IJARIIT INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact factor: 4.295
(Volume 5, Issue 4)
Available online at: www.ijariit.com

Manipulating and detecting greedy behaviour while disseminating emergency messages in urban VANET

Selvarani B.
manipremi648@gmail.com

Rahin Batcha R.
batchabaksha@gmail.com

ABSTRACT

Vehicular Ad hoc Networks (VANETs), whose main aim is to provide road safety and enhance the driving conditions, are exposed to several kinds of attacks such as Denial of Service (DoS) attacks which affect the availability of the underlying services for legitimate users. The principle reason for wellbeing application is to give security street condition data to clients and consequently spare human lives from mischances. Cautioning messages are the more basic part of the security messages and latency of this message will leads to many problems. In the proposed work urban multi-hop broadcast protocol is used to disseminate the emergency message in all the directions simultaneously. This protocol assigns the duty of forwarding and acknowledging the broadcast packet to only one node among the candidate nodes and such a forwarding node is successfully chosen by the asynchronous contention among them. In this paper an enhanced forwarder node selection scheme is adopted which can manipulate back off greedy behaviour while disseminating the emergency message and a new algorithm called Forwarding Greedy Misbehaviour Detection (FGMD) is proposed to detect the existence of greedy behaviour in VANET. By monitoring network traffic traces, the algorithm is able to affirm the existence or not of greedy nodes using newly defined five parameters by fuzzy logic. The proposed system may result in better performance in terms of Message reception rate, throughput, and transmission delay.

Keywords— *Urban vehicular Ad Hoc networks, Emergency message, Greedy behaviour, Dos attacks, FGMD*

1. INTRODUCTION

The VANET (Vehicular Adhoc Network) has received tidy attention in recent years, and a few connected standards and applications are encouraged in several countries. The VANET is considered to be a special type of MANET (Mobile Adhoc Network) where the mobile nodes are considered to be the vehicles. It is considered to be one of the inducing areas for the development of Intelligent Transportation System (ITS) in order to offer wellbeing and safety to the road users. Disseminating traffic information in VANET is a critical problem. Indifference to other networks such as Internet where data is usually unicasted, the traffic information has nature which requires broadcasting. Traffic information is destined for a public interest, and not only for an individual. So, disseminating the traffic information using broadcasting pattern is more suitable as compared to a routing approach that employs uncasing.

The broadcasting scheme has the advantage that a vehicle does not require the destination address and the route to a particular destination. As an outcome, it declines the various difficulties in VANET such as complexity of route discovery, address resolution, and topology management.

A multi-hop wireless broadcast has been considered a promising technology to support safety-related applications that have strict quality-of-service requirements such as low latency, high reliability, scalability, etc... In urban transportation system, which enables moving vehicles to quickly and accurately collect real-time road traffic information and notify neighboring vehicles of potentially dangerous events quickly. In the urban transportation environment, the efficiency of multi-hop broadcast is critically challenged by complex road structure, severe channel contention, message redundancy, etc

In urban VANETs, safety-related applications usually operate based on wireless broadcast since warning messages (e.g., accident, blocked street, traffic congestion, etc.) need to be delivered to all nearby related vehicles.

In addition, due to the limited transmission range of an On-Board Unit (OBU) in vehicles, multi-hop transmissions of warning messages are usually employed because such kind of alert information is indispensable to assist remote drivers to make an early driving decision. For example, in case of traffic accidents or jams, a remote driver expects to get knowledge of such events as early as possible, and then chooses an alternate driving route to avoid traffic jams in the urban transportation environment. However, such alert information has to be forwarded hop by hop to remote drivers. Hence a single forwarder is chosen among contending nodes by asynchronous contention among them. This chosen forwarder may sometime misbehave by not forwarding the emergency broadcast packet to its neighbors. This type of greedy behavior comes under DoS family.

The attacks and vulnerabilities against VANETs can be classified into attacks on availability, integrity and data trust, authenticity, confidentiality, and non-repudiation. Attacks on availability are mainly formed by the Denial of Service (DoS) attacks the family. DoS attacks can be achieved by external or internal malicious nodes to the network. Generally, the attacker aims to interrupt services for legitimate users. Thus, these services will be more available to him. Detecting and avoiding DoS attacks are a critical security requirement for VANETs whose main objective is to ensure the life of drivers and road users.

Multiple techniques can be used by malicious users/drivers to make the VANET experience service interruptions. In this paper, we focus on greedy behavior which is a common DoS attack. It targets the operation of the MAC layer and exploits the weaknesses of the access method to the medium. The major problem of such attacks is that they can be performed by an authenticated user which makes the detection more complicated. Obviously, handling back off parameters allows easily a greedy attack. A malicious node can, for example, choose a low value of back off instead of a random one. It can even choose zero and increases considerably its chances to access to the medium. Henceforth, to detect this type of attack, we propose a new detection algorithm which distinguishes the presence of a greedy behavior and identifies the nodes that are suspected to be compromised using as input a short periodic traffic traces.

We adopt an enhanced forwarding node selection scheme in Urban Multi-hop Broadcast Protocol (UMBP) which manipulates any greedy misbehavior while disseminating the emergency messages in VANET.

2. RELATED WORKS

C. Y. Yang et al. [1] presented a street-based broadcast scheme and each vehicle periodically broadcasts the hello message which contains its position information to neighboring vehicles. In case of a traffic accident, a vehicle broadcasts an emergency message, and the farthest neighboring vehicle serves as the relaying node to forward the emergency message. Here a smart relay mechanism was proposed. The future enhancement of this work is to prevent false warnings from malicious people.

Xiaomin Ma et al. [2] proposed a cross-layer broadcast scheme for safety related message dissemination. The scheme divides safety related messages in VANETs into three groups and assigns them different priorities. As the class-three message, beacon messages are periodically exchanged among neighboring vehicles, which include the speeds, positions, travel interval, and moving directions of these vehicles. However, repeatedly broadcasting hello or beacon messages induces the disadvantage of signaling overhead, and consumes many of wireless channel resources.

Y. Bi et al [3] proposed a Cross Layer Broadcast Protocol (CLBP) which selects a forwarding node according to a novel metric considering the distance, relative velocity, and packet error rate, achieving low latency and high reliability in the highway scenario. However, the drawback of this approach is lack of multi-directional broadcast support at intersections in urban scenarios and there exists severe packet collision.

F. J. Martinez et al. [4] presented an enhanced Street Broadcast Reduction (eSBR) scheme is to address the broadcast storm problem in urban VANETs. On reception of an emergency message, a vehicle checks by searching the message ID list whether the message has already been received or not. It keeps the emergency message if the message is received for the first time and then decides to rebroadcast the message if its distance to the sender is larger than the threshold.

M. Fogue et al [5] proposed a Profile-driven Adaptive Warning Dissemination Scheme (PAWDS) which focuses on safety related message dissemination in real urban environments. This scheme uses a mapping technique based on adapting the dissemination strategy according to both characteristics of street area and density of vehicles. This scheme is combined with enhanced street broadcast reduction (eSBR) to improve the performance. One of the drawbacks of this scheme is even though eSBR and PAWDS relieve redundant messages to some extent, they are unable to guarantee a single forwarding node at each hop.

G. Korkmaz et al [6] designed an Ad hoc Multihop Broadcast (AMB) and Urban Multihop Broadcast (UMB) to address the broadcast storm, latency and reliability issues. They utilize the directional broadcast to select remote forwarding nodes by the Request to Broadcast (RTS)/Clear to Broadcast (CTS) handshake on straight roads. At intersections, UMB embraces the repeater to broadcast emergency messages, while AMB enables a hunter vehicle to select the closest vehicle to the intersection which is used to forward emergency messages in each road direction. One of the drawbacks of UMB is the cost incurred on repeaters is high, and in case of AMB, it is waste of time in finding the vehicles closest to the intersection.

J. Sahoo et al BPAB [7, utilize different broadcast strategies according to the positions of emergency message senders. On a road, the directional broadcast scheme is adopted to iteratively divide the transmission range to select the furthest neighboring node. At intersections, the broadcast scheme selects a forwarding node in the inner region. Nevertheless, the RTS/CTS handshake may be interrupted, and additionally, the directional broadcast is sequentially embraced in different road directions, which increases the emergency message transmission delay.

Ming Li et al [8] presented an opportunistic broadcast protocol which involves two kinds of broadcast phase; where one phase quickly broadcasts the warning message using relatively long hops, and the other phase make use of additional makeup transmissions to guarantee Packet Reception Ratio (PRR). The design of both phases is optimized to minimize the total number of transmissions. Secondly, a distributed opportunistic broadcast coordination function (OBCF), an underlying MAC-layer broadcast primitive is proposed for the recipients of a single broadcast to agree on who will be elected as the actual relay nodes. The future extension of this work is to adapt the OppCast to different kinds of road topologies and disconnected networks.

Francisco J. Ros et al [9] proposed a broadcast protocol which is extension to the Parameter less Broadcast in Static to highly Mobile (PBSM). This approach tries to reduce protocol redundancy. The main novelty is the modification of the algorithm to handle acknowledgments of broadcast messages. The drawback of this approach is degradation in message reception rate when the vehicle density goes up.

Martin Koubek, et al [10] presented G- SRMB a geo broadcasting which is an extension to the Slotted Restricted Mobility Based (SRMB) broadcasting protocol which restricts the SRMB broadcasting to a geographical area where dissemination is restricted to a specific direction. This approach greatly reduces or decreases the number of redundant transmissions. G-SRMB satisfies the emergency messaging from the reliability & end-to-end delay perspective.

Hamieh et al. [11] used the linear regression mathematical concept to detect MAC greedy nodes in an IEEE 802.11 based-protocol network (MANET). This method is based on the observation that successive access times of nodes are highly correlated. It was possible to represent the behavior of nodes in a network linearly. The calculated slope of the linear regression straight is used to assess the presence or absence of greedy behavior. This proposition does not require any modification of the MAC layer of the protocol IEEE 802.11.

Raya et al. [12] proposed a greedy behavior detection scheme called DOMINO, for infrastructure networks (IEEE 802.11 hotspots). DOMINO is a software system for detection of greedy behavior in the IEEE 802.11 MAC layer for public networks. It is to be installed in the Access Point (AP), it can identify and detect greedy stations without any required modification of the standard protocol at the AP. It has the advantage to be transparent to network users.

Djahel et al. [13] proposed FLSAC (Fuzzy Logic based Scheme to Struggle Against Adaptative Cheaters) FLASAC is an Enhancement of DOMINO scheme but adapted to (WMNs). FLSAC focus the detection of greedy behaving nodes which aim to violate the proper use of the CSMA/CA protocol rules in order to increase their bandwidth at the expense of the well behaving nodes.

The proposed scheme can be implemented in such gateways or Mesh Routers to supervise attached wireless nodes behavior and also report any deviation from the proper use of the MAC protocol. However, most of the adaptive approaches in VANET do not focus on how this selected forwarding node behaves while disseminating emergency message. At the same time, a careful analysis of the existing approaches reveals the lack of a greedy behavior detection scheme that takes into consideration the particular features of VANET. This was our major motivation to tackle this issue.

3. ADVERSARY MODEL AND ASSUMPTIONS

We focus on greedy behavior which is a common DoS attack. It targets the operation of the MAC layer and exploits the weaknesses of the access method to the medium. A greedy node aims to minimize its waiting time by choosing a low back off value for faster access to the channel and therefore penalize the other honest nodes.Then, it does not respect restrictions of the channel access method and tries always to connect to the medium and maintains it for its own use. The major problem of such attacks is that they can be performed by an authenticated user which makes the detection more complicated. We consider an adversary model in which during selection of a relay node, a selected relay node may fail to send the message to the next hops; this happens by the following situation**,** A cracker might put an adversary node that misbehaves might choose the lowest backoff time always, and this node will always be elected among the contended nodes. So emergency message will never be delivered. Obviously, handling back off parameters allows easily a greedy attack. We assume that there is constant no of vehicles are available during the monitoring period $T_{p.}$ In order to enable UMBP to be tractable, the following assumptions are made.

- A traffic accident occurs either on a road or within an intersection area. Only the vehicle that first detects this event initiates emergency message dissemination, and other vehicles detecting the same event will not perform the emergency message initialization process after receiving the broadcast message.
- Packets are successfully received as long as there are not packet collisions within the transmission range *R*, and packet losses due to channel error are not considered.

4. PROPOSED WORK

The proposed work consists of two parts: i) Manipulating back off greedy behavior while disseminating emergency message by adopting an enhanced forwarder node selection scheme that reduces transmission delay depicted in figure 1 ii) To detect the existence or not of a greedy node in the network by proposing a new algorithm called FGMD depicted in figure 2.

4.1 Manipulating back off greedy behavior

In case of traffic accidents or jams, a remote driver expects to get knowledge of such events as early as possible, and then chooses an alternate driving route to avoid traffic jams in the urban transportation environment. However, such alert information has to be forwarded hop by hop to remote drivers. To achieve this Urban Multihop Broadcast protocol (UMBP) is used to broadcast emergency messages in urban transportation environment. This is a multihop broadcasting based protocol that uses eRTS/eCTS handshake approach for sending packets and receiving acknowledgments. Message dissemination is very difficult in urban areas that crowded with tall buildings and number of intersections so there occur line-of-sight problem. So, it becomes compulsory to have methods or protocols for sending data packets in urban areas. And Urban Multihop broadcast (UMB) protocol is one of them that do directional broadcasting as well as broadcasting at intersections in urban areas.

4.1.1 Broadcasting strategies: In this method, sender node try to choose the single node (furthest one) in the broadcast direction to assign the duty of forwarding and acknowledging the packets and sender selects the furthest node without knowing the ID or position of its neighbours because nodes change their topology very rapidly due to high mobility. In order to choose the farthest node, this protocol divides the road portion within the transmission range R into segments. These segments are created only in the direction of propagation. UMBP includes a novel forwarding node selection scheme that utilizes iterative partition, mini-slot, and black-burst to quickly select remote neighbouring nodes, and a single forwarding node is successfully chosen by the asynchronous contention among them. Then, bidirectional broadcast, multi-directional broadcast, and directional broadcast are considered conferring to the locations of the emergency message senders.

The sender node sends Request to send (eRTS) packets to all its neighbours in the direction of dissemination then all neighbouring nodes will compute their distance from the source node. Based on this distance, nodes will send energy burst (channel jamming signal) known as black-burst to the source node. More the distance of receiving node from the source node the longest will be black burst. Thus, length of black-burst is used to choose the furthest node and the furthest node sends the longest black burst. Nodes will try to send their black- burst in shortest possible time (SIFS) after they catch the eRTS packet. At the end of the black- burst, nodes turn around and pay attention to the channel. If they find the channel unoccupied, it means that their black-burst was longest and they are now responsible to reply with an eCTS packet after a duration called CTSTIME. Alternatively, if they find the channel busy, it means that there are some other vehicles further away and they will not send eCTS packet. During this process nodes in between can overhear the transmission as well but they cannot access the channel for a time interval specified in eRTS and eCTS packets. After getting the eCTS packet from furthest node, source node will send the broadcast packet to that furthest node. In this broadcast packet, the source node contains the ID of the node which has successfully sent the eCTS packet.

This node will be now accountable for forwarding the broadcast packet and sending and Acknowledgment (ACK) to the source. And the ACK packet ensures the reliability of packet propagation in the preferred direction.

A traffic accident may occur either on a road or at an intersection in the urban environment, which triggers the initialization of an emergency message in UMBP. At the first hop, the emergency message is bi-directionally broadcast to neighbouring nodes if the source node locates on a straight road, and a single relaying node is selected to forward the message in either direction of the source node and a single relaying node is selected to forward the message in each road branch. From the second hop, the message is directionally broadcast and only one relaying except that the forwarding node locates in an intersection area. The iteration process is performed simultaneously in two opposite directions of the source node until the candidate forwarding nodes are successfully selected in each direction. After *N* iterations, as soon as sensing the wireless channel idle for SIFS interval, a candidate forwarding node randomly selects a mini-slot from the Contention Window (CW) and starts the back off process based on the CSMA/CA mechanism, Where

$$CW= (T_{difs} – T_{sifs})/T$$

If the wireless channel keeps idle until the back off timer overflows, the candidate forwarding node sends an *e*RTS. Other candidate forwarding nodes that choose larger mini-slots stop their back off timers on receiving the *e*RTS from the candidate forwarding node within the same final FA and give up the opportunity to serve as a forwarding node. After successfully delivering an *e*RTS, a candidate forwarding node is promoted to be a forwarding node and initiates the *e*RTS /*e*CTS handshake for directional broadcast along the emergency message propagation direction on a road.

However, most of the adaptive approaches in VANET do not focus on how the selected forwarding node behaves while disseminating the emergency messages. It fails to analyse the node behaviour while forwarding the message. The selected relay node may fail to send the message to the next hops; this happens by the following situation**,** A cracker might put a node that misbehaves might choose lowest back off time always, and this node will always be elected among the contended nodes. So emergency message will never be delivered. It creates higher transmission delay. In an adversary model, during contention process among candidate forwarding nodes, a greedy node can, for example, choose a low value of back off instead of random one. It can even choose zero and increases considerably its chances to access to the medium. If a node wins the contention process by choosing low value of back off, it becomes the forwarder node to the next hop. But if the node fails to forward the message, the sender node will retransmit the packet by again conducting the selection scheme. Being greedy this node will again choose a low value of back off instead of random one and again it will access the channel. To manipulate such problem, we adopted an enhanced forwarding node selection scheme in which the sender can terminate that particular suspected misbehaving node from the selection process and keeps that node in a suspicion phase and it chooses an alternate forwarder from among the other contending node. That is if the same node twice accesses the channel continuously and does not perform its assigned duty of forwarding means, the sender node does not consider them for the forwarding selection process for the third time.

Instead, it selects an alternate forwarder among the candidate nodes by asynchronous contention among them. The suspected node is now monitored to detect the actual existence of greedy by the new algorithm FGMD

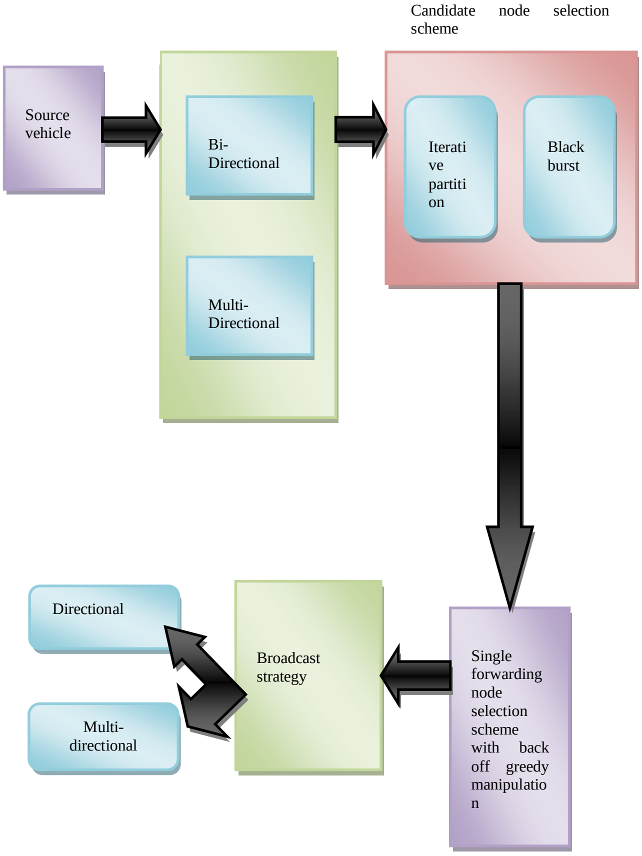

Fig. 1: Proposed Emergency Message Broadcasting Strategy

4.2 Detecting greedy behavior

For decision-making systems, where the membership of an element (node in our case) to a class (authentic or greedy) remains proportional, fuzzy logic can be an efficient tool for design. In this work, we propose a new decision scheme FGMD for detecting greedy behaviour suitable for VANETs. This scheme detects nodes which aim to violate the proper use of the CSMA/CA protocol rules in order to increase their bandwidth at the expense of the well-behaving nodes. It used newly defined metrics which best convenient to highly mobile networks and can be used during short monitoring periods. In our watchdog detection software, we have to supervise the following 5 newly defined parameters for each node in the VANET.

The duration between two successive transmissions, Transmission time, Connection attempts a number of a node, Delay, Packet Drop Ratio. From a fuzzy logic point of view, and for each parameter, we begin to suspect the existence of a greedy behaviour from a certain value of the parameter (first threshold).

Reaching a certain value of the parameter (second threshold) makes suspicion high enough. Between these two threshold values, suspicion is gradual. So, our idea is based on the use of the tools provided by the fuzzy logic theory which help to solve this kind of problems.

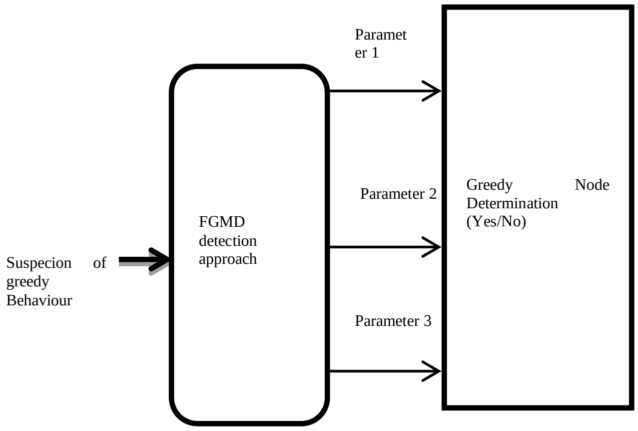
Suspecion of greedy Behaviour
FGMD detection approach
Paramet er 1
Parameter 2
Parameter 3
Greedy Node Determination (Yes/No)

Fig. 2: System Architecture of Greedy Detection Scheme

At the end of the suggestion, the fuzzy outputs are firmed but they are not directly usable. It is essential to transfer from "fuzzy world" to the "real world": It is called the defuzzification stage. Defuzzification is mainly used to provide a precise final value as a result of the end of treatment which helps to make a decision. This value is known as Crisp value. Several defuzzification techniques exist; the most used one is the method of the centre of gravity. With this method, the value of Crisp is calculated from the values of the area centre of each fuzzy set.

Table 1: Parameters to find greedy behaviour

Parameter	**Value**
T_p	Total Monitoring period
N	The total number of vehicles.
V1	A number of connections mpts.
V2	Connection duration.
V3	Average of waiting times among connections.
P1ca	Threshold of connection attempts from which we commence to suspect greedy behaviour.
P2ca	Threshold of connection attempts from which we suspect the greedy behaviour.
P1cd	Threshold of connection duration from which we commence to suspect greedy behaviour.
P2cd	Threshold of connection duration from which we suspect the greedy behaviour.
P1wt	Threshold of waiting times between connections average from which we commence to suspect greedy behaviour.
Pdr	When the packet drop ratio is high, we start to suspect the greedy behaviour.
D_L	The greedy node creates a delay in the network, where we start to suspect it.

Furthermore, we need to define the parameters mentioned in Table 1 and used especially to specify the first and the second threshold for each supervised metric. More precisely, these parameters are defined as follows:

- P1ca = TCA /N: is the threshold from which we begin to suspect greedy behavior. If the number of connection attempts of a controlled node exceeds the average TCA/N then the node is suspected.
- P2ca = 0:6TCA: is the threshold from which we classify the controlled node as greedy. We determine if a node reaches 60% of the total number of connections, then it is suspected as greedy.
- P1cd = TCD/N: is the threshold from which we begin to suspect greedy behavior. If the average of the total connections duration of a controlled node exceeds the total average of all nodes TCD/N then the node is suspected.
- P2cd = 0:5TCD: is the threshold from which we classify the controlled node as greedy. We determined that if a node reaches 50% of the total duration of connections, then it is suspected greedy.
- P1wt = min ($AIFS_t$): if the average of waiting times between connections of a controlled node is lower than $AIFS_t$ threshold, the node is greedy.

In addition to these, two additional parameters packet drop and delay characteristics are analyzed to identify the existence or not of a greedy node.

5. ALGORITHM: DETECTION APPROACH

```
INPUT: T_p: Monitoring period;
File: Collected Traffic File;
State ε G, H, S.

OUTPUT: Announce Decision (V ID, State)
Begin
Extract Vehicle IDs existing in File during the T_p period,
Extract N;
For each Vehicle ε {Vehicle IDs} do
    Calculate P1cd, P2cd, and P1wtbc;
    Calculate P1nca, P2nca;
    Calculate: V1; V2; V3;
    Calculate: Pdr, D_L
    Calculate Crisp;
    if Crisp > 50% for the class G then
        V ID is G
    else
        if Crisp > 50% for the class S then
            V ID is S
        else
            V ID is H
        end
    end
    Return: Announce Decision (V ID, State)
end
end
```

6. SIMULATION RESULTS

This session shows simulation results of my proposed work which has been implemented in NS2 software version 2.3.5. Every vehicular node move in a random manner with no stop time. In this simulation setup vehicular nodes are randomly deployed. All vehicular nodes in the network have same transmission range of 250 meters. The proposed system uses five parameters to determine the existence of greedy behaviour or not, namely 1) average waiting time 2) number of connection stabs3) T average connection duration 4) packet drop ratio and

5) delay which is calculated for a different time and different messages sent across the VANET. The exhaustive parameter settings that are used in the simulations are tabulated in below table 2.

Table 2: Parameters in Simulation

Parameter	Value
Node count	30
Average speed	36 Km/h (~10m/s)
Traffic model	CBR
Mobility simulator	Network Simulator(NS2)
MAC Protocol	IEEE802.11
Transmission range	250m
Packet Size	512 Bytes
Routing Protocol	AODV

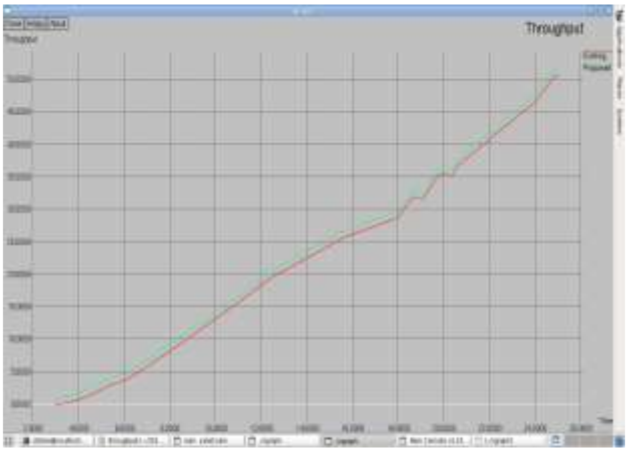

Fig. 3: X-Graph for performance comparison of throughput

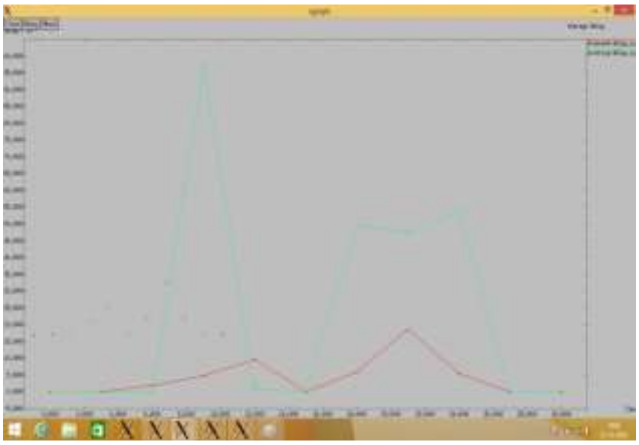

Fig. 4: X-Graph for Performance comparison of Average delay

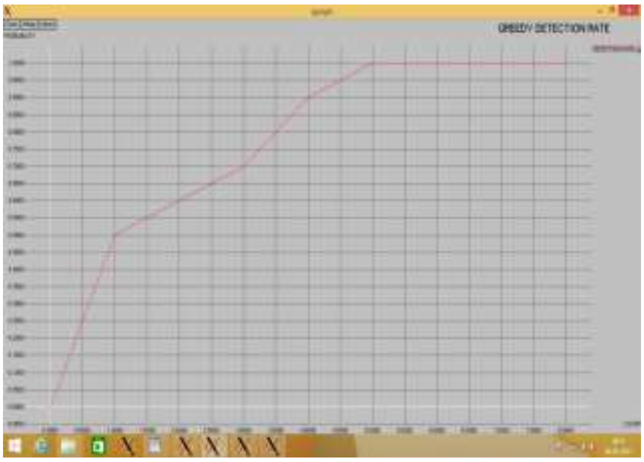

Fig. 5: X-Graph for analysis of greedy detection rate

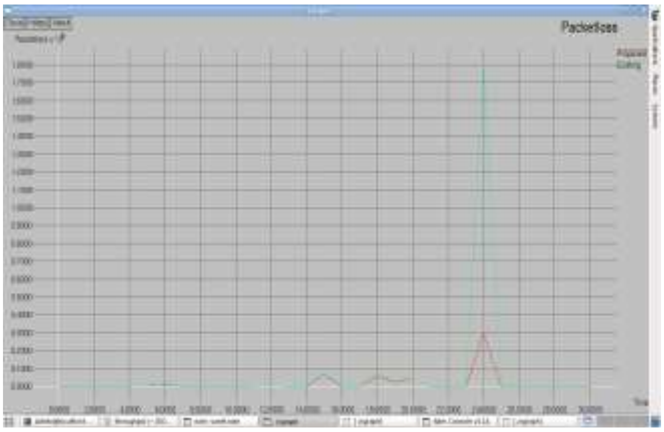

Fig. 6: X- Graph for performance comparison of packet drop

6.1 Throughput

Throughput is the number of successful messages reached to the destination vehicle i.e. the amount of data transferred over a given period of time. In proposed work, the throughput has been drastically increased which denotes the best performance of the system as shown in Fig 3.

6.2 Delay

Delay is time required for our message to reach the destination. Thus the delay has been decreased since there is successful transmission of the packet since the information has been reached to the receiver vehicle as in Fig 4

6.3 Greedy Detection Rate

It is the ratio of true detections to true examples.

6.4 Packet Drop Ratio (PDR)

Packet Drop Ratio is the number of packets lost across the network without reaching the destination vehicle as in figure 6.

7. CONCLUSION

Vehicular Ad hoc Networks (VANETs), whose main aim is to provide road safety and enhance the driving conditions, are exposed to several kinds of attacks such as Denial of Service (DoS) attacks which affect the availability of the underlying services for legitimate users. The principle reason for wellbeing application is to give security street condition data to clients and consequently spare human lives from mischances. Cautioning messages are the more basic part of the security messages and latency of this message will leads to many problems. In the proposed work urban multi-hop broadcast protocol is used to disseminate the emergency message in all the directions simultaneously. This protocol assigns the duty of forwarding and acknowledging the broadcast packet to only one node among the candidate nodes and such a forwarding node is successfully chosen by the asynchronous contention among them. In this paper an enhanced forwarder node selection scheme is adopted which can manipulate back off greedy behaviour while disseminating emergency message and a new algorithm called Forwarding Greedy Misbehaviour Detection (FGMD) is proposed to detect the existence of greedy behaviour in VANET. By monitoring network traffic traces, the algorithm is able to affirm the existence or not of greedy nodes using newly defined five parameters. The proposed system may result in better performance in terms of Message reception rate, throughput, and transmission delay. Our objective in the future is the application of the proposed algorithm for the detection of other VANET denial of service attacks such as jamming.

8. REFERENCES

[1] Y. Yang and S. C. Lo, "Street broadcast with smart relay for emergency messages in VANET," in Proc. IEEE 24th Int. Conf. Adv. Inf. Netw. Appl.Workshops, Apr. 2010, pp. 323–328.

[2] X. Ma, J. Zhang, X. Yin, and K. S. Trivedi, "Design and analysis of a robust broadcast scheme for VANET safety-related services," IEEE Trans. Veh. Technol., vol. 61, no. 1, pp. 46–61, Jan. 2012.

[3] Y. Bi, L. X. Cai, X. Shen, and H. Zhao, "Efficient and reliable broadcast in intervehicle communication networks: A cross-layer approach," IEEE Trans. Veh. Technol., vol. 59, no. 5, pp. 2404–2417, Jun. 2010.

[4] F. J. Martinez et al., "Evaluating the impact of a novel warning message dissemination scheme for VANETs using real city maps," in Proc. IFIP Networking, May 2010, pp. 265–276.

[5] M. Fogue et al., "An adaptive system based on road map profiling to enhance warning message dissemination in VANETs," IEEE/ACM Trans. Netw., vol. 21, no. 3, pp. 883–895, Jun. 2013.

[6] G. Korkmaz, E. Ekici, and F. Ozguner, "Black-burst-based multihop broadcast protocols for vehicular networks," IEEE Trans. Veh. Technol., vol. 56, no. 5, pp. 3159–3167, Sep. 2007.

[7] J. Sahoo, E. H. K. Wu, P. K. Sahu, and M. Gerla, "Binary-partition assisted MAC-layer broadcast for emergency message dissemination in VANETs," IEEE Trans. Intell. Transp. Syst., vol. 12, no. 3, pp. 757–770, Sep. 2011.

[8] M. Li, W. Lou, and K. Zeng, "OppCast: Opportunistic broadcast of warning messages in VANETs with unreliable links," in Proc. IEEE MASS, Oct. 2009, pp. 534–543.

[9] F. Ros, P. Ruiz, and I. Stojmenovic, "Reliable and efficient broadcasting in vehicular ad hoc networks," in Proc. IEEE VTC Spring, Apr. 2009, pp. 1–5.M. Li, W.

[10] M. Koubek, S. Rea, and D. Pesch, "Reliable broadcasting for active safety applications in vehicular highway networks," in Proc. IEEE VTC Spring, May 2010, pp. 1–5.

[11] M. Raya, J.-P. Hubaux, and I. Aad, "Domino: a system to detect greedy behavior in IEEE 802.11 hotspots," in Proceedings of the 2nd international conference on Mobile systems, applications, and services. ACM, 2004, pp. 84–97.

[12] S. Djahel and F. Na¨ıt-Abdesselam, "Flsac: A new scheme to defend against greedy behavior in wireless mesh networks," International Journal of Communication Systems, vol. 22, no. 10, pp. 1245–1266, 2009.

[13] A. Hamieh, J. Ben-Othman, A. Gueroui, and F. Na¨ıt-Abdesselam, "Detecting greedy behaviors by linear regression in wireless ad hoc networks," in Communications, 2009. ICC'09. IEEE International Conference on. IEEE, 2009, pp. 1–6.