APPLIED FUZZY HEURISTICS FOR GREEDY NODE DETECTION IN VANETs

**MR.X** **Mrs.R.VENITTA RAJ**

**M.ANUPRIYA,P.POOJA,K.DHIVYABARATHI**

**Abstract-The  Vehicular Ad hoc Network(VANETs) has a greater significance in Vehicle to Vehicle Communication without relaying much on the Infrastructure.Though they are used in variety of applications they are vulnerable to attacks.In this proposed approach we have to detect greedy nodes  by incorporating various various metrics like Number of times the node makes an Attempt, Connection Duration , Waiting time, Packet Delivery Ratio and Average Delay. These metrics are used by the benign nodes to learn more about malicious node behavior.In order to detect greedy nodes our proposed model has two phases namely Uncertainty  State and Resolution State .The Uncertainty  State is based on linear regression concept and Resolution state is based on Fuzzy Logic Scheme.The effectiveness of our approach is proved by extensive simulations. This proposed work can be applicable for variety of applications as they provide high level of trustworthiness by detecting greedy nodes in the network**.

**1.INTRODUCTION:**The main use of Mobile Network in VANETs is in adhoc mode.The algorithm work is to detect greedy node and safeguard the life of the passengers from the attacks[1].compare to VANETs,MANETS have less constraint.

The VANETs proposal ensures privacy for the driver and his vehicle wheather he is tramitter or receiver of the message.By handling vehicular behaviour during traffic,we ensure a safe and secure traffic management.In the proposed model we define a three newly defined metrices

A mobile ad hoc network is a collection of two or more nodes equipeed with Wireless communications and networking capabilities without central network control,which may be referred to as an infrastructure-less mobile network.

Vehicular Ad-hoc Networks(VANETs)represent a rapidly emerging,particularly challenging class of Mobile Ad Hoc Networks(MANETs).VANETs are distributed,self organing communication networks bulit up by moving vehicles,and thus characterized by very high node mobility and limited degrees of freedom in the mobility patterns.

In ad hoc networks all nodes are mobile and can be connected dynamically in an arbitrary manner.As the range of each host’s Wireless transmission is limited,so a host needs to enlist the aid of its nearby hosts in forwarding packets to the destination if it wants to communicate with the hosts outside its transmission range.so the nodes of the networks behave as routers and take part in route discovery and maintence of routers to other nodes in the network.

In[2] the attack against VANETs are of availability,integrity etc.availability of attacks are of denial of service (DoS)attack[3].A DoS attack occurs when a multiple system orchestrate a synchronized Dos attack to a single target.Dos attacks are generally used against are generally against large corporations,government sites to distrupt their web prescence.In vanets the dection of DoS is little difficult.The greedy node job is to reduce the faster time of the channels and to disturbs the other honest node.The greedy node is that disobedience that is not to work with the honest node.

The performance of MAC layer be affected in the manner of the backoff value.The contention window of the subrange be specified by receiver to sender through CTS/ACK packet.the contention window is easy to detect misbehaving nodes. The RTS/CTS(Request to send/clear to send)is the mechanishm for wireless network protocol to reduce the collision by the hidden node problem. The Distributed short range communication(DSRC) is open source protocol for wireless communication.the featured of DSRC is of high secure and high speed and is of wireless communication between vehicles and infrastructure.The DSRC is classified into 7 channels of 10 MHZ:one CCH channel (Control channel)and six SCH channel(service channel) .VANETs introduced WAVE(Wireless access in vehicular environments).this WAVE includes the data exchange between high-speed vehicles and between the vehicles and the roadside infrastructure is relied on the band of 5.9 GHz(5.85-5.925 GHz).WAVE is required to support the Intelligent Transportation System(ITS) in short range application.

The contention based method called Enhanced Distributed Channel Access(EDCA) is considered as mandatory mode for Medium Access Control(MAC).EDCA features such as Arbitration Inter –Frame Space(AIFS)and contention window for different access categories(AC) .four categories are classified according to the type of traffic:Background traffic(BK),Best Effort Traffic(BE),Video traffic(VI),Voice traffic(vo).

Time=15us,SIFS=32us represent the Short Inter Frame Space for IEEE 802.11.

CCH SCH

AC CWmin CWmax CWmin CWmax

BK min max min max

BE (min+1)/2 min min max

VI (min+1/4)-1 min+1/2 min+1/2 min

VO (min+1/4)-1 min+1/2 (min+1/4)-1 min+1/2

Min=15 Max =511

The EDCA uses access channel method as CSMA/CA(Carrier Sense Multiple Access with collision Avoidence.The backoff procedure follows the backoff value[0,CW] equal to initial value CWmin,if the CW fails to reaches CWmax then the CW increases,when channel is idle the backoff value reduced,the node send immedieately it the value reaches zero.

=\*time (1)

Different AIFSN(arbitration inter frame space number)are been selected on the basis of access categories for use with CCH and SCH for control and service channels.the detection of greedy node be understand on the basis of CWmax,CWmin and AIFSN values.

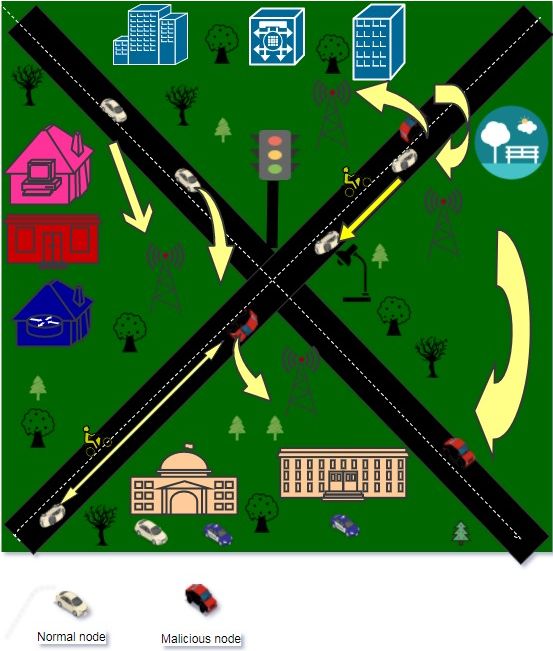
**2.MANET ARCHITECTURE AND CHARACTERISTICS:**

**1.Dynamic topologies:**

In MANET nodes are free to move readily,thus network topoly which it act as a multihop may change suddenly at unpredictable times,and consist of both bidirectional and unidirectional links.

**2.Bandwidth**-constrained,variable capacity links:

Wireless links have significantly lower capacity than hardwired counterparts.one effect of the relatively low to moderate link capacities is that congestion is typically the norm rather than expectation.



**3.Energy-constrained operation:**

The nodes in a MANET may rely on batteries or other exhaustible means for their energy.The most important system design criteria for optimization may be energy conservation for these nodes.

**4.Limited physical security:**

Mobile Wireless networks are generally more prone to physical security threats than the infrastructure based networks.The increased possibility of eavesdropping,spoofing and denial-of-service attacks shoud be considered.This provides the decentralized nature of network control in MANETs to be robust against the single points of the failure of more centralized approaches.

**3.RELATED WORK:**

The problem in this paper are we have to detect the dos attacks,MAC layer misbehaviour and also to detect the greedy behaviour .The approaches mainly focus on the VANETs on the IEEE802.11 protocol.In that we have proposed foe Mac greedy behaviour detection in Wireless Mesh Networks(WMNs.There be classified as Three series

* Mac Design Solutions:To reduce Back off algorithm weekness a new Mac layer is introduced to detect the greedy attacks.
* Monitoring solutions:Without modification of the MAC layer an extra component is added to detect greedy attacks.
* Game theory solutions:the detection of greedy attacks be based on the game theory approach.

DOMINO was Proposed by Raya et al.[6](System for greedy behaviour in the MAC layer of IEEE 802.11 public Networks).DOMINO can detect and identify greedy attacks without any modification of the access point.It can detect some manipulation techniques such as CTS and ACK delay and reduction of Backoff time.

Confident was proposed by Buchegger and Le Boudec it is been mainly used in Mobile ad-hoc networks and it works properly on the participating nodes cooperate in routing and forwarding.CONFIDENT for making misbehaviour unattractive to deny cooperation.

login attempts,connection duration,connection waiting time

Djahel et al prosed a FLASC(fuzzy logic based scheme to struggle adaptive cheaters).The main objective of FLASC is to detect greddy nodes which aim to violate proper use of CSMA/CA protocol.

In VANETs regular changes in private communication pseudonyms are important to avoid illegal tracking of vehicles and to ensure anonymity.Pseudonym change protocol based on the detection of trusted neighbours.This protocol triggers the pseudonym change in several vehicles at the same time ,a solution that improves vehicles anonymity.

The security protocol based on the dyanamic change of pseudonyms for privacy in Vehicular Ad hoc networks(VANETs).The privacy for the driver and his vehicles wheather he is transmitter or receiver of the messages.

**3 PROPOSED DETECTION ALGORITHM**

**3.1 Algorithm Overview**

The watchdog software determines the responsible for greedy behaviour detection for three defined metrices. we have queue length,throughtput,packet delivary ratio.

Calculate slope of regression of straight line

Close to 1

Coefficient calculation

Collection of traces

Close to 1

Greedy behaviour suspicion

No greedy behaviour

Greedy determination(yes/no)

These metrices are responsible for low mobility networks.In VANETs there is no enough time to perform the detection of greedy behaviour backoff parameters.the number of connection attempts,connection duration and waiting time are supervised.so that in this project is combines linear regression and Watch dog concepts for the VANETs.The decision scheme uses strength of design tools by the fuzzy logic to determine either greedy or it is honest.

**Unsavoury State :**In **Unsavoury State** phase,we determining whether our network contains any greedy node or not .In 802.11p architecture, if the first node communicate with other node,next node will be wait till first node break its transmission. Now first create the number of node in network with fixed coordinates.Then generate the trace file. Using this coordinates find the correlation coefficient.Why we calculate the correlation means a number between +1 and -1 calculated so as to represent the linear interdependence of two variables or set of data. If correlation coefficient is nearer to 1 means we must calculate slope of linear regression line .If slope also nearer to 1 means greedy node is not present in this network.Otherwise greedy is may or may not be present.So that finding the exact result we use watchdog tool.

**Algorithm 1. Greedy Unsavoury State :**

**INPUT** :Greedy=false. **OUTPUT**:Network contains Greedy or not **begin** **repeat** 1)Collect coordinates of nodes 2)Calculate the coefficient P  **if** P is nearer to 1 **then** execute step 3. **Else** execute step 4. 3)Calculate slope **if** the slope is nearer to 1Greedy=false; **Else** execute step 4. 4)Greedy is Suspected .run watchdog tool  **until** No communication; **end**

**Resolution State:**

In this state,we using the fuzzy concept for finding the existence of greedy node.For each parameter we start to find the behavior of the node as Greedy,Suspected,Normal using the threshold value.Before doing that we should know about fuzzy concept. In our software tool monitoring the three parameter. 1)Number of Connection Attempt 2)Average of Connection Duration 3)Average of waiting time.

**Fuzzy Concept:**

In fuzzy concept,it contains the 3 phase. 1)Fuzzification(using membership function). 2)Rule Generation(Application of fuzzy rule) 3)Defuzzification(Obtaining the crisp or actual values).

**Fuzzification:**

Here,we use three parameter which is monitor by the watchdog tool as linguistic variable.For each value of linguistic variable,we fix its membership to one of the following fuzzy sets “low”,”high”,”medium”.Output of the membership should be between -1 and +1.

**Description of the Parameter**

**Parameter**  **Description**

n No:of node C No:of Connection attempt at t. C Connection duration during t. C1 low threshold value of connection attempt. C2 high threshold value of connection attempt . C1 low threshold value of connection duration. C2 high threshold value of conncetion duration. C1 high threshold value of waiting time. C2 low threshold value of waiting time

**Rule Generation:**

Here,For each parameter we generate the rule using the threshold value. :low threshold value.if node exceeds this value,node is suspected. **** high threshold value.if node exceeds this value,node is greedy. :low threshold value.if node exceeds this value,node is suspected. :high threshold value.if node exceeds this value,node is greedy. low threshold vaue.if node being this value,node is greedy.:high threshold value.if node being this value,node is suspected. L1🡪Number of connection attempts L2🡪Connection duration L3🡪Waiting time

**Defuzzification:**

At the end of rule generation phase,we use defuzzifier .The output of defuzzification is called **crisp** value.

cp= 

l🡪low h🡪high m🡪medium N🡪normal S🡪suspected G🡪greedy

**Fuzzy rules1:**

**If** L1🡪L **AND** L2🡪L **THEN** node is N **If** L1🡪L **AND** L2🡪M **THEN** node is N **If** L1🡪L **AND** L2🡪H **THEN** node is S **If** L1🡪M **AND** L2🡪L **THEN** node is N **If** L1🡪M **AND** L2🡪M **THEN** node is S **If** L1🡪M **AND** L2🡪H **THEN** node is G **If** L1🡪H **AND** L2🡪L **THEN** node is S **If** L1🡪H **AND** L2🡪M **THEN** node is S **If** L1🡪H **AND** L2🡪H **THEN** node is G

**Fuzzy rule2:**

**If** L1🡪N **AND** L2🡪L **THEN** node is N  **If** L1🡪N **AND** L2🡪M **THEN** node is N **If** L1🡪N **AND** L2🡪H **THEN** node is S **If** L1🡪S **AND** L2🡪L **THEN** node is S **If** L1🡪S **AND** L2🡪M **THEN** node is S **If** L1🡪S **AND** L2🡪H **THEN** node is G **If** L1🡪G **AND** L2🡪L **THEN** node is G **If** L1🡪G **AND** L2🡪M **THEN** node is G **If** L1🡪G **AND** L2🡪H **THEN** node is G

**Algorithm 2:Resolution State**

**INPUT** :Trace fie,state ϵ{N,S,G} **OUTPUT**  :show(node,state) **begin** Get node from trace file. Calculate tcd,tca  **while(true)** Calculate TH1ca,TH2ca,TH1cd, TH2cd,TH1wt,TH2wt; Calculate:L1,L2,L3 Calculate:crisp value;  **if** crisp >50% **if** class is G **then** state= greedy  **else**  **if** class is S **then**  state=suspected  **else** node is normal.  **End End.**  **Return**:annonce(node,state) **End**

--------------------🡪3--------🡪4

In this proposed system we also find trust of path in network using **PDR(Packet Delivery Ratio)** and **AD(Average Delay)** is achieved by **FUZZY concept .**From algorithm 2 we get node is normal or suspected or greedy**.**

**Algorithm 3:Trust Value**

INPUT :PDR,AD OUTPUT :trustworthy node or not **begin if PDR** is low ,**THEN** path is untrust. **Else** **if**  **AD** is low ,**THEN** path is trustfull. **Else**  path is generally trust.  **End End**

Here we take m value is 3.After receiving ACK we calculate PDR and AD.

**Description:**

N node of node  from trace file  time of receiving node time of sending node  time for acknowledgement  maximum tolerable delay

**4.EVALUATION:**

To evaluate the Unsavoury State ,Resolution state and Trust value state which form

**REFERENCES:**

[1] M.N.Mejri,j.Ben-Othman,and Hamdi,”Survey on VANET security Challenges and possible cryptographic solutions,”Vehicular common.,vol.1,pp.53-66,2014. [2] A.Dhamgaye and N.Chavhan,”Survey on security challenges in VANET,” Int.j.comput.sci.,vol.2,pp.88-96,2013. [3] S.Zeadally,R. Hunt,Y.-S. Chen,A. Irwin,and A.Hassan,”Vehicular ad hoc networks(VANETs):status,results,and challenges,”Tellecommun.Syst.,vol.50,no.4,pp.217-241,2012. [4]M.N.Mejri and m. Hamdi,”Recent advances in cryptographic solutions for vehicular networks,”in proc.Int.symp.netw.comput.commun.,2015,pp.1-7.

[5]A.hamei,J.Ben-Othman,A.Gueroui,and F.Nait-Abedesselam,”Detecting greedy behaviours by linear regression in wireless ad networks,”in proc.IEEE Int.conf.commun.,2009,pp.1-6. [6]M.Raya,J.-P.Hubaux,and I. Aad.”Domino:A system to detect greedy behaviour in IEEE 802.11 hotspots,”in proc.2nd Int.conf.Mobile syst.appl.serv.,2004,pp.84-97. [7]DSRC,2013.[Online].Available: http://grouper.ieee.org/groups/scc32/dsrc/