DoS Attack Detection in Vehicular Ad-Hoc Network Using Malicious Node Detection Algorithm

Miss S.A. Ghorsad Dr. P. P. Karde Dr. V. M. Thakare Dr. R.V Dharaskar

***Abstract*:- Vehicular ad hoc network (VANET) is known as an essential factor of smart Transportation systems. The key benefit of VANET communication is noticed in dynamic protection systems, which objective to enhance security of travelers by exchanging caution messages between automobiles. Security is also one of the major aspect while message is being communicated in Vanet thus here we have tried to build a secure and reliable framework for Vanet communication which will check the node by MVND algorithm for its malicious state before it enters in a network and we hybrid the VANET with the inexpensive wireless sensor network. Therefore, sensor nodes are deployed along the roadside to sense road conditions, and to store and forward information about dangerous conditions to vehicles regardless of the density or connectivity of the VANET thus here we proposed "Vanet WSN system with MVND" which tries to adapt the benefits of both the framework i.e Hybrid Vanet WSN system and MVND Algorithm.**

***Keywords* –VANET- Vehicular Ad-hoc network, MVND – Malicious vehicle node detection algorithm, RSU-Road side units.**

I. INTRODUCTION

Communication protocols or Routing protocols is one of the basic need of Vanet communication. How Vanet should work how it should perform its operation all these steps depends on the type of communication protocol which is used. Each routing protocol have its own advantages and drawbacks. The selection of communication protocol depends mainly on the type of application in which it needs to be used and what services are needed.

Here we have discussed a hybrid VANET with the inexpensive wireless sensor network. Sensor nodes are deployed along the roadside to sense road conditions, and to store and forward information about dangerous conditions to vehicles regardless of the density or connectivity of the VANET. Rechargeable Solar Batteries is used as an additional power resource. Then we have also discussed an Secure and stable Vanet Architecture model which works with MVND algorithm in order to find out malicious node in a network. Radio channel modeling also have an important impact on the performance on Vanet communication protocol which is discussed in detail later and at last we proposed an new methodology i.e ""Dos-attack detection in Vanet using MVND algorithm"

II. BACKGROUND

Vehicular Ad Hoc Networks should, collect and distribute safety information to massively reduce the number of accidents by warning drivers about the danger before they actually face it. VANET does not give guarantee for timely detection of dangerous road conditions or maintain communication connectivity when the probability of low density of road side units. To overcome this serious problem, the VANET is hybrid with the inexpensive wireless sensor network. Thus sensor nodes are deployed along the roadside to sense road conditions, and to store and forward information about dangerous conditions to vehicles regardless of the density or connectivity of the VANET. Rechargeable Solar Batteries as an additional power resource is used. [1]

Security is one of the main challenges that must be tackled. Another important concern is scalability is a serious issue for a network designer how to maintain stable communication and services in VANET. Thus a more secure and stable cluster scheme for VANETs that uses drop ratio to categorize nodes as malicious is proposed. An entropy-based WCA (EWCA) cluster maintained scheme which can handle the stability of the vehicular network is also proposed.[2]

A key aspect of any wireless system is radio propagation. Radio propagation modelling have a significant impact on the performance of communications techniques in traditional mobile and wireless communication systems and ad-hoc networking systems. [3]

An Attacked Packet Detection Algorithm (APDA) is proposed which is used to detect the DOS (Denial-of-Service) attacks before the verification time. This minimizes the overhead delay for processing and enhances the security in VANET. [6]

An scheme is proposed to enhance the security performances of position-based routing protocols. Like other security solutions, this scheme employs digital signature to guarantee the identity authentication, data integrity and non-repudiation. This mechanism has been proved efficiency and has better security and network performance by comparing with the hybrid signature routing scheme via NS2 simulation.[8]

BUSNet is a virtual mobile backbone infrastructure that is constructed using public buses. The bus nodes isused as the cluster-heads to gather the routing control messages and data packets transmitted among the vehicles. [9]

The use of wireless links renders a vehicular ad-hoc network (VANET) vulnerable to malicious attacks such as Denial of Service, black hole attack, Sybil attack, selective forwarding and altering routing information. [10]

III. PREVIOUS WORK DONE

The objective of CAR 2 CAR communication is to increase road safety and driving efficiency by means of cooperative intelligent transportation systems (ITS), vehicle to vehicle (V2V) and vehicle to infrastructure (V2I) communications.

The CVIS (Cooperative Vehicle-Infrastructure Systems) project deals with intelligent co-operative systems that are based on V2V and V2I communications to achieve

improvements both in the efficiency of the transport systems and in the safety of all road users [1].

Here two different algorithms appropriate for VANET in highway road. First, algorithm have proposed SVWCA as a new vehicular clustering algorithm based on the WCA technique in two part first one for formation of cluster and second for maintain of cluster properly for less overheads. The SVWCA technique primarily focuses on improving the CH duration, membership duration and security and second for maintaining cluster stability as possible. Using SVWCA, communication cost for joining to a new cluster in network decreases because the membership duration for every vehicle has improved. SVWCA be able to enhance network connectivity while selecting cluster-heads. SVWCA make use of disbelieve value in the weighted sum operation. The disbelieve value has been obtained from malicious vehicle node detection (MVND) algorithm [2].

The performance and efficiency of these routing protocols is heavily influenced by the selection process of the neighboring nodes that are candidates to relay the information from source to destination, the density of neighboring nodes, the radio link reliability and the number of relaying nodes needed to send the data packet from the source to the destination node. [3].

IV. EXISTING METHODOLOGIES

- **System and protocol architecture**

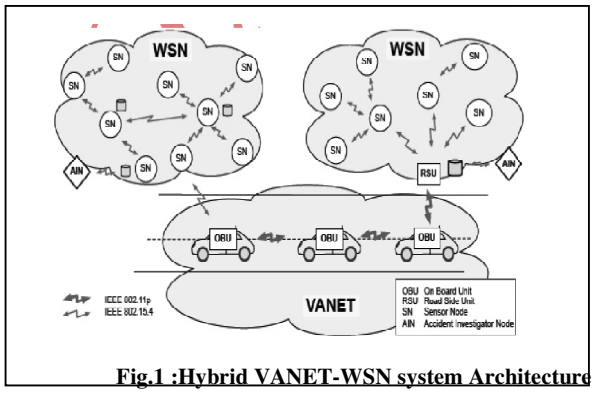

Fig.1 :Hybrid VANET-WSN system Architecture

- **Vanet-wsn communication protocol**

In Hybrid VANET-WSN System, three different types of communication are distinguished; each of them follows specific rules and aims to accomplish a special task, as stated below.

1. Sensors to Sensors communication aim to ensure reliable event detection and fast event report to WSN-Gateway.
2. Inter Vehicle-WSN communication is responsible for timely report of any detected event to the coming vehicles which in their turn send back the received warning messages to other WSN-Gateways on the road to their destinations.
3. Vehicles to Vehicles communication ensures the dissemination of the warning messages gathered from WSN-Gateways to the whole VANET. [1]

Secure and stable vehicular clustering based on weighted clustering algorithm (**SVWCA**) consists of the clustering formation and clustering maintenance phases.

Phase-I: Clustering Formation

Phase-II: Stable Clustering Using Mobility Prediction

- **Malicious vehicles node detection (MVND)Algorithm :**

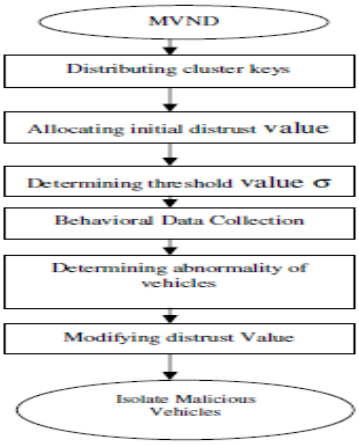

Fig 2 : Flowchart of MMV Algorithm.

- **Behavioral Data Collection**

The behavioral data collection module is responsible for the collection of node behaviors and formation of behavioral data set. A node's behavior is described in terms of the percentage of the amount of behavior for total amount of packets that the vehicle has received, such as PDR (packet drop rate), PMOR (packet modification rate)and PMIR (packet misroute rate). [2]

5. Analysis and discussion

1. **Sensors to sensors communication**

Warning message header shown in Figure 3 is exclusively added by the WSN-Gateway then the intermediate sensors relaying the detector sensor with WSN-Gateway forward a smaller packet format. As a result, the transmission delay and the consumption of energy are decreased.

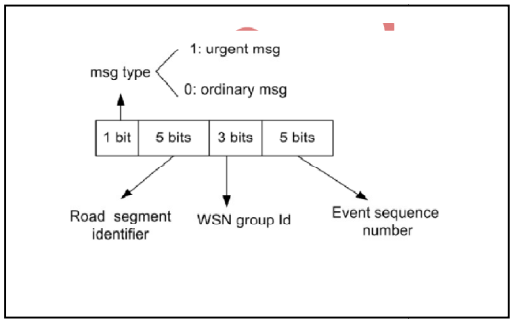

Fig 3 : Warning message's header added by the WSN-Gateway

2. **Vehicle to sensor and sensor to vehicle communication**

In order to decrease the time taken for connection establishment between the WSN-Gateway and the vehicles' cluster head the modification is done in the format of the beacon broadcasted by the cluster head by adding the following fields

A] Its current speed

B] Its Id (identifier)

C] The coordinates of its destination

3. **Vehicle to vehicle (V2V) communication**

The role of V2V communication is to ensure large dissemination of the warning messages. The cluster based routing protocol is used since the vehicles are already

organized in clusters for their communication with WSN-Gateways. [1].

The SVWCA technique primarily focuses on improving the CH duration, membership duration and security and second for

Hybrid Vanet WSN-System	**Secure and stable vehicular clustering based on weighted clustering algotithm (SVWCA)**
Sensor is used in order to detect the environmental condition.	) No such sensor is used.
No threshold value is defined	2) Threshold value is defined Known as disbelieve value in order to detect malicious node.
3) Sensors get activated or get ON an work whenever there is any change in surrounding so as to work in power saving mode	3) Each node has to be detected first in have to work all the time no power saving mode is applied.
4) Warning message is transferred in short time so that reliability is maintained.	4) Security is maintained by detecting the malicious node before the message is passed.

Table 1: Comparison between Hybrid Vanet WSN- system and SVWCA

maintaining cluster stability as possible [2].

The radio channel propagation highly influences the performance and operation of wireless communication systems. The influence can be even more remarkable in vehicular communication networks given the low antenna heights, the highly dynamic network topology and the strict performance requirements established by traffic safety applications. [3].

VI. Proposed Methodology

Here we try to detect the malicious node (node which is creating Dos-attack) in a network with malicious vehicle node detection (MVND) algorithm.

Outcome result possible:

MVND algorithm can be used to detect one of the malicious node in network such as node which is creation dos-attack in a network can be considered as malicious and with the help of MVND algorithm it can be detected easily.

VII. Conclusion

Thus we have tried to build a secure and reliable communication framework so that the malicious node can be detected by MVND algorithm.

References

[1] Pushpender Singh, AmitAshthana, Manik Chandra Pandey, "A Hybrid Vanet-Wsn System For Driving Safety Using Efficient Communication Protocol" ,International Journal Of Advance Research In Science And Engineering (IJARSE),Vol. No.2, Issue No.5,May 2013.

[2] AnkitTemurnikar and Dr.SanjeevSharma,"Secure and Stable VANET Architecture Model" ,International Journal of Computer Science and Network (IJCSN),Vol 2, Issue 1, PP 37- 43, 2013.

[3] Javier Gozalvez, Miguel Sepulcre& Ramon Bauza, "Impact of the radio channel modelling on the performance of VANET communication protocols",Telecommunication system (2012),Vol-50, Issue-3,PP. 149-167,09 december 2010.

[4] Sing B, Hasbullah, H. , "A framework for early detection of incident in dense traffic using vehicular ad-hoc networks"Computer & Information Science (ICCIS), 2012 International Conference on (Vol:2),PP. 777 – 783, 12-14 June 2012.

[5] Srikanth, V. ; Swathi, D. ; Tabassum, M. ; Ramesh Babu, I." Algorithms for dynamic node events and fault tolerance in wireless sensor networks" Wireless, Mobile and Multimedia Networks, 2008. IET International Conference on,PP-235 – 239,11-12 Jan. 2008.

[6] Tzung-Shi Chen,Taiwan, Wen-Hwa Liao,Ming-De Huang , Hua-Wen Tsai," Dynamic object tracking in wireless sensor networks"13th IEEE International Conference, Vo:1 , 16-18 Nov. 2005.

[7] RoselinMary,Maheshwari, M.,Thamaraiselvan, M., "Early detection of DOS attacks in VANET using Attacked Packet Detection Algorithm (APDA)" Information Communication and Embedded Systems (ICICES), 2013 International Conference **,PP.**237 – 240 , 21-22 Feb. 2013.

[8] JieHou ,Lei Han **,**Jiqiang Liu**,** Jia Zhao," Secure and efficient protocol for position-based routing in VANETs" Intelligent Control, Automatic Detection and High-End Equipment (ICADE), 2012 IEEE International Conference on,PP- 142 – 148, 27-29 July 2012.

[9] Tian, Daxin**,**Yunpeng Wang**,** Guangquan Lu**,** Guizhen Yu "A vehicular ad hoc networks intrusion detection system based on BUSNet" Future Computer and Communication (ICFCC), 2010 2nd International Conference, Vol-1, PP-225-229, 21-24 May 2010.

[10] Erritali, M., El Ouahidi, B." A review and classification of various VANET Intrusion Detection Systems"Security Days (JNS3), 2013 National,PP. 1 – 6, 26-27 April 2013**.**

Author Profile's

Dr. V.M. Thakare was born in Wani, Maharashtra in 1962. He was worked as Assistant Professor for 12 Years at Professor Ram Meghe Institute of Technology & Research, Badnera and P.G.Department of Computer Science, S.G.B. Amravati University, Amravati .Currently

he is working as Professor & Head in Computer Science from last9 years, Faculty of Engineering & Technology, Post Graduate Department of Computer Science, SGB Amravati University, Amravati. He has published 110 papers in various National &International Conferences & 30 papers in various International journals. He is working on various bodies of Universities as a chairman & members. He has guided around 400 more students at M.E / MTech, MCA M.S &M.Phil level. He is a research guide for Ph.D. at S.G.B. Amravati University, Amravati. His interest of research is in Computer Architecture, Artificial Intelligence and Robotics, Database and Data warehousing & mining.

Mr. Pravin P. Karde : Received Ph.D. in Computer Science &Engineering from S.G.B. Amravati University, Amravati in the year 2012. He has published 25papers in various National & International conferences & 10 papers in International journals. He is a Board of studies member of University for Computer Sci Engg. Discipline. He is a research

guide for Ph.D. at S.G.B. Amravati University, Amravati. His interest of research is in Computer Architecture, Database and Data warehousing & mining. Network Security.

Dr. Rajiv V. Dharaskar is working as Director, MPGI Integrated Campus, Nanded. He is having 27 years of teaching and 19 years of R&D experience in the field of Computers & IT. Professor has authored number of books on Programming Languages and over **226** research papers on computer engineering. He is guiding more than 15 PhD research scholars on various subjects like Digital Forensics / Cyber Security, Software / Usability Engineering, HCI, Mobile Computing, E-Commerce, E-Learning etc. He has delivered numerous Keynote addresses at international conferences and serves on several International advisory boards. He is on editorial or review board of prestigious International Journals and worked as a Reviewer for dozens of International Conferences.

Ms. Seema A. Ghorsad was born in Amravati (Maharashtra) India on 24th December 1988. **She** receives the B.E. degree in Computer Science and Engg from H.V.P.M's College of Engineering & Technology Amravati in 2011. She is presently pursuing M.E from Sant Gadge Baba Amravati University, Computer Science Department, Amravati. Her area of research is Vehicle adhoc Network(VANET), Database and Operating System.