seer Conference 2002.
[9] S. Kannan, T. Kalaikumaran, S. Karthik and V.P. Arunachalam, “A Review on Attack Prevention Methods in MANET” Journal of Modern Mathematics and Statistics Year: 2011 | Volume: 5 | Issue: 1 | Page No.: 37-42.
[10] Humaira Ehsan and Farrukh Aslam Khan, “Malicious AODV Implementation and Analysis of Routing Attacks in MANETs”, 11th International Conference on Trust, Security and Privacy in Computing and Communications, IEEE, 2012.
[11] Ms. Arpita Raverkar, “Route Discovery in Insecure Mobile Ad hoc Network”, IEEE, 2011 978-1-4244-8679-3/11/.
[12] Abdur Rashid Sangi, Jianwei Liu and Likun Zou, “A Performance Analysis of AODV Routing Protocol under Combined Byzantine Attacks in MANETs”, IEEE, 2009978-1-4244-4507-3/09/.
[13] NS-3 simulator, http://nsnam.org