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. 3, Issue 11, November 2015

A Survey on DSR-Based Routing with Hybrid Defence for Mitigating Collaborative Attacks Using CBDS in VANET

Vipul Suresh Gunjal[1,] Prof. SachinP. Godse[2]

P.G Student, Dept. of Computer Engineering, SAE Kondhwa, SPPU,Pune, Maharashtra, India

Assistant Professor, Dept. of Computer Engineering, SAE Kondhwa, SPPU, Pune, Maharashtra, India

ABSTRACT: Now a days Due to rapid improvements in the wireless and Ad-hoc Network Domain, the development of a special category of wireless ad hoc networks called Vehicular Ad-hoc Network (VANET). VANET is Type of Mobile ad hoc network (MANET) with no infrastructure. During VANET Communication, VANET Communication Security is currently grate Challenge in presence of Different Attacks Such as DoS, BlackHole attacks, WormHole Attacks, Sybil Attacks, Timing attacks, etc. In the presence of malicious nodes, Preventing or detecting malicious nodes launching Grayhole or collaborative Blackhole attacks is a major challenge. This Paper introduces a new Routing Mechanism for VANET Communication by Using Proactive & reactive Defence Scheme known as Hybrid Defending against Collaborative Blackhole Attacks &GrayHole Attacks. Proposed Scheme is known as CBDS (Co-Operative Bait Detection Scheme) which is based on DSR Based Routing Protocol for Mitigating against Variants of Collaborative Attacks. CBDS is already proposed for MANET but We Are trying to use it in VANET to Provide Smooth, efficient & secure Routing in VANET by using Reverse Tracing Technique. Proposed scheme is more secure and efficient than existing malicious node detection mechanisms.

KEYWORDS: Vehicular Ad Hoc Network (VANET), Mobile Ad Hoc Networks (MANETs), Cooperative Bait Detection Scheme (CBDS), Dynamic Source Routing (DSR), Hybrid Defence, Proactive Defence, Reactive Defence, Reverse Tracing.

I. INTRODUCTION

MANET is a Wireless Mobile Ad Hoc Networks having a collection of mobile nodes which are Some Times acts as Router While Routing during Communication.Nodes in MANET Are Free flow elements of a Network. MANET is a Wireless Ad Hoc Network Known as a mesh mobile network. MANET, WSN & Wireless Mesh Network are Ad Hoc Network with Infra-structured Based or infra-structure less Wireless Type of Network.

VANET is a Vehicular ad hoc network same as MANET but In VANET nodes are in the form of Vehicles. The main idea behind VANET is to communicate among vehicles on the Urban or Village area Roads. Several research projects have focused on this interesting and useful area in order to implement it in the best possible way. Currently huge scope available in this area for researcher.VANET consist of a number of On-Board Units (OBU) which are located inside the vehicles and a number of Road-Side Units (RSU) which form the infrastructure of the network. VANET Communication in VANET is divided into different categories:

1. Vehicle-to-Vehicle (V2V) Communication (Inter-vehicular Communication)
2. Vehicle-to-Infrastructure(V2I)Communication,
3. Inter-Road Side Communication.

The goal of VANET's is to enhance vehicles, passenger's safety along with comfort by distributing traffic, road andweather conditions among nearby vehicles on the road of respective area.

VANET havemany challenging research issues such as data sharing, security issue, Communication media, Network establishment etc. which are caused Due to high mobility and unreliable channel condition with wireless Ad hoc Network. Various applications of VANET must be protected from intruder because compromising VANET applications like safety applications are directly related loss of human life or network damage. A vehicular Adhoc network can be affected by Active and Passive security attacks like DOS (Denial of service attack), message suppression attack and timing attack, Sybil attack, BlackHole attacks, Wormhole attacks, etc. Malicious vehicles on Road May disturb the VANET Communication Network during routing process.

The lack of any infrastructure added with the dynamic topology feature of VANETs make these networks highly vulnerable to various routing attacks. Among number of attacks Blackhole and Grayhole attacks known as variants of Blackhole attacks. These type of attacks are active type of attacks which are possible due to insider attacker within the VANET Network.

A. *BlackHole attacks on VANET Communication:*

BlackHole attack is one type of active insider Attack on availability of VANET.Blackhole Attacks also known as **packet drop attack.**In black hole area where the network traffic is redirected due to active insider attackers within Network or packet dropping occurs. In this case, malicious node receives message for its neighbour which to be forwarded to next hop within the network. But due to internal active malicious behaviour of vehicle, the message to be forwarded is get lost within network. Which cause data loss & leakage within network.

Blackhole attacks are divided as per number of Blackhole nodes available in the VANET Network. Classification as follows:

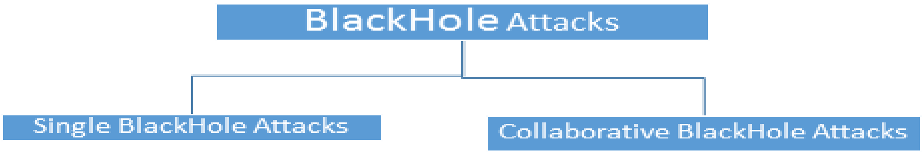

Fig.1.Classification of Blackhole Attack.

1) *Single Blackhole attacks:*

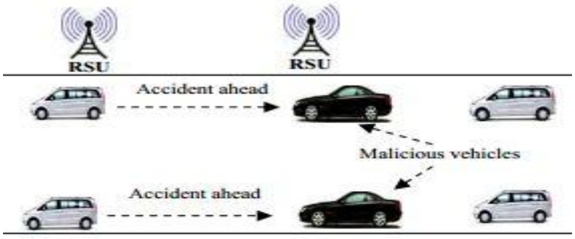

Fig.2.Blackhole Attack in VANET[4]

A malicious node transmits a malicious broadcast informing that it has the shortest path to the destinationand indicates that packet should route through this node after transmitting the fake routing information. The impact of this attack is that the malicious node can either drop or misuse the intercepted packets without forwarding them to Neighbour vehicle. Figure 2 shows a Black Hole attack where a Black Hole region is created by a number of malicious vehicles & they refuse or denial to broadcast the received messages from the legal vehicles to the other legitimate vehicles. This type of attacks also known as Simple Blackhole attack with only one malicious Vehicle in the path.

2) *Collaborative Blackhole attacks:*

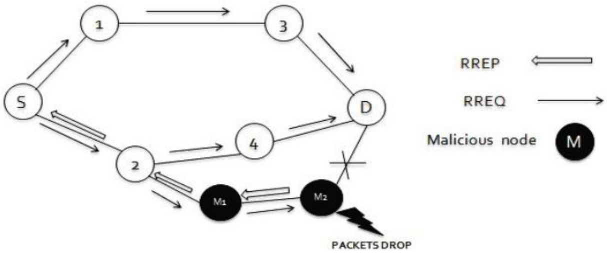

Fig.3.Collaborative Blackhole Attack in VANET [1][2]

Collaborative Black hole attack is a Variant of Blackhole attack with two or more black hole vehicles. In this type of black hole attack malicious nodes work in teams. This type of Blackhole attack is more serious and hazardous than Simple Blackhole attack in VANET due to its cooperative nature of attack. This is an attack done by insider which cause active attack. Fig 3 shows collaborative black hole attack.

When two or more malicious nodes works as a group, the damage can be even worse. In this paper we are trying to mitigate this type of attack by using proposed scheme.

B. *Gray hole attack on VANET:*

Grayhole attack is one type of Active Attack on availability and also known as a variation of Black Hole attack. The malicious vehicle is not initially recognized as Malicious since it turns malicious after elapsed time during VANET communication. It then selectively discards/forwards the data packets when packets go through such a node. Grayhole attack is also insider active attack.

Our focal point in this survey Paper is to trash out the saviour security issues related to VANET. basic requirement and challenges to design to fail safe and secure framework, and we will also discuss the solution presented to solve these challenges and requirements for mitigating Blackhole attacks, Collaborative Blackhole attacks and Grayhole attack. In The Recent years many research works have been focused on the security ofVANETs. Most of them deal with prevention and detectionapproaches to combat individual misbehaving nodes.[1]

Section 2 Explains about Detection & prevention approaches available for MANET and VANET. Section 3 will have brief literature survey on previously existing Detection and prevention scheme for mitigating against collaborative Blackhole attacks &grayhole attacks. Section 4 proposes a new Hybrid Defence mechanism which is known as Cooperative Bait Detection Scheme (CBDS) for VANET.

II. Related work

Many of the researchers have investigated the problem in Detection of malicious node in MANETs. Mainly these solutions deal with the detection of a single malicious node or require huge resource, which in turn High Network Overhead in terms of time and cost for detecting cooperative Blackhole attacks.Defending against Simple Blackhole attack is easier in MANET than Detection and mitigating Collaborative attacks.

Our literature survey is based on Variant of Blackhole attacks detection and prevention mechanism, by using Various Malicious Detection Scheme available in VANET.

A. *Intrusion Detection Schemes:*

Detection mechanisms are grouped into two broad categories:

1) Proactive Defense/Detection Scheme
2) Reactive Defense/Detection Scheme[1] [2]

1) Proactive Detection Scheme

Proactive detection schemes are schemes that need to constantly, continuously, regularly detect or monitor nearby neighbour nodes. In these schemes, due to the availability of malicious nodes, the overhead of detection is constantly created, and the resource used for detection is constantly wasted which causes Network overhead. However, one of the advantages of these types of schemes is that it can help in preventing or avoiding an attack in its initial stage during VANET Communications. So this type of Malicious Node Detection is known as Proactive Detection.

Literature Survey Explains Several Proactive detection schemes available in MANET.

2) Reactive Detection Scheme

Reactive Detection schemes Used as per demand only when the destination node/vehicle detects a significant loss in the packet delivery ratio (PDR). In literature survey of this paper Reactive Detection schemes also reviewed along with Previously Existing Detection Schemes.

B. *Routing Mechanism:*

In MANET and VANET For data routing for VANET Communication Various Routing Protocols are available such as:

1) Proactive Routing Protocols,
2) Reactive Routing Protocols,
3) Hybrid Routing Protocols [6].

Our focus in this paper is related to DSR-Based routing which is Reactive Routing Protocol. There are few DSR-Based Proactive and Reactive schemes available such as DSR, 2ACK, BFTR, DCBA, DBA-DSR, BDSR, REAct, etc.

III. LITERATURE SURVEY

We had Brief Survey on existing intrusion detection schemes available for Detection of Single Blackhole attacks & Collaborative Blackhole attacks. This Survey includes Detection schemes Based on Proactive Defense, Reactive Defense and Hybrid Defense.

Table 1. Existing Detection Schemes

Current System	Description
A watchdog and pathrater scheme(2000)[3][8]	This system detect malicious nodes present in a MANET by using **Proactive Detection** Scheme.
CONFIDANT: Cooperation of Nodes, Fairness In Dynamic ad-hoc Networks(2002)[3]	In this system they have studied routing scheme to avoid blackhole attack in MANETs with Trust Manager.
Resource-EcientACcounTability(REAct) Scheme based on Random Audits [3][9] William Kozma Jr.et al.(2009)	This paper propose a **reactive** misbehaviour **detection** scheme REAct. It is designed for non-cooperative black hole attack only.
Bait DSR (BDSR) based on Hybrid Routing Scheme Proposed by Po-Chun Tsouet al. (2011)[3]	It design a novel solution named Bait DSR (BDSR) scheme to prevent the collaborative black hole attacks using proactive and reactive method to form a **hybrid Detection** based on the **DSR** on-demand routing.
A novel scheme for Detecting Blackhole Attacks in MANETs (so-called DBA-DSR) is introduced in Year 2012[3]	In this paper new protocol designed to identify and isolate the blackhole nodes present in the MANET. This protocol is a modified version of **DSR**
Mitigating Collaborative Blackhole Attacks On DSR-Based MANET(2013)[3][10]	This paper Introduces a new modified version of **DSR** Protocol Known as **DCBA**, Which is combination of Modified DSR and BDSR Protocol. For detection of collaborative blackhole attacks in MANET.[10]
An Acknowledgement based approach for the detection of routing misbehaviour in MANET's (2007)[1]	Liuetal.proposed a 2ACK scheme for the detection of routing misbehaviour in MANETs with two-hop acknowledgement packets. **2ACK** is a **proactive Defence Scheme.**
Providing fault-tolerant adhoc routing service in adversarial environments(2004)[1]	This paper introduced a prevention mechanism called best-effort fault-tolerant routing (**BFTR**). BFTR scheme uses end-to-end acknowledgements which uses **Reactive Defence Scheme**.

V. PROPOSED ALGORITHMS

The goal of this Survey paper is to propose a new Intrusion detection Scheme for Securing VANET Communication. The propose a detection scheme called the cooperative bait detection scheme (CBDS), which aims at detecting and preventing malicious nodes effects grayhole/collaborative blackhole attacks in MANETs. We are trying to Use same Technique in VANET against malicious nodes launching grayhole/collaborative blackhole attacks**.** CBDS is DSR-based Routing mechanism along with Hybrid Detection scheme as a Combination ofPractive and Reactive

Defence Schemes. Using CBDS We are trying to avoid internal active attacks such as collaborative blackhole and grayhole attacks.

A. *Proposed Algorithms:*

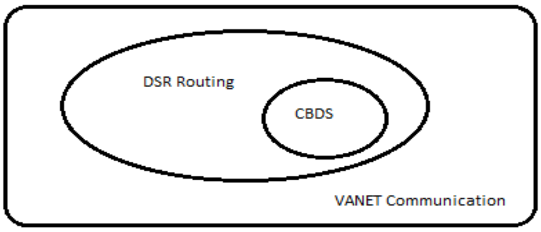

Fig. Proposed Hybrid Detection scheme with DSR In VANET

Proposed Detection scheme is DSR-Based Routing Mechanism with Hybrid Defence Scheme For detection of Malicious Vehicles for mitigating Effects of Collaborative Blackhole and grayhole Attacks.

B. *DSR Routing Mechanism:*

Dynamic Source Routing Mechanism is Reactive Routing Scheme for VANET Communication between Vehicular Nodes of V2V Communication Protocol. DSR involves two steps:

1. Route Discovery
2. Route Maintenance. [1][2][10]

C. *CBDS: Co-operative Bait Detection*

Proposed CBDS scheme merges the advantage of proactive detection at the initial step and the reactive response detection at the later steps in order to reduce the resource wastage& increasing efficiency. [1]

The CBDS scheme includes combination of three steps:

1. **the initial bait step;**
2. **the initial reverse tracing step; and**
3. **Reactive defense step**, i.e., the DSR route discovery startprocess. [1] [2]

The first two steps are initial proactive defence steps (Pro-active Detection),whereas the third step is a reactive defence step (Reactive Detection).

1) Initial Bait Step:

The aim of this phase is to force the malicious node or vehicle to send a reply RREP By sending Bait Request RREQ'. This can be achieved by generating the address of bait RREQ' which is the address of neighbour node selected randomly within sources one hop-node. This phase is divided into two steps as:

a. **Bait Phase**: this is activated when bait RREQ' is used for initial Routing. And waiting for Reply.
b. **Bait analysis**: after Bait phase initiated Bait Analysis Is done in two scenario first, when Vr vehicle node is malicious which cause Blackhole attack & secondly When Vr node of VANET Had not having Blackhole node.

Case 1:- When Vr Vehicle node is not Malicious

When neighbour node Vr is not a malicious Vehicle this means it not launches Blackhole attack then, When source node Sent Bait RREQ'. Other vehicles in addition to Vr Reply's RREP which means there is Malicious or Blackhole Vehicle Node Exist in Routing Path. So Reverse Tracing is initiated for Detecting Variants of Blackhole Nodes which is Next Step of this phase.

If only Vrneighbour node sent RREP, It shows that there are no Malicious Vehicle Available in the Network which then initiate The Route Discovery Process of DSR Routing Protocol.

Case 2:- When Vr node is a malicious

In this case when source vehicle sent bait RREQ', the other vehicle nodes along with Vr sent RREP, which indicate that malicious vehicle exist within routing path. Then reverse tracing initiated for detection of variants of Blackhole attacking nodes as explained in next step.

When Vr not replying RREP deliberately then that Vr Vehicle node directly listed as malicious Blackhole Node which is entered or listed in Blackhole list By Source Vehicle.

When only The Vr node sent RREP, Which conclude that there is no malicious vehicle in network & then Route discovery process started.

2) Reverse Tracing Technique:

Reverse tracing is used to detect the behavior of Malicious vehicle Via Reply to the Bait RREQ' Message. Reverse tracing is done to find:

a. **The dubious path information 'S'**&
b. **The temporary trusted zone "T"**.

If Malicious Vehicle has received the Bait RREQ', Then malicious Vehicle sent False or Wrong Reply RREP (i.e. False RREP).then Reverse tracing operation is performed as shown in figure for vehicular node which receives RREP to achieve Above goal of Reverse tracing.

Reverse tracing operation can be done as follows:

i. When any malicious vehicle Vm, Replies with False RREP i.e FRREP, then the **address list P** is recorded in the RREP as follows:

$$\mathbf{P} = \{\mathbf{V1}, \mathbf{V2}, \dots\dots\dots, \mathbf{Vk}, \dots\dots.\mathbf{Vm}, \dots\dots\dots.\mathbf{Vr}\}$$

ii. If the intermediate vehicular node Vk receives the RREP, then that node will separate the address list P by the destination address V1 of the RREP in the IP field & address list Kk is generated with route information from source vehicle V1 to destination vehicle Vk as:

$$\mathrm{Kk} = \{\mathrm{V1}, \dots\dots\dots, \mathrm{Vk}\}$$

iii. Then the node Vk determines the difference between two Address list generated as :

$$\mathrm{Kk}' = \mathrm{P} - \mathrm{Kk}$$
$$\mathrm{Kk}' = \{\mathrm{V1}, \dots\dots, \mathrm{Vk}, \dots..\mathrm{Vm}, \dots\dots\dots\mathrm{Vr}\} - \{\mathrm{V1}, \dots..,\mathrm{Vk}\}$$
$$\mathrm{Kk}' = \{\mathrm{Vk}+1, \dots\dots, \mathrm{Vm}, \dots..\mathrm{Vr}\}$$

The operation result Kk' is stored in the RREP's "Reserved field" and then source node receive the RREP and the address list Kk' of Vk nodes that received the RREP.

iv. If intermediate node Vk received the RREP ,it will compare following :
   1. The source address in the IP fields of the RREP;
   2. The next hop of intermediate node Vk in the address list P = {V1,…….,Vk,…..Vm,……,Vr};
   3. One hop of Vk.

If The Source address in RREP is matches with Next hop of Vk and One Hop of Vk, then the received Kk' can perform a forward back. Else Vk should forward back the Kk' that was produced by itself.

v. The malicious vehicle generates the dubious path information S i.e intersection set of Kk' as :

$$\boldsymbol{S} = \boldsymbol{K1}' \cap \boldsymbol{K2}' \cap \boldsymbol{K3}' \cap \dots.\cap \boldsymbol{Kk}'.$$

Then The Source Vehicle Node Obtain this dubious path information set S.

vi. Then Source node Obtains The Temporarily Trusted Set T as :

$$\boldsymbol{T} = \boldsymbol{P} - \boldsymbol{S}.$$

vii. Malicious vehicles may present in set S, to detect them the source vehicle send the test packets to this route with recheck message to the second node towards the last node in The Temporarily Trusted Set T. this confirms that vehicle node entered is in a promiscuous mode. This detected vehicle information is sent to the source vehicle node which stores information related to malicious vehicle in the Blackhole list & sent the alarm packets within network to inform other Vehicles that this Vehicle is malicious and terminate the operations with this node. To push off this vehicle from Communication network to provide security to network.

viii. If the last vehicular node discards or dropped the test packet instead of diverting it, then source node Updates information related with this node as a malicious by entering it in to the Blackhole list

In this Way By using Reverse Tracing CBDS Can also detect multiple a malicious Vehicles When Malicious Vehicles Send the reply RREP. We can detect and prevent Collaborative Malicious Nodes. First Two Steps are Proactive Defence Strategy can be applicable To Vehicular Node as Applied to MANET Nodes.

3) *Reactive Defense:*

After Proactive defence now it’s time to initiate the DSR Route Discovery Process Known as Reactive Defence. Now when the route is established & the destination Vehicle detects the drop in Packet delivery ratio (PDR) Then the Detection mechanism i.e. Reverse tracing is performed. Dynamic threshold algorithm is used which is explained in [1].

D. *Working Of CBDS :*

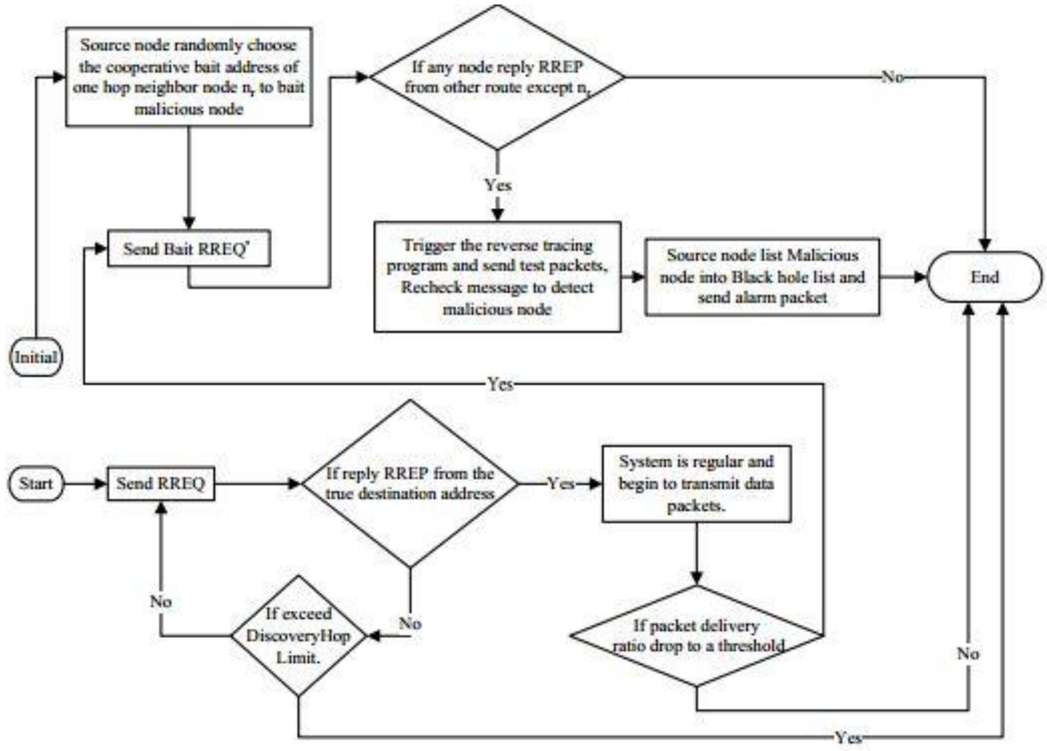
Source node randomly choose the cooperative bait address of one hop neighbor node n_r to bait malicious node
If any node reply RREP from other route except n_r
No
Yes
Send Bait RREQ'
Trigger the reverse tracing program and send test packets, Recheck message to detect malicious node
Source node list Malicious node into Black hole list and send alarm packet
End
Initial
Yes
Start
Send RREQ
If reply RREP from the true destination address
Yes
System is regular and begin to transmit data packets.
No
If exceed DiscoveryHop Limit.
No
If packet delivery ratio drop to a threshold
No
Yes

Fig. Proposed Hybrid Detection scheme with DSR in VANET [1][2]

In this way Collaborative Blackhole and Grayhole attacks which are Variants of Blackhole attacks are detected & mitigates the effect caused due to malicious Vehicles in VANET. Proposed scheme is more secure and efficient intrusion detection scheme for VANET during V2V Communications.

VI. Conclusion & Future Work

Thus in this literature Survey paper we had Introduction and Survey about VANET which is a wireless Ad hoc Network. We also reviewed Proactive and reactive Defence Strategies available for MANET, which we are trying in VANET Communication also as explained in Proposed Algorithm. This paper proposes a new Hybrid Mechanism for defending against Malicious Nodes in VANET Under the collaborative Blackhole attacks &gray Hole attacks, known as Co-Operative Bait Detection Scheme (CBDS) along with DSR Routing. This protocol already used for detecting malicious nodes in MANET, but we can Use CBDS for V2V Type of VANET Communication. Proposed Scheme is secure and efficient along with High Packet Delivery Ratio (PDR) Than Existing Schemes. As CBDS is DSR-Based Routing, End-to-End delay is a slightly more than DSR. CBDS outperform previous Existing DSR-Based Schemes like BDSR, DSR, DBA-DSR, .etc. in terms of Network Throughput AND PDR.

Implementation of Proposed Scheme in VANET poses a great challenge due to its high mobility, frequent link disruption topology & several security attacks. But, the major Loophole of this approaches to implement in VANET is that they are too heavy & expensive to deploy for VANET, we need to Eliminate These Drawbacks by More Future Research Work in this Area. In near future, it is expected that Vehicular ad hoc networks will deploy in different countries Across the Globe including Asian Countries like India.

Also, Our future work related to this paper are (1) we can investigate the feasibility of Using CBDS to detect and defend other types of Collaborative Attacks like Wormhole attacks, Sinkhole attacks, etc. other than Variant of Blackhole Attacks on VANET. (2) We are trying to provide more security to data packet transfer through VANET Communication (i.e V2V) by Integrating CBDS with Other advanced and well-known massage Authentication Schemes like MAC, RSA, and ECDSA for more Secure VANET Communication

REFERENCES

1. Jian-Ming Chang, Po-Chun Tsou, Isaac Woungang, Han-Chieh Chao, and Chin-Feng Lai, "*Defending Against Collaborative Attacks by Malicious Nodes in MANETs: A Cooperative Bait Detection Approach*", IEEE, 1932-8184, 2014.
2. Jian-Ming Chang, Po-Chun Tsou, Isaac Woungang, Han-Chieh Chao, and Chin-Feng Lai, *"CBDS: A Cooperative Bait Detection Scheme to Prevent Malicious Node for MANET Based on Hybrid Defense Architecture",* IEEE, 978-1-4577-0787-2/11, 2011.
3. Isaac Woungang, Sanjay Kumar Dhurandher, RajenderDheerajPeddi , and IssaTraore, " *Mitigating Collaborative Blackhole Attacks on DSR-Based Mobile Ad Hoc Networks* ", Springer-Verlag Berlin Heidelberg, pp [308-323], 2013.
4. VinhHoa LA, Ana Cavalli, *"SECURITY ATTACKS AND SOLUTIONS IN VEHICULAR AD HOC NETWORKS: A SURVEY",* International Journal on Ad Hoc Networking Systems (IJANS) Vol. 4, No. 2, pp [4201-4220], April 2014.
5. Felipe Cunha, AzzedineBoukerche, Leandro Villas, AlineViana, Antonio A. F. Loureiro, "*Data Communication in VANETs: A Survey, Challenges and Applications",*INRIA Saclay. Hal, [Research Report] RR-8498,-00981126 v2, 2014.
6. PriyankaSirola et al., "*An Analytical Study of Routing Attacks in Vehicular Ad-hoc Networks (VANETs)*", International Journal of Computer Science Engineering (IJCSE), ISSN: 2319-7323, Vol. 3 No.04, pp[210-218], Jully 2014.
7. SyedaArshiya Sultana and SamreenBanuKazi,"*Reverse Tracing Scheme to Prevent the Cooperative Attacks in MANETs*", International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE), ISSN: 0976-1353, Volume 14 Issue 2 , pg 338- 344, April 2015.
8. S. Marti, T. J. Giuli, K. Lai, and M. Baker, "*Mitigating routing misbehavior in mobile ad hoc networks*," in Proceedings of the 6thAnnual International Conference on Mobile Computing and Networking (MobiCom), pp. [255-265], 2000.
9. W. Kozma, and L. Lazos, "*REAct: resource-efficient accountability for node misbehavior in ad hoc networks based on random audits,"* inProceedings of the Second ACM Conference on Wireless Network Security (WiSec), pp. [103-110], 2009.
10. Isaac Woungang, Sanjay Kumar Dhurandher, RajenderDheerajPeddi, and Mohammad S. Obaidat, "*Detecting Blackhole Attacks on DSR-based Mobile Ad Hoc Networks* ", IEEE , 978-1-4673-1550, 2012.

BIOGRAPHY

Vipul Suresh Gunjalis a PG Student of Department of Computer Engineering from Sinhgad Academy of Engineering, Kondhwa, SPPU, Maharashtra, India. He Had Completed His Graduation In Computer Engineering From A.V.C.O.E, Sangamner in Year 2013 from UoP. His Research Interest Areas are Network Security & Cryptography, VANET and Image Processing.

Prof Sachin P. Godseis an Assistant Professor with the Dept. of Computer Engineering, SinhgadAcademy of Engineering,Kondhwa, SPPU, Pune, Maharashtra, India. He is Pursuing His Ph. D. He is P.G Project Guide Of main Author of this Survey paper. His Research Areas are WSN, VANET.