IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 4, April 2017

A Survey on Novel Framework for Enhancing Security of IoT in Transport Domain

Aakansha Naikare[1], Chaitali Barhate[2], Saili Dhadve[3], Chaitali Deokar[4]

Department of Computer Engineering, Dr. D. Y. Patil Institute of Technology, Savitribai Phule Pune University[1,2,3,4]

Abstract: Today, as the numbers of vehicles are increasing, it results in more traffic congestion and crashes and thus being one of the major issues in developing countries which are to be effectively addressed by improving the current transportation systems, by considering the needs which are necessary of reducing the road traffic congestion and improving road safety. Transport security System is an advanced application which provides web enabled services for transport and traffic system, which results in a safer, coordinated traffic network system. This system can be used very efficiently in network and traffic analysis, which is a spontaneous creation of wireless network of vehicles for exchanging information about on road traffic, for improved traffic and transport management and to enable various users to be sufficiently informed about the road and make safer and smarter decisions on road by using transport networks. As the technology has to be used widely, there is a high need for a low cost traffic analysis technology with high security and QoS. To go for any further developments, a thorough analysis on the available technologies are essential to get a closer view on the current scenario. Proposed system is using android application to send data to server. Server will analyze incoming data for any attacks. Attacks like Brute Force, GPS Spoofing, DDOS attack and message tempering will be detected using this proposed system.

Keywords: GPS Spoofing, DDOS attack, Brute Force attack, Message Tempering.

I. INTRODUCTION

There are several methods are available for secure transportation, Even though these methods make road transportation system better, they are not sufficient to improve the road traffic system to a greater extend or it is unsatisfactory for the current technological world. Today there are many types of hacking takes place to disturb road traffic, due to these types of attacks users will get wrong information about road traffic, Location and speed of traffic. This proposed system is used to detect and avoid attacks from transport network and provide real traffic analysis to the user at all the time.

- Basically this proposed system is used to detect traffic analysis on road, system uses android application for user which send real time data to Server.
- Vehicle to Server communication using Android application. In this mode, a vehicle can receive, transmit or exchange valuable traffic information such as traffic conditions and road accidents with other vehicles.
- Main work is related to Network attacks, System is able to detect and analyze network attacks.
- Proposed system is able to detect following attacks:

a) Detect GPS spoofing
b) Detect and prevent Brute Force attack
c) Detect Message tempering by performing analysis on message sent by user
d) Detect DDOS attack and prevent it.

II. LITERATURE SURVEY

This paper [1] provides a summary of the recent state of the art of VANETs, it presents the communication architecture of VANETs and outlines the privacy and security challenges needs to be overcome to make such safety of networks usable in practice. It identifies all existing security problems in VANETs and classifies them from a cryptographic point of view. It regroups, studies and also compares the various cryptographic schemes that have been separately suggested for VANETs, evaluates the efficiency of proposed solutions and explores some future trends that will shape the research in cryptographic protocols for intelligent transportation systems.

VANET is a type of Ad-hoc network in which movements of nodes are limited along roads. To communicate with each other and with road side units, nodes are equipped with radio devices in VANET. VANET are widely used for safety and comfort applications. Authentication of data is important in this kind of application. So security is one of the important factor in VANET. Different kinds of attacks are there in VANET and different technique is also there to

DOI10.17148/IJARCCE.2017.64172

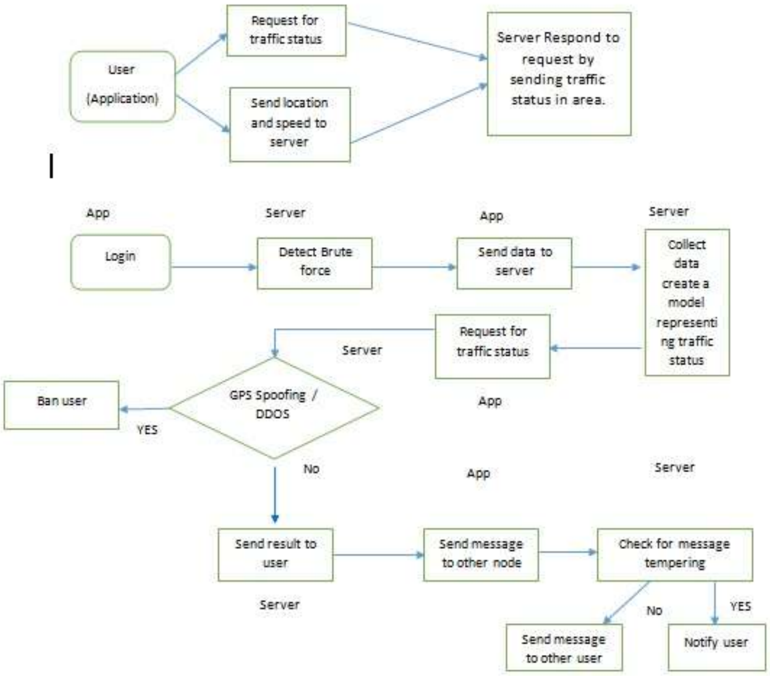
detect and prevent this attack. This paper we will identified attacker using watchdog and apply Bayesian filter to avoid/reduce false positive of node, recognized by watchdog [2].
Intelligent Transport System (ITS) is an advanced application. It provides web enabled services for traffic and transport system, which results in a safer, coordinated traffic network system. ITS is very nicely used in VANET (Vehicular Ad-hoc Network), which is a spontaneous creation of wireless network of vehicles for exchanging information between them, for improved traffic and transport management and to enable various users to be sufficiently informed about the road and make safer and smarter decisions on road by using transport networks. As the technology has to be used widely, there is a high need for a low cost VANET technologies with high security and QoS. To go for any further developments, a thorough analysis on the available technology is essential to get a closer view on the current scenarios. Therefore the result of this study can open doors for a better technologies for future VANETs. This paper considers a few existing technologies such as Vehicular Cloud, CROWN and VANET-Cloud and a comparison on these is carried out [3].
Vehicular ad hoc networks (VANETs), a subset of Mobile Ad hoc Networks (MANETs), refer to a set of smart vehicles used on the road. These vehicles provide communication services among one another or with Road Side Infrastructure (RSU) based on wireless Local Area Network (LAN) technologies. The main benefits of VANETs are that they enhance road safety and vehicle security while protecting drivers' privacy from attacks perpetrated by adversaries. Security is one of the most critical issues related to VANETs since the information transmitted is distributed in an open access environment. VANETs face many challenges. This paper presents a survey of the security issues and the challenges they generate. The various categories of applications in VANETs are introduced, as well as some security requirements, threats and certain architectures are proposed to solve the security problem. Finally, global security architecture for VANETs is proposed [4].
Vehicular Ad hoc Networks (VANETs) have emerged recently as one of the most attractive topics for researchers and automotive industries due to their tremendous potential to improve traffic safety, efficiency and other added services. However, VANETs are themselves vulnerable against attacks that can directly lead to the corruption of networks and then possibly provoke big losses of time, money, and even lives. This paper presents a survey of VANETs attacks and solutions in carefully considering other similar works as well as updating new attacks and categorizing them into different classes[5].
This paper [6] discusses malicious false data injection attacks on the wide area measurement and monitoring system in smart grids. First, methods of constructing sparse stealth attacks are developed for two typical scenarios:
1) random attacks in which arbitrary measurements can be compromised; and 2) targeted attacks in which specified state variables are modified. It is already demonstrated that stealth attacks can always exist if the number of compromised measurements exceeds a certain value. In this paper, it is found that random undetectable attacks can be accomplished by modifying only a much smaller number of measurements than this value. It is well known that protecting the system from malicious attacks can be achieved by making a certain subset of measurements immune to attacks. An efficient greedy search algorithm is then proposed to quickly find this subset of measurements to be protected to defend against stealth attacks. It is shown that this greedy algorithm has almost the same performance as the brute-force method, but without the combinatorial complexity. Third, a robust attack detection method is discussed. The detection method is designed based on the robust principal component analysis problem by introducing element-wise constraints. This method is shown to be able to identify the real measurements, as well as attacks even when only partial observations are collected. The simulations are conducted based on IEEE test systems.

Cloud computing is a network access model that aims to transparently and ubiquitously share a large number of computing resources. These are leased by a service provider to digital customers, usually through the Internet. Due to the increasing number of traffic accidents and dissatisfaction of road users in vehicular networks, the major focus of current solutions provided by intelligent transportation systems is on improving road safety and ensuring passenger comfort. Cloud computing technologies have the potential to improve road safety and travelling experience in ITSs by providing flexible solutions (i.e., alternative routes, synchronization of traffic lights, etc.) needed by various road safety actors such as police, and disaster and emergency services. In order to improve traffic safety and provide computational services to road users, a new cloud computing model called VANET-Cloud applied to vehicular ad hoc networks is proposed. Various transportation services provided by VANET-Cloud are reviewed, and some future research directions are highlighted, including security and privacy, data aggregation, energy efficiency, interoperability, and resource management[7].

III. ARCHITECTURAL DESIGN

In our propose system, user has to register to create an account on the server for traffic analysis. once the user has create his/her account on the server, he/she will be able to login to this smart transportation application. while logging in the application if the user enters wrong id or password, brute force will be detected and the user will be banned for 24 hours same like that of ATM system for security purpose.

DOI10.17148/IJARCCE.2017.64172


User
(Application)
Request for traffic status
Send location and speed to server
Server Respond to request by sending traffic status in area.
App
Server
App
Server
Login
Detect Brute force
Send data to server
Collect data create a model representing traffic status
Request for traffic status
Server
App
Ban user
YES
GPS Spoofing / DDOS
No
App
Server
Send result to user
Send message to other node
Check for message tempering
Server
No
YES
Send message to other user
Notify user

The diagram show the what attacks are taking place and where it is taking place. while logging in the application the server will check for brute force, if brute force is detected then the app will send data to the server. this data is the location and speed details of the users vehicle. the server will then collect this data, create a model representing the traffic status and then the app will send the request for traffic status to the server. now server will check for GPS Spoofing and DDOS attack. if any of these attacks are detected then the server will ban the user if not the server will send the result of traffic status to the app. when the app receives the traffic status it send message to other nodes, here the server the check for message tempering if message tempering is detected then the server will notify it to the user else send message to the user.

IV. CONCLUSION

Proposed system is useful to detect and prevent attacks like Brute force, DDOS, GPS spoofing and message tempering etc. Study and compare the various solutions that have been separately proposed for these attacks and evaluate their efficiency.

ACKNOWLEDGMENT

We would like to express my deepest appreciation to all who provided me the possibility to complete this paper. A special gratitude we give to our project guide Prof. Swati Nilam, whose contribution in stimulating suggestions and encouragement, helped me in writing this paper.

REFERENCES

1. Mohamed Nidhal Mejri a, Jalel Ben-Othman a, Mohamed Hamdi b,"Survey on VANET security challenges and possible cryptographic solutions ", 2014
2. Jay Rupareliyaa , Sunil Vithlanib, Chirag Gohelc," Securing VANET by preventing attacker node using Watchdog and Bayesian Network Theory ",2016
3. Greeshma S Chirayila, Ashly Thomas,"A Study on Cost Effectiveness and Security of VANET Technologies for Future Enhancement ",2016
4. Richard Gilles Engoulou, Martine Bellaïche , Samuel Pierre, Alejandro Quintero, "VANET Security Surveys", 2014
5. Vinh Hoa LA, Ana CAVALLI, ."Security Attacks and Solutions in Vehicular Ad Hoc Networks: A Survey", (IJANS) Vol. 4, No. 2, April 2014
6. Jinping Hao, Robert J. Piechocki, Dritan Kaleshi, Woon Hau Chin and Zhong Fan "Sparse Malicious False Data Injection Attacks and Defense Mechanisms in Smart Grids", IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, VOL. 11, NO. 5, OCTOBER 2015
7. Salim Bitam, Abdelhamid Mellouk, And Sherali Zeadally, "Vanet-Cloud: A Generic Cloud Computing Model For Vehicular Ad Hoc Networks", FEBRUARY 2015
8. Peter Hillmann, Frank Tietze, and Gabi Dreo Rodosek "Tracemax: A Novel Single Packet IP Traceback Strategy for Data-Flow Analysis" 2015
9. Ajay Rawat, Santosh Sharma, Rama Sushil "VANET: SECURITY ATTACKS AND ITS POSSIBLE SOLUTIONS", Volume:3, Issue:1, 2012
10. J.P. Hubaux ; S. Capkun ; Jun Luo, "The security and privacy of smart vehicles" Volume: 2, Issue: 3

DOI10.17148/IJARCCE.2017.64172