International Journal of Enhanced Research in Management & Computer Applications, ISSN: 2319-7471
Vol. 3 Issue 4, April-2014, pp: (13-17), Impact Factor: 1.147, Available online at: www.erpublications.com

Detection of Attack through Data Consistency in VANET

Shivani Aggarwal[1], Arun Malik[2]
[1]M. Tech. (CSE), Lovely Professional University, Punjab, India
[2]Asst. Professor, Lovely Professional University, Punjab, India

Abstract: Today's VANET has taken a lot of space in our routine life. Due to which there are attacks happening in today's life. This research paper is telling about the attacks happening in daily life. Data Consistency has a great role in detecting the attacks.

INTRODUCTION

Vehicles are the important part of the human life. Now-a-days Industries are performing most of work on the VANETs to improve the safety on the roads. Industries are also making VANET popular in the information and entertainment applications. A VANET is made by equipping vehicles with a unit named as on-board unit (OBU). With the help of OBU, one vehicle can communicate with other vehicle by using IEEE 802.11p, developed specially for the VANETs having wireless communication. To communicate between OBUs, VANET research have the units known as the road side units (RSUs).

During recent years, MANET has taken a lot of attention in the research field. Today VANET is becoming popular day by day. It has taken attention towards itself. VANET is used in the real time applications to solve the problems like safety of roads, position verification in day to day life. It is used for the message authentication in the vehicles. VANET is almost like as the MANET, can be say as an application of MANET.

VANET has a great role in the car applications also. Active Research in VANETs is demonstrated by numerous papers in the academic Literature. VANET is the sub type of the MANET.VANET is mostly used there where infrastructure cannot be made. The network is infrastructure less. There is no involvement of network administrator. VANET is used in the wireless networks.

Hundreds of people every year are injured due to the road accidents throughout the country. In today's life there is very difficult to survive for the people without vehicles. If there will be so much vehicles. So there is the possibility of more road accidents. People have less patience. Due to which there are more accidents. To solve this situation VANET is there to solve it. Now1 a days there are many curved roads. VANET is very useful. It also gives the best solution in the of curving roads. From here we can say that how much VANET is helpful in various ways.

During last 20 years, Vehicular Ad Hoc Networks (VANET) has become famous now a days in today's researches efforts, Current solutions to achieve good VANET, to protect the network from attacks still not enough, to reach a target, for manufacturer to get safe life. For getting a strong VANET networks, we will have to use strong security and privacy features and we will have to take challenges of VANET.

RSUs roadside units is used for the linking of nodes to each other. We improve the game theoretic approaches for the application cases having scenarios. We decide to introduce a defensive mechanism for the VANET security with heuristic based ant colony optimization. An experimental evaluation is done to calculate the performance of the proposed defensive mechanism in game theoretic approach using heuristic based.

In this section, it has been described that how the journey has been completed from cellular network to VANETs. There were many stages in the evolution of VANETs. It has moved from cellular network to mobile ad-hoc network, after that from mobile ad-hoc network to VANET.

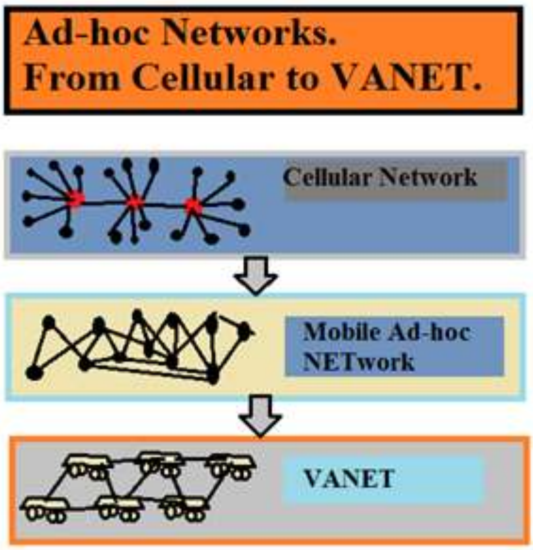

Figure 1: Evolution of VANET

Cellular Network

Firstly, there are cellular network which is made up of the cells. Cellular network is a mobile network which is wireless and distributed among cells. Each has one fixed location cell which is known as transceiver. This location is known as cell site or base station. In this cellular network, to avoid interference, each cell has a different set of frequencies from its neighbouring cells. Over a wide geographic area, these cells provide radio coverage, when these cells are joined together. This gives us a large number of transceivers (eg, mobile phones, pagers etc.) which are portable. These transceivers communicate with each other and also with the fixed transceivers

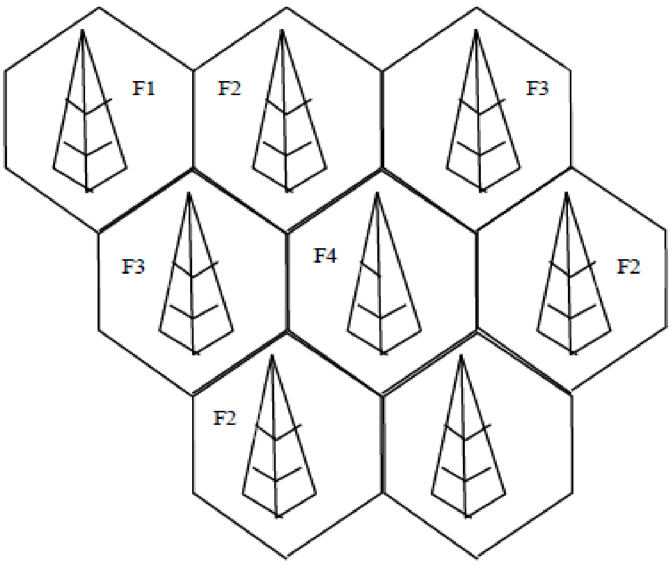

Figure 2: Frequency Reuse Factor

Cellular Network has the following features:

- Same frequency can be used for the multiple links.
- Single Transmitter use more power than mobile devices.
- Single transmitter can use any given frequency.
- Cells can reuse frequency to increase both coverage and capacity.

MANET (Mobile Ad-hoc Network)

MANET is infrastructure less network. It is used in the mobile devices. MANET is a self-configuring network. Each device can move in any direction. These devices move independently and can change their links frequently to other devices. Each device acts as a router and forwards unrelated traffic to its use. MANET has a primary challenge that to maintain the information continuously, MANET is equipping each device continuously required to properly route traffic. These networks are connected to the larger networks.

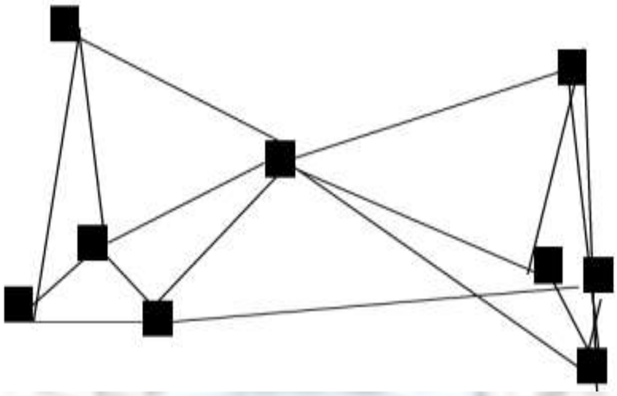

Figure 3: MANETs

MANETS are basically type of wireless ad-hoc network. It has a routable networking environment on the top of the layer. MANETs has become a very popular research due to the growth of the laptops and 802.11/Wi-fi.

Types of MANETSs are:

- VANETs (Vehicular Ad-hoc Networks)
- iMANETs (Internet based Mobile Ad-hoc Networks)
- InVANETs (Intelligent Ad-hoc Networks)

VANETs (Vehicular Ad-hoc Networks)

VANET is known as vehicular ad-hoc network. It uses the mobile nodes (cars) to create a mobile network. VANETS are basically subsets of MANETs. In VANETs, mobile nodes in MANETS, are used as cars or vehicles. These nodes are basically used for the communication between the two vehicles. They connect to an infrastructure to communicate with each other to communicate with each other. These networks have large number of mobile nodes for communication. These nodes are dispersed in roads. There networks' infrastructure is not present in real, it is assumed.

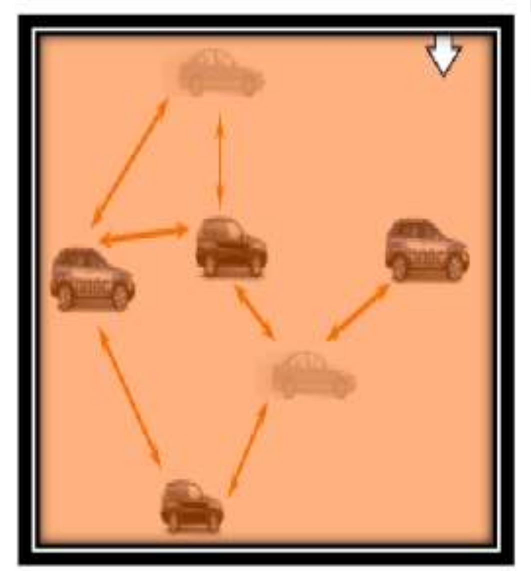

Figure 4: VANET: Communication between vehicles

Present Work

VANET (vehicular Ad hoc Network) is increasing day by day in the research areas having a large number of research cases. These applications contains the safety of the road, enhanced and efficient traffic, edutainment services. To make ultimate disposal successful, it is important that all applications are meet with proper security methods. VANET is unsafe from the attackers. In the vehicle communication network, when one vehicle send the data to another vehicle, then the data can be attacked by the attacker. Then that data can be tampered by the attacker. We will check it through the data consistency. If the data will be tampered by the attacker, data will be inconsistent otherwise the data will be consistent. There are data to be sent from one vehicle to another vehicle. Then that data can be tampered by the attacker. We will check it through the data consistency and the tampered message will not be available.

Conclusion

In this dissertation we have to detect the attack by checking the data consistency in the VANET. In this we have send the data from one node to another node and after that it will check the data consistency. If the data has not been tampered by any attack then the data send is the consistent. The central idea to check the data consistency is to detect the attack. So that we can know that data is not consistent and not allow to open the data. It is not protectable and can spoil the systems or vehicles. The message will send from one vehicle to another vehicle. Then if the data will be tampered then the message will not be protected. Because it will be known that message has been tampered by the attacker In the future, we will work on the data consistency and we will take some parameters to check the consistency. We will see how the parameters like time, energy and cost is effected when there is attack on it.

We will show it with the help of graph by taking the metrics like

- Field size
- MAC
- Fading
- Path loss
- Noise

As a result, data consistency mechanisms that tell about redundancy are limited and taken as probabilistic rather than absolute in nature. We are currently assessing scenarios of colluding attackers, as well as protocols that use conflict detection as a baseline to identify the bad Information in conflict situations.

References

[1]. Jinyuan Sun, Member, IEEE, Xiaoyan Zhu, Chi Zhang, Student Member, IEEE, and Yuguang Fang, Fellow, IEEE," RescueMe: Location-Based Secure and Dependable VANETs for Disaster Rescue", IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, VOL. 29, NO. 3, MARCH 2011

[2]. Osama Abumansoor, Member, IEEE, and Azzedine Boukerche, Senior Member, IEEE," A Secure Cooperative Approach for Nonline-of-Sight Location Verification in VANET",IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, VOL. 61, NO. 1, JANUARY 2012.

[3]. Tansu Alpcan, Member, IEEE, and Sonja Buchegger, Member, IEEE, "Security Games for Vehicular Networks", 280 IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 10, NO. 2, FEBRUARY 2011.

[4]. Stefan Dietzel, Jonathan Petit, Geert Heijenk, and Frank Kargl "Graph-Based Metrics for Insider Attack Detection in VANET Multihop Data Dissemination Protocols" IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, VOL. 62, NO.4, MAY 2013

[5]. Ghassan Samara, Wafaa A.H. Al-Salihy, R. Sures, "Security Issues and Challenges of Vehicular Ad Hoc Networks (VANET)"

[6]. Asif Ali Wagan 1, Bilal Munir Mughal, Halabi Hasbullah3, "VANET Security Framework for Trusted Grouping using TPM Hardware: Group Formation and Message Dissemination" 978-0-7695-3961-4/10 $26.00 © 2010 IEEE DOI 10.1109/ICCSN.2010.115

[7]. Gongjun Yan, Stephan Olariu, and Michele C. Weigle, Old Dominion University, "Providing Location Security in VANETs". IEEE Wireless Communications December 2009

[8]. Tim Leinmuller, DaimlerChrysler AG Elnar Schoch and Frank Kargl, "Position Verification Approaches for VANETs". IEEE Wireless Communications October 2006

[9]. Qin Li, Amizah Malip, Keith M. Martin, Siaw-Lynn Ng, and Jie Zhang, "A Reputation-Based Announcement Scheme for VANETs", IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, VOL. 61, NO. 9, NOVEMBER 2012

[10]. Shi-Jinn Horng, Shiang-Feng Tzeng, Yi Pan, Pingzhi Fan, Senior Member, IEEE, XianWang, Tianrui Li, Senior Member, IEEE, and Muhammad Khurram Khan " b-SPECS+: Batch Verification for Secure Pseudonymous Authentication in VANET" IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 8, NO. 11, NOVEMBER 2013

[11]. Rongxing Lu, Member, IEEE, Xiaodong Lin, Member, IEEE, Tom H. Luan Xiaohui Liang, Student Member, IEEE, and Xuemin (Sherman) Shen, Fellow, IEEE, "Pseudonym Changing at Social Spots: An Effective Strategy for Location Privacy in VANETs", IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, VOL. 61, NO. 1, JANUARY 2012

[12]. Irshad Ahmed Sumra,Iftikhar Ahmad, Halabi Hasbullah Computer and Information Sciences Department, Jamalul-lail bin Ab Manan Advanced Information Security Cluster," Classes of Attacks in VANET",

[13]. Joo-Young Kim, Student Member, IEEE, Donghyun Kim, Student Member, IEEE, Seungjin Lee, Student Member, IEEE, Kwanho Kim, Student Member, IEEE, and Hoi-Jun Yoo, Fellow, IEEE "Visual Image Processing RAM: Memory Architecture with 2-D Data Location Search and Data Consistency Management for a Multicore Object Recognition Processor"` IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS FOR VIDEO TECHNOLOGY, VOL. 20, NO. 4, APRIL 2010.