Volume: 09 Issue: 04 Pages: 3510-3514(2018) ISSN: 0975-0290

# Enhancing the Efficiency of Routing Protocols in VANETS by defending Dos Attacks using BF-IPCM

**Pavan Kumar Pagadala, Research Scholar**
Computer Science and Engineering
Anna University, Tamilnadu,India
pavankumarpagadala@gmail.com
**Dr. N.M Saravana Kumar, Professor & HOD**
Computer Science and Engineering
Vivekanadha College of Engineering for Women, Tiruchengode, Tamilnadu, India
saravanakumaar2008@gmail.com

**ABSTRACT**

**Routing in VANETs (pure ad hoc architectures) with dynamic nature of the network becomes a challenging task for finding and maintaining routes. So, detecting the misbehaving vehicles is an important task in for improving the efficiency of the vehicles and to incorporate the reliable and secure routing in the transport system. Due to the self -configure (mobility) characteristic of the VANETS, it is very difficult to the road side and base station units to keep track of the actions happening among the vehicles. Obviously the attackers will have the fraudulent nature that same will persist over time with them that will be effected to the normal vehicles which is travelling in the network from the non trustworthy vehicles. So detection and proper action is needed to improve the efficient routing of the vehicles in the network. Earlier we have many techniques for detecting and preventing the misbehaving vehicles depending upon the threshold values, mobility factors, power ratios etc., now we are proposing a new technique called Bloom-Filter based IP Choke Mechanism for locating the harmful vehicle. In this paper we will discuss about the proposed technique on how to identify the malicious vehicle and how to defend the attacked vehicle by blocking it form the routing process.**

Keywords: **Bloom-Filter based IP Chock (BF-IPCM), Mobility, Routing, VANETS**.

Date of Submission: Jan 03, 2018 Date of Acceptance: Jan 16, 2018

## I. Introduction

A Vehicular Ad-Hoc Network is a shade of Mobile ad-hoc network which offers communication among vehicles to the road side unites and base stations via radio waves. They persists characteristics as MANETS with them. Due to the high mobility of nodes network topology changes occur frequently. Here the nodes move with higher average speed and the number of nodes is assumed o be very large. The two major services offered by VANETS are, inter vehicular services and vehicle-to-infrastructure communication services. These are used in real time communications such as Military Battlefield, local danger warning, weather information, mobile e-commerce, internet access and in many applications. Some important issues of VANETs are, Unpredictability of environment, Unreliability of wireless medium, Resource-constrained nodes, Dynamic topology, Security and Reliability, Power Consumption and The limited bandwidth. So for efficient and reliable routing it must follow the security requirements to detect or prevent the attacks against misbehavior vehicles. The following figure shows the architecture of VANET and routing process with DoS attack.

## II. Routing in VANET

Routing is a process of sending the packets or data from source to destination. In VANETS Routing is classified into three categories. They are Topology based, Transmission Strategies (Broadcast, Multi cast, Uni cast and Geo cast) routing and Cluster Based Routing Protocols. We know VANET and MANET share the same principle that not relying on fixed infrastructure for communication, and have many similarities, e.g., self-organization, self-management, low bandwidth and short radio transmission range. Thus, most ad hoc routing protocols are still applicable, such as AODV (Ad-hoc On-demand Distance Vector) and DSR (Dynamic Source Routing). AODV and DSR are designed for general purpose mobile ad hoc networks and do not maintain routes unless they are needed. Hence, they can reduce overhead, especially in scenarios with a small number of network flows. Even after most ad hoc or topology routing protocols (e.g., AODV and DSR) suffer from highly dynamic nature of node mobility because they tend to have poor route convergence and low communication throughput.

Node movement in VANETs is usually restricted in just bidirectional movements constrained along roads and streets. So routing strategies that use geographical location

Volume: 09 Issue: 04 Pages: 3510-3514(2018) ISSN: 0975-0290

information obtained from street maps, traffic models or even more prevalent navigational systems on-board the vehicles make sense. This fact receives support from a number of studies that compare the performance of topology-based routing (such as AODV and DSR) against position-based routing strategies in urban as well highway traffic scenarios. Therefore, geographic routing (position-based routing) has been identified as a more promising routing paradigm for VANETs.

In cluster-based routing, a virtual network infrastructure must be created through the clustering of nodes in order to provide scalability.. Each cluster can have a cluster head, which is responsible for intra- and inter-cluster coordination in the network management functions.

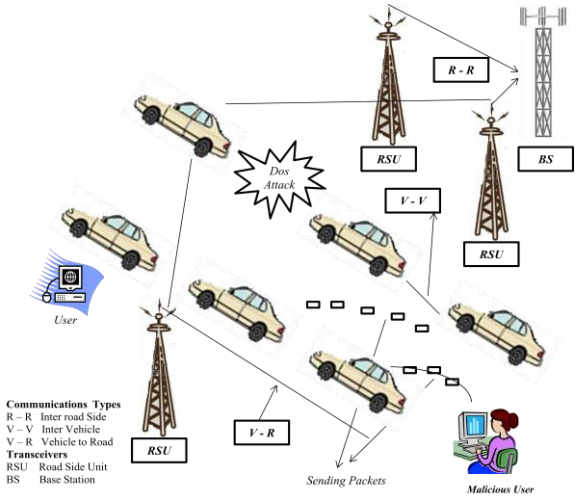


**Fig 1: Routing Process in VANET with DoS Attacks**

Nodes inside a cluster communicate via direct links. Inter-cluster communication is performed via the cluster-heads. The creation of a virtual network infrastructure is crucial for the scalability of media access protocols, routing protocols, and the security infrastructure. The stable clustering of nodes is the key to create this infrastructure. Many cluster-based routing protocols [20]–[22] have been studied in MANETs. However, VANETs behave in different ways than the models that predominate in Manet's research, due to driver behavior, constraints on mobility, and high speeds. Consequently, current MANETs clustering techniques are unstable in vehicular networks. The clusters created by these techniques are too short-lived to provide scalability with low communications overhead. Cluster-based routing protocols can achieve good scalability for large networks, but a significant hurdle for them in fast-changing VANET systems is the delay and overhead involved in forming and maintaining these clusters.

## III. Security Challenge in VANET

VANET poses a number of the foremost difficult issues in wireless ad hoc and detector network analysis[19]. additionally, the problems on VANET security become more challenging due to the distinctive options of the network, like high-speed quality of network entity or vehicle, and extremely great amount of network entities specifically, it's essential to create sure that "life-critical safety" data can't be inserted or changed by an attacker; likewise, the system ought to be ready to help establishing the liability of drivers; however at a similar time, it ought to protect as way as possible the privacy of the drivers and passengers. It is obvious that any malicious behavior of users, like a modification and replay attack[3] with regard to the disseminated messages, might be fatal to alternative users. VANET security ought to satisfy the following needs like Message Authentication and Integrity, Message Non-Repudiation, Entity Authentication, Access Control Message, Privacy and Anonymity, Liability Identification, Jamming, Impersonation etc.,

### Attacks in VANET

In VANET, there are some problematic issues most of which are flied around security issues such as data integrity, privacy, and confidentiality. Moreover, there are some issues which can influence the efficiency of VANET such as unpredictable temporary situations (e.g. creating traffic jam because of an accident). The security of VANETs is one of the most critical issues because their information transmission is propagated in open access environments. It is necessary that each one transmitted information cannot be modified by users WHO have malicious goals. Moreover, the system must be able to detect the obligation of drivers while still maintaining their privacy. There are so many different kinds of attacks that we cannot enumerate every possible one. The most obvious attack we can imagine may be an adversary send some false information and try to convince other drivers and the system. Due to the nature of open wireless medium used in VANET, there are a different type number of possible attacks by that the VANET is exposed to. The purpose of the attackers is to create problem for legal users, and as a result services are not readily available, thus denial of service. Some of the attacks are mentioned below.

### Sybil Attack

In this attack sort, a node sends multiple messages to alternative nodes and every message contains a special fancied supply identity in such some way that the creator isn't proverbial. The fundamental goals of the assaulter are to produce associate illusion to alternative nodes by causation wrong messages and to enforce alternative nodes on the road to go away the road for the advantages of the assaulter.

### Black Hole Attack

In this problem a node refuses to participate in the network or when an established node drops out to form a black hole. In this all the traffic of the network gets redirected towards a specific node which is actually doesn't exist

Volume: 09 Issue: 04 Pages: 3510-3514(2018) ISSN: 0975-0290

which results in data lost. The malicious code picks whether to drop a packet to perform a denial-of-service attack or to use its place on the route as the first step in a man-in-the-middle attack.

**ID Disclosure**

It is a passive attack[2]. During this attacker send the malicious code to the neighbors of the target node and collects the desired information. They take the ID of the target node and its current location. Due to this target vehicle's ID are disclosed and that they lose their privacy. In this global observer will access their information by observance the route of the target vehicle. For this purpose attacker will use the RSU (Road side Unit).

**Man in the middle attack**

The attacker sits in the middle of the two communicating vehicle and launch this attack. In this type of attacker control all the communication between the sender and the receiver but communicating vehicles assume they are directly communicating with each other [7]. In MIMA attacker listen the communication between the vehicles and inject false or modified message between the vehicles.

**Brute force**

Safety information is crucial in VANET. For secure VANET application as appropriate cryptographic algorithms and approaches. The attacker can use the brute force technique to find the cryptographic key.

**Denial of service (DOS) attack**

In DOS [9] the most objective is to prevent the legitimate user from accessing the network services and from network resources. DOS attack will occur by jam the channel system so no authentic vehicle will access it.In VANET it's most major problem because the user cannot communicate within the network and pass data to other vehicle that could result in a lot of devastation in life important application. 3 alternative ways through offender can do it.

a. In basic level the attacker overwhelm the node resource so that it cannot perform other necessary tasks which results in becoming the node continuously busy and not able to do anything else.
b. In extended level the attacker jam the channel by generating the high frequency in the channel so no vehicle is able to communicate to other vehicle in the network.
c. Drop the packets.

***1) Overwhelm the Node Resources***

In this DOS basic level attack, the goal of the attacker is to overwhelm the node resources such that the nodes cannot perform different necessary and important tasks. The node becomes continuously busy and utilizes all the resources to verify the messages. In fig. 1Node behind the attacker node receives this message.

However, the sending of identical message is continuously, so keeps the victim node busy and so fully denied for accessing the network. The attacker launches attack to Road Side Unit (RSU) as depicted in Fig.2

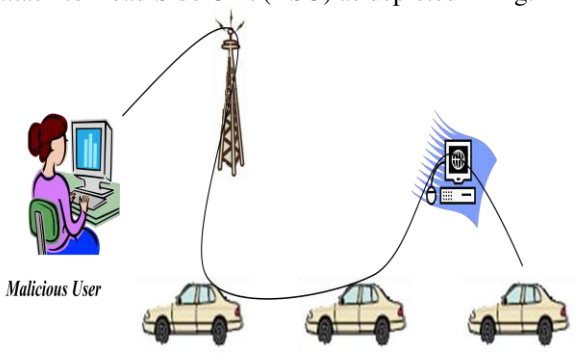


**Fig 2: DOS Attack in V – I Communication**

When RSU is continuously busy to verify the messages, the other nodes need to communicate with the RSU will not be able to get any response from it, so the service is unavailable. Hence, sending important life info during this situation is full of risk.

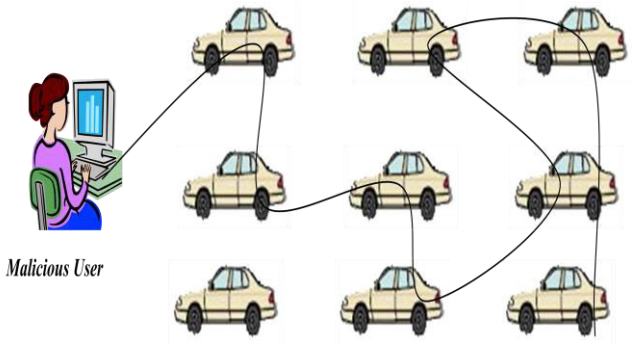


**Fig 3: DoS Attack in V – V Communication**

***2) Extended Level- Jamming the Channel***

This is a high level of DOS attack within which attacker jams the channel, therefore not permitting another user to access the network. Attacker sends high frequency channel and jams the communication between any nodes in a domain, as depicted in Fig. 3. These nodes cannot send or receive messages in that domain; i.e. services are not available in that domain due to this attack. When a node left the domain of attack, only then it will send and/or receive messages. The next stage of attack is to jam the communication channel between the nodes and the infrastructure.. During this way, sending and/or receiving messages to/from different nodes aren't possible and would fail due to network inaccessibility.

Volume: 09 Issue: 04 Pages: 3510-3514(2018) ISSN: 0975-0290

## IV. Related work

### 1. Bloom-filter-based DoS detection scheme

The Bloom-filter-based DoS detection scheme is a class that uses a combination of reactive and proactive approaches. The proactive approach[5] is used to maintain the new IP addresses (nodes) and the reactive approach is used to determine all of the connected vehicles' (nodes) . In this type of detection scheme, the network scalability is increased by forming a near zone by the closer vehicles which reduces the bandwidth, collision and computational overhead. The Bloom-filter is a compact and space-efficient probabilistic data structure for high-speed online Membership which checks against large data sets. It includes an array of bits, which are initialized to zero. Each member of a data set is mapped to bits that are randomly selected from array through hash functions. The false positive ratio is the probability of mistakenly treating a non-member as a member.

### 2. Traffic capacity based DoS detection scheme

The traffic capacity- based DoS detection scheme is the process of identifying accurately which of the flows aimed at the victim are attack flows and which ones are legitimate. Raya et al. [9] extended the traffic capacity model for the DoS detection and prevention of IP spoofed addresses in DoS attacks by using the packet detection mechanism. When the packet reaches the destination it contains the marking which is marked by all of the RSU's on the path that the packet traverses. According to this scheme, packets that traverse on the same path contain the same mark. Based on this information, the Bloom-filter out the packets and learns the signatures from the dropped packets and detects the list of the upstream hosts to rate the limit of the traffic before it reaches the victim.

## V. Bloom-Filter Based IP-Chock Detection Algorithm

Due to the high mobility and unreliable nature of the VANET system, detection of DoS attacks is more difficult. The IP-chock detection scheme[1] depends on the store and the checking of the abnormal traffic.

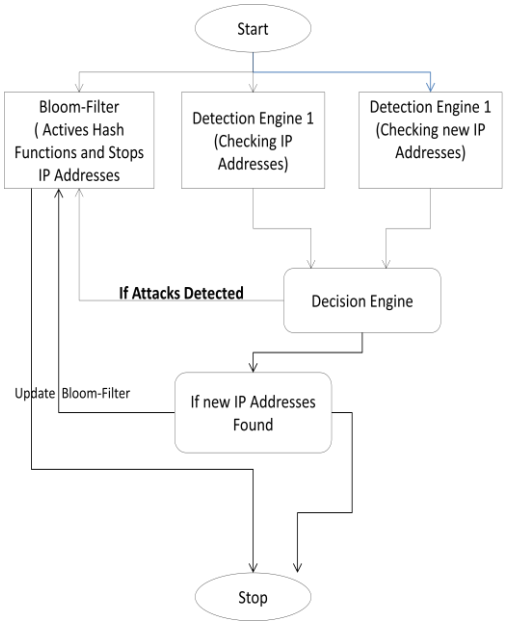


**Fig 4: Bloom – Filter IP Chock Mechanism (BF-IPCM)**

The aspect of this relies on the process of sending incoming traffic from the moving source to the moving outgoing traffic destination, taking the decision of electing the mobility of the vehicles which are restricted by the traffic pattern and traffic layout.

The IP-Chock DoS attack detection module[1] perceives abnormal traffic by using IP-chock algorithms. Let one assume that many vehicles are travelling on a high way, each vehicle travelling on the highway maintains its speed in a fixed range which comprises the three main phases of the process. The three main phases of the process are the Detection Engine phase 1, Detection Engine phase 2 and Bloom Filter phase. The consequence of these processes is based on the first stage for sensing the change through the mounted sensors on the vehicle. In the second stage, it processes the values of these sensors to decide if these values indicate the possibility to affect the network. Once the decision has been taken, the third stage plays the role of detecting the DoS attacks in the infrastructure. The detection Engine phase 1 (DE-1) is responsible fo rgathering the data (IP addresses) required to be processed later in the next phase. The main function of this phase is checking for all incoming traffic information. The detection Engine phase 2 (DE-2) processes the information collected in the previous stage (DE-1), if this stage has not found malicious IP addresses, then information is stored in a database; otherwise, it is sent to the Decision Engine (DE).

The last phase is the active Bloom-Filter with a hash function. If in the information collected by the Decision Engine, stage contains malicious IP addresses, then it generates an alarm and sends a reference link to all of the connected vehicles and does not send it to the VANET infrastructure. The successful detection process from the

Volume: 09 Issue: 04 Pages: 3510-3514(2018) ISSN: 0975-0290

incoming traffic, to the outgoing traffic, is significantly dependent on the DE

## VI. Conclusion:

Efficiency and scalability are the key requirements in the design of immunity against DoS attacks in VANET systems. The proposed scheme provides an end-to-end solution for immunity against DoS attacks. This is a novel scheme for detecting DoS attacks, which is based on the Bloom-filter. IP spoofing addresses of DoS attacks can be detected and defended by using the Bloom-filter based IP-CHOCK detection (BFICK)[1] method. It provides the availability of a service for the legitimate vehicles in the VANET. This proposed scheme is simple and highly efficient in terms of computational cost as well as storage space. This scheme works easily for high attack rates. This scheme can be used for the trace-back for the source of the attacks.

**References:**

[1] Karan Verma , IP-CHOCK (filter)-Based Detection Scheme for Denial of Service (DoS) attacks in VANET, 978-1-4799-0059-6/13/$31.00 ©2014 IEEE

[2] Routing in Vehicular Ad Hoc Networks: A Survey, 1556-6072/07/$25.00©2007IEEE IEEE Vehicular Technology Magazine | June 2007

[3] J.Nethravathy Identifying Malicious Nodes and Performance Analysis in VANET, International Journal of Applied Engineering Research ISSN 0973-4562 Volume 11, Number 9 (2016) pp 6716-6719 © Research India Publications. http://www.ripublication.com

[4] Ghassan Samara, "Security Issues and Challenges of Vehicular Ad Hoc Networks (VANET)", IEEExplore.

[5] PriyaSharma, "Enhanced attacked packet detection algorithm used for detecting attack in vanet". IRF International Conference, Pune, India, ISBN: 978-93-85832-03-1.

[6] Uzma Khana, "Detection-of-Malicious Nodes (DMN) in Vehicular Ad-Hoc Networks", Procedia Computer Science 46 (2015) 965 – 972, doi: 10.1016/j.procs.2015.01.006, Elsevier, Available online at www.sciencedirect.com

[7] Ayonija Pathre "Identification Of Malicious Vehicle In Vanet Environment From Ddos Attack ", Volume 4, No. 6, June 2013 Journal of Global Research in Computer Science

[8] Li, F., Wang, Y., "Routing in vehicular ad hoc networks: A survey," Vehicular Technology Magazine, IEEE, pp.12-22, vol.2, no.2, June 2007.

[9] M. Raya, Eviction of misbehaving and faulty node in vehicular networks", IEEE Journal on Selected Areas and Communications, Volume 25 Issue 8, pp. 1557-1568, July 2007.

[10] S. Marti, T.J. Giuli, K. Lai and M. Baker, Mitigating routing misbehavior in mobile ad hoc networks, in Proc. of the 6th annual international conference on Mobile computing and networking (MOBICOM '00), Boston, Massachusetts, USA, August 2000.

[11] S. Bhargava and D. P. Agrawal. Security Enhancements in AODV Protocol for Wireless Ad Hoc Networks. In the Proceedings of the 2001 IEEE Vehicular Technology Conference.

[12] J. Douceur. The Sybil Attack. In the Proceedings of the 1st International Peer To Peer Systems Workshop (IPTPS 2002), March 2002.

[13] Al-kahtani, MS. Survey on security attacks in Vehicular Ad hoc Networks (VANETs). In: 6th International Conference on Signal Processing and Communication Systems (ICSPCS); 2012. p. 1-9.

[14] Y. Hu, A. Perrig and D. Johnson. Packet Leashes: A Defense against Wormhole Attacks in Wireless Ad Hoc Networks. In INFOCOM 2003.

[15] Daeinabi A, Rahbar AG, Detection of malicious vehicles (DMV) through monitoring in Vehicular Ad-Hoc Networks, Springer, Multimedia Tools and Applications 2013. 66: 325-338.

[16] Y. Hu, A. Perrig and D. Johnson. E±cient security Mechanisms for Routing Protocols in the Proceedings of the network and distributed system security symposium (NDSS), 2003.

[17] Fonseca E, Festag A. A survey of existing approaches for secure ad hoc routing and their applicability to VANETs. NEC Network Laboratories; 2006.

[18] Coussement R, Saber BAB, Biskri I. Decision support protocol for intrusion detection in VANETs. ACM, DIVANet '13; 2013. p. 31-38.

[19] Ruj S, Cavenaghi MA, Huang Z, Nayak A, Stojmenovic I. On Data-Centric Misbehavior Detection in VANETs. In: Vehicular Technology Conference (VTC Fall), IEEE; 2011.