ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2016

Efficient Detection of Selfish Node Using SVM Learning Technique in Mobile Ad hoc Network

Avni Verma[*1], Nitin Tiwari[2]

M. Tech Research Scholar [Computer Technology and Application], Department of Computer Science and Engineering, Gyan Ganga College of Technology, Jabalpur, Madhya Pradesh, India[*1]

Asst. Professor, Department of Computer Science and Engineering, Gyan Ganga College of Technology, Jabalpur, Madhya Pradesh, India[2]

ABSTRACT: A MANET is a remote framework in which center points can go about as sender/authority or even as representatives favour switches. Center points in a MANET may misbehave with a mean to protect resources. This happens because of limited resources available for each center. This causes an extraordinary impact all in all framework execution. In this paper we inspect about MANET as zones and gatherings with a Static Agent as a central center point and a Zonal Agent for each zone. It is a change over Mobile Agent based building outline which is made possible in light of the way that by exhibiting Zonal Agents. Along these lines, the structure has the limit recognize Selfish and Malicious Nodes with reduced measure of information exchange between the center points moreover discuss the methodologies for better eventual outcomes of self trotted center points and gathering approaches for center point order.

KEYWORDS: MANET, Misbehaviour, Zonal Agent, Misbehaving nodes

I. INTRODUCTION

Portable specially appointed Networks (MANETs) is the most applicable scope of examination overwhelmingly as a consequence of the diverse challenges that it stances to the present traditions and designs. Existing models and traditions are missing to ensure the organizations required by a MANET. Adaptable Ad-Hoc frameworks are remote, structure less, self-masterminding, independent frameworks. Centers can fill in as sender/recipient or even as a switch [1]. This reduces the prerequisite for additional structure for sending data bundles and performing coordinating limits. The correspondence between these portable/static centers happens through remote associations.

They may talk direct with each other or by using diverse centers as switches. Every one of the center points in the framework are permitted to move achieving strange changes to the framework topology. This speaks to a monstrous test before the framework supervisors. All framework works out, for instance, finding the topology and passing on data packages, must be executed by the centers themselves, either autonomously or in light of current circumstances. Dependent upon its application, the structure of a MANET may transform from somewhat, static framework that is uncommonly control constrained to a broad scale, versatile, significantly component framework [2]. In this way, Monitoring of a MANET at times enables to perceive any bottlenecks in the framework which may hamper the framework execution or may realize repudiation of organization to the present center points. In this paper, we propose a novel structure to distinguish Selfish and Malicious center points in a MANET. The structure relies on upon a voting based framework to recognize a potentially acting fiendishly center point and after that using the flexible authorities to perceive a possibly escaping acting up hub as either narrow minded or a noxious hub.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2016

II. ANALYSIS OF APPROACHES FOR SELFISH NODES

A. *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 technique. AODV is alliance of commonly DSR and DSDV. It embraces the essential on interest strategy for Route Discovery and Route conservation from DSR and the utilization of jump by bounce guiding grouping number and sporadic signals from DSDV [7] is an on interest directing convention, AODV just wishes to ration the steering data about the dynamic ways.

In AODV, directing data is kept up in steering tables at hubs. Each versatile hub keeps up a next-bounce steering table, which limit the destinations to which it right now has a way. A directing table ends, in the event that it's not upgrade its entrance until reactivation has been in a specific indicated day and age. Besides, AODV embraces the destination succession number strategy utilized by DSDV as a part of an on-interest procedure. Hi messages can be utilized to perceive and manage connections to neighbors. On the off chance that Hello messages are utilized, every single eager hub irregularly telecast a Hello message that every one of its neighbors delight. Since hubs irregularly send Hello messages, if a hub neglects to interest a few Hello messages from a neighbor, a connection break is recognized.

B. *Flooding and its used in Attack:*

Flooding (appeared in figure 1) is an imperative message spreading system for system wide show inside portable impromptu systems (MANETs). Topological mindfulness is not vital for flooding in MANET [8]. Each the directing convention depends on the on interest steering is built up way by means of the flooding technique. While attacker utilized this flooding to interfere with the correspondence it's called flooding assaults.

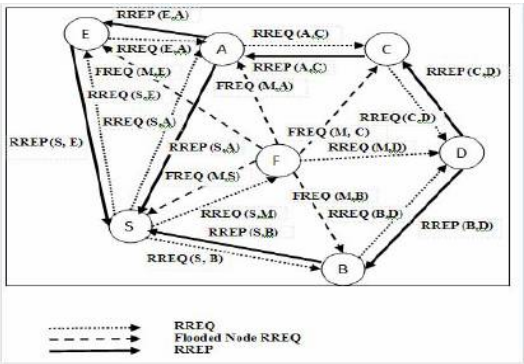

Figure 1: Flooding attack

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.

III. LITERATURE SURVEY

Author Alokparna Bandyopadhyay, Satyanarayana Vuppala and Prasenjit Choudhury [1] have recommended default esteem for the RREQ_RATELIMIT is 10 as proposed by RFC 3561. Notwithstanding, a pernicious hub can supersede the confinement put by RREQ_RATELIMIT by expanding it or handicapping it, in this manner permitting it to send substantial number of RREQ bundles every second. A hub can do as such as a result of its discretion over its parameters. This grants it to surge the system with false course asks for, prompting a kind of DoS assault because of the system load constrained by the false RREQs.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2016

Creator Humaira Ehsan and Farrukh Aslam Khan [10] have been recommended assessment of system execution for AODV particularly as far as bundle proficiency, steering overhead, and throughput. Creator Arpita Raverkar [11] has been characterizing three parameter Route revelation, throughput and postponement for recognition of flooding assault.

Creator S. Kannan, T. Kalaikumaran, S. Karthik and V.P. Arunachalam [9] has been utilized to recognize malevolent hub who surges in the system utilizing RREQ messages, has proposed a factual way to deal with keep away from the sending of such parcels by means of the idea of RREQ tallies. Creator Abdur Rashid Sangi, Jianwei Liu and Likun Zou [12] has been talk about assault has been finished by the approve hub. Assaults have been started by verified hubs/gadgets in Ad Hoc Network to upset the network called byzantine assault. Regardless of the way that these ambushes can be begun uninhibitedly yet are all the additionally alarming if start normally. They highlight the execution corruption of AODV directing convention, when the byzantine assaults are started in a blend.

There are numerous rowdiness location frameworks [1], [3], [4], [2], [7], [8] proposed by different creators. [1] Utilizes Mobile Agent (MA) to assemble information about the hubs in a group and choose whether a connection is getting out of hand. The framework results in substantial measure of work being finished by MA and information transmitted between hubs. It spares the measure of information to be surveyed to distinguish getting into mischief hubs since MA gets the information from every hub locally yet the RERR parcel being transmitted to every hub in every one of the zones is a major overhead for the unified Static Agent (SA). Reference [4] proposes 2 plans to identify egotistical hubs in a MANET specifically TWOACK and S-TWOACK. TWOACK sends back an exceptional affirmation bundle called as TWOACK along the course on which parcel has been sent.

TWOACK goes in precisely turn around heading to the first parcel. Every hub in turn figures the quantity of TWOACK parcels got and number of information bundles sent, which empowers to recognize getting out of hand connections. S-TWOACK is an advancement of TWOACK, since it transmits TWOACK parcels just for chose information bundles. This diminishes the quantity of affirmations being transmitted over the system.

IV. RESULTS AND DISCUSSION

NS-3 NETWORK SIMULATORS AND PROPOSED ALGORITHM

Step 1: Collect all the metrics using NS-3 test bed and save as XML file.
Step 2: Extract XML file using DOM (Dynamic Object Module) and input in SVM.
Step 3: Calculate PDR, CO and PMIR
Step 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-occasion system test system in which the execution of re-enactment center and models is in C++. NS-3 is worked as a library which can either be statically or powerfully connected to a C++ fundamental program that characterizes the recreation topology and begins the test system. NS-3 likewise sends out just about its whole API to Python, permitting Python projects to import a "NS-3" module in much comparable route as the ns-3 library is connected by executables in C++.

Essential capacity of NS-3 test system is to re-enact systems of imparting hubs and the movement among them. To do this, NS-3 offers its essential deliberations of figuring hubs by applications to produce activity and net gadgets and channels toward move the activity. Bolster Vector Machine (SVM) - In machine learning, bolster vector machines (SVMs, or bolster vector systems) are regulated learning models with related learning calculations that inspect information and recognize designs, expected for classification and weakening examination. The crucial SVM takes an arrangement of information and predicts, for each given information, which of two practical classes shapes the info. SVM used to order the hub into two gatherings typical hub and malignant hub.

COMPARISON TABLE: If more misroute packets are detected then more processing power required which indicates more PMIR using mobile agent approach and if we classified nodes using SVM then we can identified and classified nodes which use less processing power and less PMIR as shown in Table 1.

And figure 2 in which X axis represent number of nodes and Y axis represent PMIR and this indicate PMIR ratio by nodes with SVM and Mobile agent approach.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2016

Mobile node	PMIR Ratio	
	With SVM	With MOBILE AGENT approach(Base Paper)
15	22	30
30	25	32
45	28	34
60	30	37
75	32	40
90	34	42

Table: 1

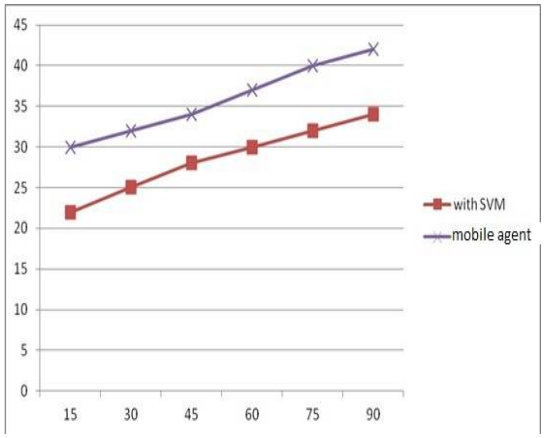

Fig 2: Comparison Graph

Table 2 indicates the number of parameter used by base paper and our approach for increasing lifetime and improving QOS parameter for Mobile ad hoc network using AODV.

Parameters	PDR	CO	PMIR	DELAY	Classification Technique	Routing
Base Paper	No	No	No	No	No	Agent based
Our approach	Yes	Yes	Yes	Yes	Yes (SVM)	AODV

Table: 2

V. CONCLUSION

In this paper examination over the Mobile Agent Based Architecture and gives different good circumstances over other existing systems. Since it distinguishes Selfish and moreover malignant center points, it is better than anything existing structures speculatively. It uses less number of messages.

In any case, we haven't coordinated a trial examination of the proposed basic designing however speculative written work exhibits that the amount of messages being transmitted and the amount of events that happen for recognizable proof of misbehaving center points is not precisely the Mobile Agent based procedure and we furthermore examination the gathering philosophies like SVM for better eventual outcome of course of action of centers concerning time.

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 17th White House Papers Graduate Research2004 CiteSeer.
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 2th IEEE Workshop on Mobile Computing Systems and Applications, New Orleans, LA, February 1999, pp.90-100.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2016

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" CiteSeer 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/

BIOGRAPHY

Avni Verma is a Master of Technology research scholar in Computer Technology and Application stream, Gyan Ganga College of Technology, Jabalpur, Madhya Pradesh, India.

Nitin Tiwari is an Asst. Professor in Computer Science and Engineering department, Gyan Ganga College of Technology, Jabalpur, Madhya Pradesh, India.