ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 3, Issue 8, August 2016

A Study on Different Challenges and Features in VANET

[1] Sindhu Grover [2] Pooja Mittal
[1][2] Department of Computer Science & Applications,
Maharshi Dayanand University, Rohtak, Haryana, India,

Abstract: **-- Vehicular Ad hoc Network (VANET) provides the communication in distributed dynamic environment. Security is the primary issue for any network model. The main purpose of adopting VANET technology is to increase safety and efficiency on roads. The hybrid nature of network exists at multiple levels and different aspects. In this paper, some of major issues in this dynamic network is identified. The network is divided in different communication policies and for each policy, the security threats are identified separately and described in this work. The paper has defined the security attacks with different communication forms are discussed in this paper.**

Index Terms: **— VANET, Security, Intelligent Transportation System, Reliability, Policies.**

I. INTRODUCTION

Vehicular Ad hoc Network (VANET) is most challenging network form identified today as intelligent transportation system. VANET is a subtype of the MANET. It covers multiple applications associated with traffic and vehicle management including packing space management, traffic light controller, vehicle speed monitoring, automated toll management etc. The network is defined in different regions with different specifications. It also requires specialized infrastructure to control the region traffic. Heavy traffic, large number of packet communication, hybridization of technologies and protocols, mobility and dynamic scenario increases the challenges in the network. The communication in this network is present in different forms. These forms include vehicle-to-vehicle communication, vehicle to infrastructure communication and the communication between these infrastructure devices. Each kind of communication requires separate methodology and control mechanism. The major requirement in this network is secure the communicating information even because of high aspects of dynamism. Multicast, broadcast and dedicated communication methods increases the communication challenges. The position awareness and the distribution of this information to authenticated point is required for same safe and secure communication. The paper has explored each and every aspect of privileged security in this network form. Some of security concerns of this network are shown in figure 1. The foremost challenge is because of the heavy network communication.

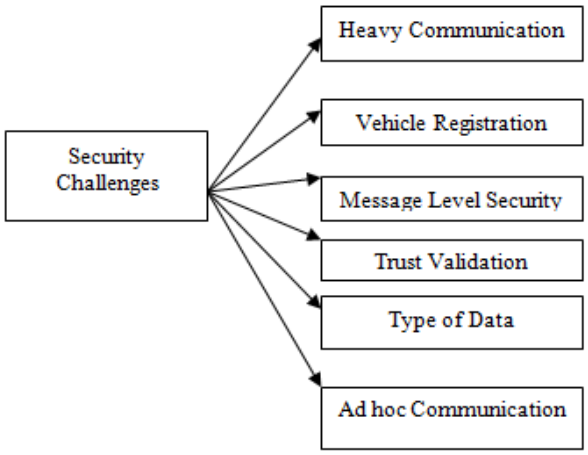

Figure 1: Security Concerns for VANET

Authorization is about to avail the communications, products or the resources based on the profile match as well as to keep safe the information from others. The profile match defines the user level identification to achieve the security. The trust level analysis also comes under the security specification. The trust is analyzed for the customer as well as the vendor. The trust certificates are distributed to proven the trust. The data integrity is the security issue that deals with the data distortion or the error generation in the data communication or the availability. The most concerned issue in the security system is the communication level security. When the data

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 3, Issue 8, August 2016

is being transferred, the issue can be in the form of attacks or the incomplete transaction. The session level security is defined to handle these kinds of problems in VANET system

VANET system is an organized architecture that is defined in several means. One of such effective representation is the communication level based architecture. This architecture is defined with three main communication constraints or the model called V2V, V2I and I2I. The V2V is described as the machine on demand communication that avail the physical resources or the hardware in the form of remote communication to the customer. V2I (Platform-as-a-communication) is defined as the complete application environment by using which the developers can interacted with development software in a shared remote server system. I2I gives the concept of public VANET where an end user can interact to the system in an integrated environment and multiple vendors are available to provide the requested communications.

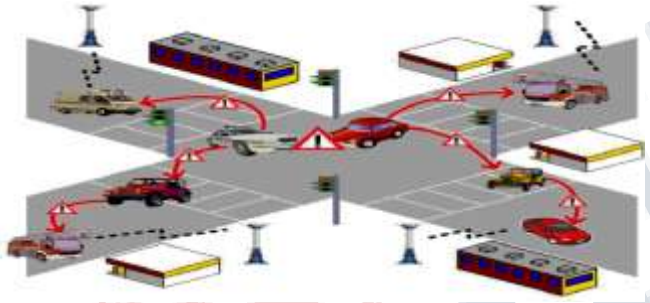

Figure 2: VANET Architecture [1]

In this paper, the security aspects related to the VANET communication model are explained. These aspects include the issues and the relative solutions. In this section, the exploration to the VANET system and its security concerns is defined. This section also explained the VANET communication model. In section 2, the work done by the earlier researchers in the area of VANET system is explained. In section 3, the work VANET communication security models are explained along with issues and the solutions. In section 4, the conclusion of the paper work is described.

II. LITERATURE REVIEW

Lot of work is already done in the area of VANET communication and the Architecture. Some of the earlier work done in same area is presented here. Author has defined a work to reduce the instruction Communication under the dynamic compilers. Author defined a Communication approach under the feedback analysis so that effective allocation will be done. The presented framework is defined to benefit the instruction Communication under multithreaded server application [1]. Author has defined a work on multithreaded Distributed VANET system to perform the dynamic modelling. The paper describes the design under dynamic to evaluate the runtime of pattern mapping.

The another step is to define the regression model to achieve the Communication policy to identify the changing behavior of the threading system. The main objective of author was to define a scalable heuristic approach for estimating the growth of the system count [2]. Author is defined as an analytical model to achieve the task Communication under the analytical modelling. Author estimated the potential aspects under the memory and bandwidth analysis to restrict the number of task. Author implemented the Communication under the real hardware [3]. In year 2013, Author has performed the performance analysis for the functionality analysis under asymmetric platforms. Author has performed the analysis under the heterogeneity under the utility and applicability analysis. Author has defined the work under the workload analysis and defined it under different processes and different configuration for the resource analysis [4].

Author defined the characteristics analysis under the Communication process for multi programmed environments. Author defined a time and space slicing mechanism for the parallel programming and defined the concurrent job execution under single Distributed VANET environment. Author has defined a performance analysis system under the utilization and responsiveness under different computing platform [5]. Another work for the heterogeneous Communication policies for real time multi Distributed VANET system is considered for the multimedia mapping for design space. Author has defined a suitable Communication policy so that system energy can be minimized. The presented framework includes the analysis on energy reduction approaches for dynamic power management [6]. Another work on power management for multi-core architecture for the Architecture is defined for the process estimation under platform evaluation. Author defined the effectiveness and scalability of the system. Author highlighted the scalability limitations for the thread Communication algorithm for small scale multi Distributed VANET system. Author has defined the Communication overhead without loss of accuracy [7]. In Year 2005, Rony Ghattas presented some approach to improve the functionality of the micro Distributed VANET system under the energy and power constraints. This system was defined under low bit system and to enhance the system performance. The main advantage of the system is to reduce the cost and complexity of this new micro Distributed VANET system along with the reduction of power consumption [8].

In Year 2003, Andrei Terechko defined the Communication under the high level language with some

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 3, Issue 8, August 2016

variable definition with global values. Author defined the long range and large impact Transmission for the compiler optimization for local values under the Communication units. The paper has defined three main algorithms for assigning the values to different cluster under the multi pass Communication approach under the variable definition. Author also defined the performance measures for optimizing the algorithm [9]. In Year 2004, Andrew Riffel also defined a multi pass partitioning problem with recursive denominator split along with heuristic algorithm so that the robustness over the approach will be achieved. This paper redefines the MPP as a Communication problem and uses Communication algorithms that allow incremental resource estimation and pass computation in effective time [10]. Another work on improvement over the energy efficiency was presented by Hiroshi Sasaki. The proposed method groups several instructions as a single issue unit and reduces the required number of ports and the size of the structure for dispatch, wakeup, select, and issue. The present paper describes the micro architecture mechanisms and shows evaluation results for energy savings and performance [11]. Flavius Gruian presented an addresses Communication approach for reduced energy of hard real-time tasks with fixed priorities assigned in a rate monotonic or deadline monotonic manner. The approach Author describes can be exclusively implemented in the RTOS. It targets energy consumption reduction by using both on-line and off-line decisions, taken both at task level and at task-set level [12].

Martin Schoeberl perform the investigation on the overhead analysis on object oriented operations. Author also presented the work so that the overhead over the system will be reduced as well as the dispatch and field access will be done effectively. Author presented this work for a real time embedded system. The main objective presented by the author to reduce the hardware cost and to optimize the application output [13]. In Year 2000, Jared Stark presented work on instruction Communication for pipelined processing. Author defined the work to improve the pipelined Communication. Author has defined the technique to eliminate the ability to improve the execution of dependent instruction under the consecutive cycles. The presented approach by the author has defined the frequency check with the sacrifice of IPC [14].

III. SECURE VANET COMMUNICATION MODELS

VANET System architecture is defined under three communication models called V2V, V2I and I2I. These three communication models have their own responsibilities and processes integrated with the application environment. Because of the separate communication model, each model requires different treatment to deal with security issues. In this section, all three communication models are defined with separate security mechanism. These models along with security considerations and specification is given here under

3.1 V2V Security Consideration

V2V is also defined as a utility computing defined as the virtual machine, device or resource that is available to the VANET clients on request. These resources include the infrastructure sharing, memory sharing, hardware and storage sharing. These resources are defined as the resource pool that is connected to the data center to provide the client access in virtual environment. To provide the secure access on these resources, network and the storage communications an effective authentication and secure communication. The V2V model is generally available to the private users under the security state definition. The users can also option the security level to their existing system by using security tools such as security patches, anti-virus etc. This kind of private access is also provides along with secure session specification. The secure session means the access of the resources as the login performed and provides secure access till the user is logged in to the VANET system. The most critical attacks issues associated with this communication model as well as defined security communications or tools are shown in figure 3

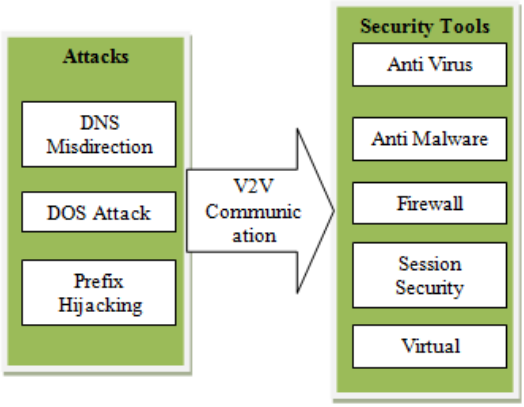

Figure 3: V2V Communication Security Model

As we can see, in figure 3, most critical security issue associated with this communication model is availability. The monitoring and auditing tools are applied on this communication model to avoid the availability risk. The logical to physical system isolation is also performed to avoid the availability problem. This constraint includes the implementation of IPSec, virtual constraints, VLAN components to avail the communication and resource under high degree of reliability.

The storage is the most critical resource provided by V2V. The storage system is connected to the users directly to store the bulk of data over the server by persisting the secure communication and authentication. The storage system includes the abstract definition of storage location, type, storage device etc. The VANET system provides the secure session or tunnel based communication

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 3, Issue 8, August 2016

along with gateway security. Separate protocols are defined on this constraint to achieve the secure communication over the VANET storage system.

These protocols are available on this communication constraint in the form of API. NFS (Network File System) is the most common of these used by any network application. This protocol allows secure file management over the network or distributed system. IPSEC provides the secure communication over the web. When the file uploading or downloading is performed, the authentication check on communicating user is performed using IPSEC. SMB (Server Message Block) allow to provide the secure session or block based communication with VANET system so that effective security will be attained and the secure transmission to the system will be obtained. In short, the resource security is one of the critical vectors that require the authentication as well as communication level security.

3.2 V2I Security Consideration

This model provides the complete development platform or the environment for developers to create, deploy or integrate new applications or the software products in VANET environment. This communication model integrates the development tools and offers the developers to work in a shared environment. It allows multiple remote users to work on a software system in a group. It requires the authenticated information sharing along with specific locks so that the protection as well as sharing will be attained. This model requires the access control mechanism among the developers based on the identity as well as the position in the development group. The security issues and mechanism adapted by these constraints is shown in figure 4.

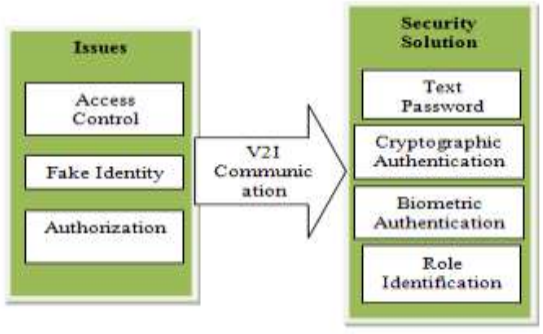

Figure 4: V2I Communication Security Model

As shown in the figure, V2I model is having the major issue associated with identity and the role based security. The different authentication mechanisms are available on this model to attain the security such as biometric password, image passwords, graphical passwords etc. This constraints having the issues related to authorization and authentication.

3.3 I2I Security Consideration

This communication model is the top-most model of VANET communication architecture. This model exists at the application level so that the direct interaction of an end user is to this model. Because of this, I2I Communication model requires the specialized attention in terms of security. This communication constraint is available in public domain so that any user can enter to this communication constraint and perform the communication. This communication is having the integration of two main parties connected based on the communication agreement. These parties are the VANET vendor and the VANET customer. The trust is the most critical vector of this constraints. The trust is defined as the reliability vector for both the vendor as well as customer. Another issue associated with this model is the application integration to the VANET system. The application can be a window application, web application or the mobile application. The android environment is one of the example of such application environment that integrated with VANET system to attain the application level security. The issues and the security solutions associated with this constraint is shown in figure 5.

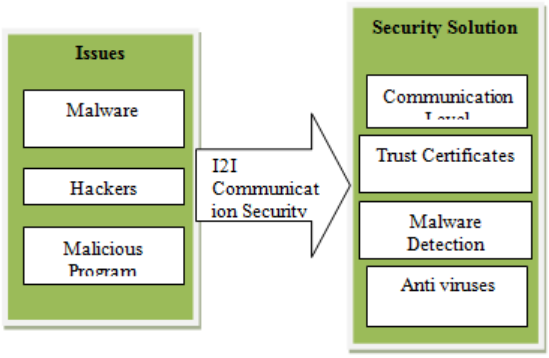

Figure 5: I2I Communication Security Model

Here figure 4 is showing the associated security issue and the security solution to the I2I communication Model. This communication model having the issues because of the public and the direct connection with end customer. The hacking and malware inclusion are the main threats of this constraints. This model provides the security by defining the trust agreement or the communication level agreement between the VANET customer and the communication providers so that the integrated secure communications will be attained.

This section has discussed the security problems and the associated actions defined on different communication models of the VANET architecture so that the relevant precaution as well as action can be taken to secure the information.

IV. CONCLUSION

In this paper, Different challenges associated with different communication forms in VANET are described in detail. An exploration to the VANET communication model and the integrated security aspects is defined. Each model is described respective the security threats and the security solution so that the effective communication gain will be obtained from the VANET system.

REFERENCES

[1] Ayonija Pathre," A Novel Defense Scheme against DDOS Attack in VANET", 978-1-4673-5999-3/13 ©2013 IEEE.

[2] Subir Biswas," DDoS Attack on WAVE-enabled VANET Through Synchronization", Globecom 2012 - Communication and Information System Security Symposium 978-1-4673-0921-9/12 ©2012 IEEE.

[3] Yeongkwun Kim,"A Taxonomy for DOS attacks in VANET", 2014 International Symposium on Communications and Information Technologies (ISCIT) .

[4] S. RoselinMary," Early Detection of DOS Attacks in VANET Using Attacked Packet Detection Algorithm (APDA)".

[5] Abdul Quyoom," A Novel Mechanism of Detection of Denial of Communication Attack (DoS) in VANET using Malicious and Irrelevant Packet Detection Algorithm (MIPDA)", International Conference on Computing, Communication and Automation (ICCCA2015) ISBN:978-1-4799-8890-7/15 ©2015 IEEE.

[6] Usha Devi Gandhi," Request Response Detection Algorithm for Detecting DoS Attack in VANET", 2014 International Conference on Reliability, Optimization and Information Technology -ICROIT 2014, MRIU, India 978-1-4 799-2995-5/14©20 14 IEEE.

[7] Karan Verma," Reference Broadcast Synchronization-Based Prevention to DoS attacks in VANET", 978-1-4799-5173-4/14©2014 IEEE.

[8] Ikechukwu K. Azogu," A New Anti-Jamming Strategy for VANET-Metrics-Directed Security Defense", Globecom 2013 Workshop - Vehicular Network Evolution 978-1-4799-2851-4/13 ©2013IEEE.

[9] Jalel Ben-Othman," Modeling and Verification Tools for jamming attacks in VANETS", Globecom 2014 - Wireless Networking Symposium 978-1-4799-3512-3/14 ©2014 IEEE.

[10] Li He," Mitigating DoS Attacks against Signature-Based Authentication in VANETs", 978-1-4673-0089-6/12 ©2012 IEEE.

[11] Swati Verma," Impact of Gray Hole Attack in VANET", 2015 1st International Conference on Next Generation Computing Technologies (NGCT-2015) 978-1-4673-6809-4/15 ©2015 IEEE.

[12] Sebastian Bittl," Emerging Attacks on VANET Security based on GPS Time Spoofing", 2015 IEEE Conference on Communications and Network Security (CNS) 978-1-4673-7876-5/15 ©2015 IEEE.

[13] Gilles Guette," On the Sybil attack detection in VANET", 1-4244-1455-5/07@ 2007 IEEE.

[14] Irshad Ahmed Sumra," Classes of Attacks in VANET", 978-1-4577-0069-9/11©2011 IEEE.

[15] Mandeep Kaur Saggi," Isolation of Sybil Attack in VANET using Neighboring Information", 978-1-4799-8047-5/15@ 2015 IEEE.

[16] Stefan Dietzel," Context-adaptive Detection of Insider Attacks in VANET Information Dissemination Schemes", 2015 IEEE Vehicular Networking Conference (VNC) 978-1-4673-9411-6/15 ©2015 IEEE.

[17] Irshad Ahmed Sumra," Behavior of Attacker and Some New Possible Attacks in Vehicular Ad hoc Network (VANET)".