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 3, March 2015

Sybil Attack Resistant Cryptographic Traffic Information Dissemination in VuC

Vandana C.P, Nitty Sarah Alex

Assistant Professor, Dept. of Information Science Engineering, New Horizon College of Engineering, Bangalore, India

Senior Assistant Professor, Dept. of Information Science Engineering, New Horizon College of Engineering, Bangalore, India

ABSTRACT: VANET based Cloud has evolved recently from traditional VANET (Vehicular Adhoc Networks) leveraging the power of cloud computing technologies. VANET based Cloud aims at disseminating reliable, accurate traffic information to VANET applications to make the transportation system safe. However, the Adhoc, decentralized nature of VANET, makes them attractive for security attacks. Since VANET is directly related to human lives, security and privacy issues are of paramount importance. Sybil attack is one such network layer attack observed in VANET, which completely disrupts the routing mechanism in network topologies, connections and increases the bandwidth consumption tremendously. This paper proposes AODV based cryptographic approach to disseminate secure traffic information resistant to Sybil attack in VANET.

KEYWORDS: VANET using cloud VuC, Sybil attack, Traffic Information, AODV

I. INTRODUCTION

Vehicular Ad-hoc Network (VANET) [1] is a variation of Mobile Ad hoc Network (MANET) which is defined as a set of moving nodes (vehicles) in a wireless network, with moving vehicles as mobile nodes and Road Side Units (RSUs) as static nodes. The paradigm shift of VANET to VANET based Cloud (VuC) [13] aims as providing rich, safe, reliable and quick transportation services with help of various powerful cloud techniques.

In VANET clouds, vehicular nodes pool their resources and use cloud resources to maintain efficiency in traffic management. Based on the nature of VANET shown in Fig.1, there are three basic architectures of VANET-based clouds[13]: VC (Vehicular Clouds), VuC (Vehicles using Clouds), and HVC (Hybrid Vehicular Clouds). In VANET, vehicles which provide services like Cloud are called Vehicular Cloud while Vehicles which uses Cloud Computing for its working called as Vehicles using Clouds (VuC). VuC is formed by combining VANET which has internet access, storage, on-board computation along with cloud techniques.

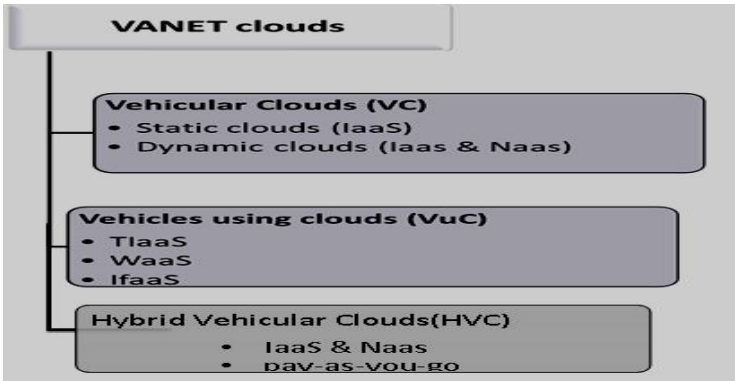

Fig.1 Types of VANET clouds

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 3, March 2015

Cloud computing is a concept based on pay-as-use service which provides on-demand self-service, resource pooling, scalability, location independent online access and many more features. Eg: Usage of electricity in our homes is based on each person needs and at the end of the month we pay exactly for what we have used. VANET-based clouds is due to the emergence of CC (Cloud Computing) in recent some years, as CC has changed the mind set of people when it comes in terms of money and man-work in setting up a company.

VANET clouds have many services which come under the various cloud architectures:
Infrastructure as a Service (IaaS) - The cloud provider provides its VANET nodes with computing, network and storage resources. Some of major CC services are File as a Service (FaaS), Database as a Service (DaaS).
Network as a Service (NaaS) –This service is provided in VANET clouds, as all moving cars do not have internet access. In NaaS, the car with access to internet can offer its excess capacity to the other cars in VANET upon request.
Traffic Information as a Service (TIaaS) – As seen in [14] a VuC framework proposed by Hussain [14] which has Co-operation as a Service(CaaS) with sub-layers TIaas, WaaS & IfaaS. TIaaS provides the vehicular nodes with fine grained traffic information based on their current and near-future locations and their heading.
Warning as a Service (WaaS) - which provides the vehicles with timely warning messages in hazardous situation (eg: ambulance approaching, on-road accidents or traffic jam) along with the necessary security measures that must be taken by the vehicles in specific situations.
Infotainment as a Service (IfaaS) – This is concerned with entertainment delivery to the vehicles through cloud services and is used later in the future.

VANET is formed by high mobility vehicles which are connected to wireless communication devices, GPS and digital maps. It also allows vehicles to connect to Road Side Unit (RSU), which are fixed infrastructure with powerful computing devices so as to support safer and comfortable driving experience. Due to the presence of obstacles (like tall vegetation and buildings) the transmission performance may degrade rapidly. Thus to accomplish an effective transmission range need to maintain by disseminating the traffic information and warning message to the cloud.

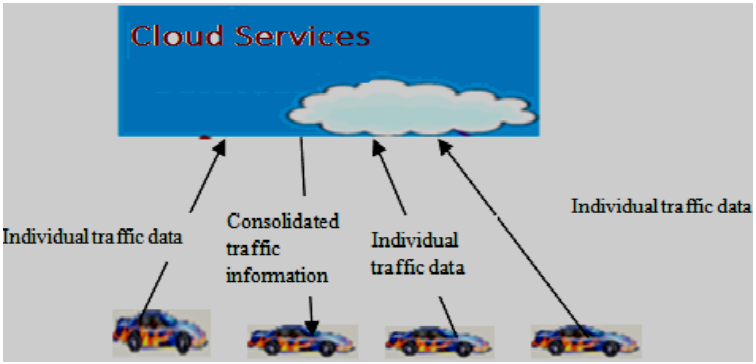

Fig.2 Traffic flow in VuC

As shown in Fig.2, all the individual vehicles in VuC will be transmitting their traffic data periodically to the cloud via the RSU. The cloud will leverage its computing powers to consolidate the individual traffic data to traffic information and disseminate to the vehicles so that the traffic management is smooth and effective.

II. RELATED WORK

In VANET using clouds, which is a type of MANET, in the process of traffic information dissemination which involves mobile nodes, a node can pretend to be more than one node using the identities of other legitimate nodes which is referred as node forging or sybil attack [3][11]. A vehicle in Sybil attack, forges the identities of multiple vehicles which there by can be used to play any type of attack in the system and create illusion (false identities) of presence of additional vehicles on the road. Sybil attack can create every type of attack that can be generated by after spoofing the positions or identities of other nodes in the network. Thus it degrades the integrity of data, security and resource utilization and as well to reduce the effectiveness of fault-tolerant schemes.

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 3, March 2015

The various types of **Sybil attack in VuC architecture** are as follows:

a] Stolen and Fabricated identities:

Stolen identity is that identity which the malicious node takes from the legitimate node and use it to attack. This is unidentifiable to see whether the legitimate node is destroyed. Whereas fabricated identities are that identities that the malicious node takes the exactly from the legitimate node called as identity replication in which same identity is used many times in a network.

b] Simultaneous and Non-Simultaneous Attack:

In simultaneous attack, all the replica nodes participate at the same time by cycling one identity between all nodes. Non simultaneous is one in which the attacker uses the same number of the identities equal to number of devices.

c] Distributed Storage:

Sybil attack creates replica of nodes to store it in several nodes which will affect the architecture.

d] Routing:

Routing will be affected if a node is present in a number of routes with same identity of many malicious nodes.

e] Data Aggregation:

The Sybil nodes act as number of different users, the aggregated data changes completely, as the data is grouped completely into one node and thus false information occurs.

f] Misbehaviour Detection:

As Sybil node uses its virtual identities to increase its credit trust vales and reputation, it will become inaccurate to detect the nature of the malicious node.

g] Fair resource Allocation:

Due to its multiple identities which create multiple virtual identities, Sybil node affects the allocation of the resource and sharing of resources.

Sybil attacks can incur great security threats to VANETs. First, Sybil nodes may cause an illusion of traffic congestion. A greedy driver may convince the neighbouring vehicles that there is considerable congestion ahead, so that they will choose alternate routes and allow the greedy driver a clear path to his/her destination. Second, Sybil nodes may directly or indirectly inject false data into the networks, greatly impacting on the data consistency of the system [15]. For example, VANETs may rely on multiple vehicles voting to generate a traffic status report. However, if some of the voters are Sybil vehicles, the report may be deviated from the fact, depending on the benefits of the malicious. Finally, Sybil node may launch other types attacks such as channel jamming attacks and message suppression attacks.

The various Sybil attack detection mechanisms have been proposed for the VANET are discussed below:

Directional Antenna based approach

Sybil attack detection based on directional antenna [3] verifies the direction of the arrival packets from vehicle units. It checks whether the packet has come from a real neighbour or a forged one. But this approach can't detect attacks in all scenarios in real world.

Propagation Model based approach

In this approach [4] [5] the received signal strength from the sending vehicle unit is measured and is used to compute vehicle nodes position. This position is compared with vehicles claimed position, if not matching Sybil attack is detected. However this approach may fail if the malicious node employs the same radio propagation model to compute the signal strength. However this approach has limited accuracy and requires realistic radio propagation model due to high mobility of vehicle nodes in VANET.

Resource Testing based approach

This technique [6][7][15] is based on the assumption that every physical entity is equipped with limited computational, storage, bandwidth resources. A typical problem is given to all the nodes in the network for testing computational resources. If resources of a single node are used to simulate multiple entities, any particular entity will be resource constrained. This approach is not suitable as a malicious node may have more computational resources when compared with genuine nodes. This approach may in turn generate more traffic in the network leading to congestion.

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 3, March 2015

Detection and localization of nodes based approach

This technique is based on GPS technique [5] [8]. The physical location of nodes is compared its claimed coordinates. It has limited scope and has dependency on GPS technique.

Timestamp Series based approach

In this approach [9], the main assumption is that it would be rare for arbitrary two vehicles to pass through a few different RSUs (far apart from each other) always at the same time. If a message sent out by any vehicle unit contains several timestamps issued to this vehicle by the previously passed RSUs, Sybil attack can be detected if multiple messages contain very similar series of timestamps. It has serious limitations like, if RSU units are located at intersections, it may make the Sybil attack detection difficult.

Public Key Cryptography based approach

In this approach [10,11], public key cryptography and authentication using digital signature and certificates technique is employed. Certificates are issued by Certifying Authority (CA). This At any time, messages with valid certificates are considered, preventing Sybil attack. The only requirement is that each node should be assigned one certificate at a time. For privacy implementation, these certificates are changed from time-to-time.

Existing solutions are also based on ECDSA (Elliptic Curve Digital Signature Algorithm) [15]. The public key is available to all vehicles in VANETs. Both the source and destination nodes are obligated to agree upon the elliptic curve domain parameters. However in VANETs, it is difficult to deploy PKI as there is no guarantee of the presence of infrastructure and is very complex, time and memory consuming procedure.

III. PROPOSED ALGORITHM

A. *Sybil Attack Threat Model:*

Sybil attack is created by creating a false neighbouring presence in the VANET. We have employed Adhoc on Demand Distance Vector Routing (AODV) protocol to simulate the Sybil attack in VANET. AODV, a multihop reactive routing protocol works purely on demand basis. A destination sequence number is utilized to record change in topology and loop free routing in intermediate node. As route discovery is important when a source node wants to communicate with any particular destination in order to forward data packet.

AODV uses route discovery by broadcasting RREQ (Route Request) to all its neighbouring nodes. Once the source node broadcast a RREQ to its neighbours it acquires RREP (Route Response) either from its neighbours or that neighbours rebroadcasts RREQ to their neighbours by increment in the hop counter. If node receives repeated route requests from same broadcast ID, it drops the requests to make the communication loop free. RREQ use multihop to reach to particular destination. If RREP is not received by the source node, it automatically setups reverse path to the source node.

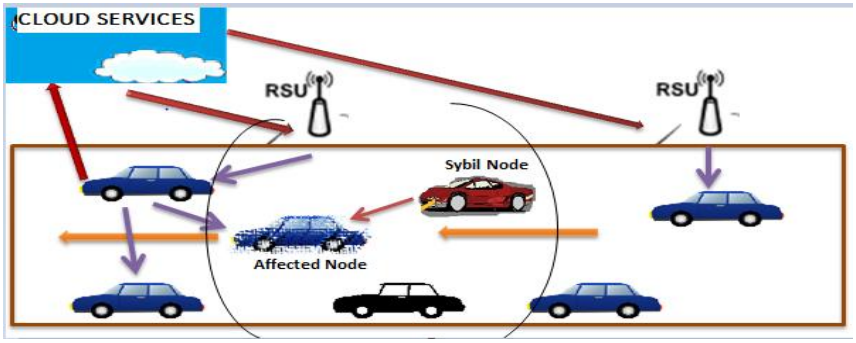

Fig.3 Sybil attack model in VuC

A reverse path is set for a limited period of time only if node keeps the record of its neighbour from which it gets the RREQ. The intermediate nodes stored the particular destination sequence number information to compare it with the RREQ destination sequence number, if in case it is greater than or equal to stored sequence number of the intermediate node then the RREP is generated to source node following the same route from destination node to source node. This method is also known as the forward path discovery by means of two nodes which is used for communication.

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 3, March 2015

B. *Proposed Methodology:*

We propose a cryptographic based approach to prevent Sybil attack in VANET. The communication between vehicular nodes, RSU and cloud infrastructure is encrypted to provide location privacy which cannot be breached by Sybil nodes. The proposed approach mandates that the Sybil nodes should be physically present at the location to get access to the proposed cryptographic technique.

The following are the assumptions made to conclude on the proposed methodology:

- The cloud infrastructure is secure and is not susceptible to internal security attack.
- Each vehicle has a unique vehicle ID (K_v) which is provided at initialization time.
- K_v is readily available to the road side unit RSU.
- Each RSU unit has a fixed transmission range in which it can transmit/receive data with vehicle units.
- The fixed RSU have high speed internet connection to the cloud.

Terms	Meaning
K_v	Unique vehicle id
K_{rand}	Random number generated by RSU
KID	ID for K_{rand} , expires within a lifebound
Message	Individual Traffic data sent by Vehicle units to RSU and from RSU to cloud
Message1	Consolidated Traffic data created by the cloud and sent to RSU and from RSU to Vehicle unit
Ks	Secret key shared between the cloud and the RSUs

Table.1 Notations used in the proposed system

The road side units (RSU) broadcast RREQ named as K_{rand}, a random number generated by the RSU. Along with K_{rand}, a KID unique identification number is sent which is used to check the lifetime of the K_{rand}. KID will be initialized to a value 1 and will be incremented until a configured life bound. This KID will help the RSU to identify the unique K_{rand} sent by it to the same vehicle. During traffic jam, the vehicle may be stuck near the same RSU for more time interval, receiving multiple broadcasted K_{rand}.

In such scenario, the appended KID will help the RSU to retrieve the identity of the K_{rand}. However, the KID will expire within a lifetime. The broadcasted K_{rand} and KID will be received by the vehicle units travelling in the transmission range of the RSU. Vehicle unit will create a new K_{encryt}, which is the XOR of Krand, KID and K_v (the vehicle id provided at initialization time).Using this K_{encryt}, the vehicle units will encrypt the individual traffic information and will send to the RSU unit. If the sender is genuine and locally present, it will possess the valid Krand. Hence the RSU can check the authenticity of the vehicle unit, avoiding Sybil attack.

The RSU unit will maintain a hashmap of the K_{rand} and KID broadcasted by it for a specified life period. Based on the KID the RSU will decide the K_{rand} to choose and generate the $K_{decrypt}$. Same will be used to decrypt the data. This individual traffic data sent from vehicle units will be encrypted using the Ks, secret key shared between RSUs and cloud infrastructure. Cloud will decrypt the Message using Ks and will collate the individual traffic data to construct the consolidated traffic information. This consolidated information will be encrypted using Ks which will be RREP and will be sent to the RSU. The RSU will decrypt the message1 using its secret key Ks. Since the message1 will include the vehicle id, RSU can construct the $K_{decrypt}$. Using $K_{decrypt}$, the Message1 is sent to vehicle units. The purpose of using random number and ID based encryption is to provide location confidentiality against outsiders, remedy message contents manipulation, and to stop outdated messages from lingering around the network.

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 3, March 2015

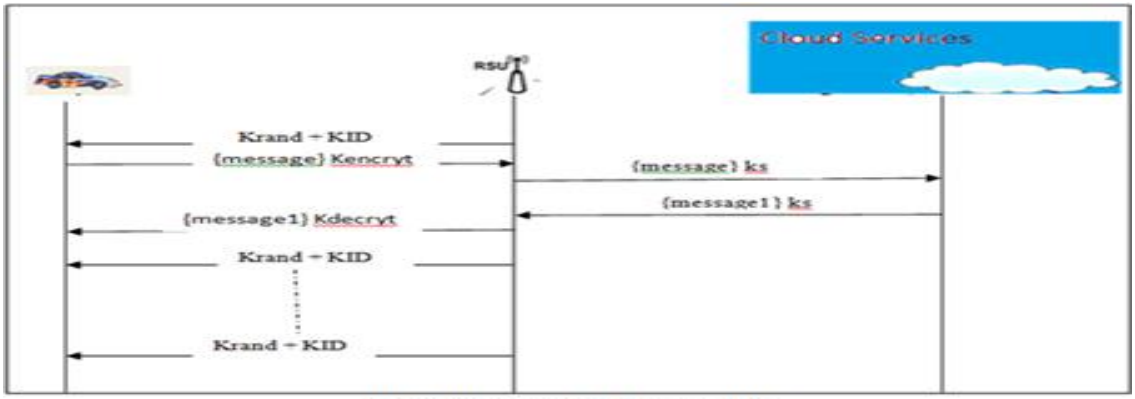

Fig 4.Proposed Approach

IV. SIMULATION RESULTS

The simulation of the cryptographic solution between vehicular nodes and RSUs is carried out using NS2 simulator with 50 vehicular nodes, 5 Sybil nodes and 10 RSU nodes.

A. *Simulation Environment:*

The parameters shown in Table.2 are configured using the simulation tool NS2[12]. MobiSim[12] is used for generating the traffic pattern in VANET.AODV routing protocol is used for communication between vehicular nodes and RSU nodes.

PARAMETER	VALUE
Area	1000 m * 1000m
Simulation Time	250seconds
Number of vehicle nodes	50
Traffic Model	Mobisim
Number of Sybil attackers	5
Number of RSU	10
Routing Protocol	AODV
Mac protocol	802.11a
Data rate	1packet per second
Data Packets	512 bytes/packet

Table.2 Parameters used for simulation

B. *Simulation Result Analysis:*

The Performance of the proposed system is measured in terms of packet delivery ratio and control packet overhead.

Packet delivery ratio: It is measured as the ratio of the total number of packet received at the destination and the total number of packets sent by the source. In **Fig.5**, number of Sybil nodes are 5, RSU nodes are 10 and the number of vehicular nodes are increased from 0 to 50 for different traffic a pattern using MobiSim simulator. It is observed that the PDR becomes stable once the proposed cryptic approach is in place as the location privacy is in place making the drop rate reduced by Sybil nodes.

Control Packet Overhead: Normal AODV control packet overhead is compared with the proposed cryptographic approach on AODV. Since the proposed approach employs broadcast of random number and further encryption process, the control packet computation is necessary. As shown in the **Fig.6**, the control packet overhead is high in the proposed security approach on AODV. But this provides security against Sybil attack.

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 3, March 2015

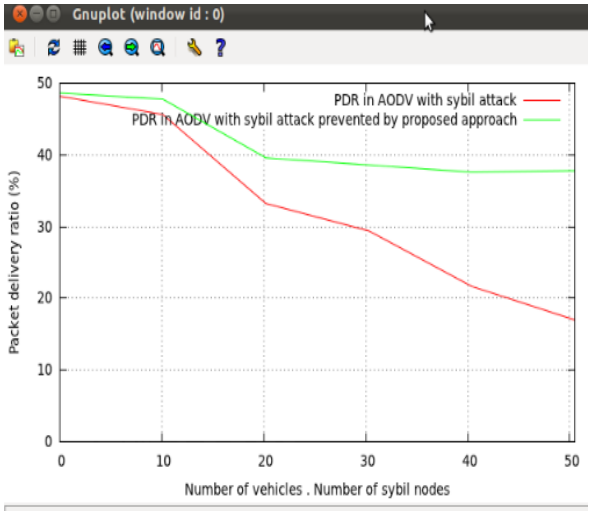

Fig.5 PDR analysis with Sybil attack and proposed approach

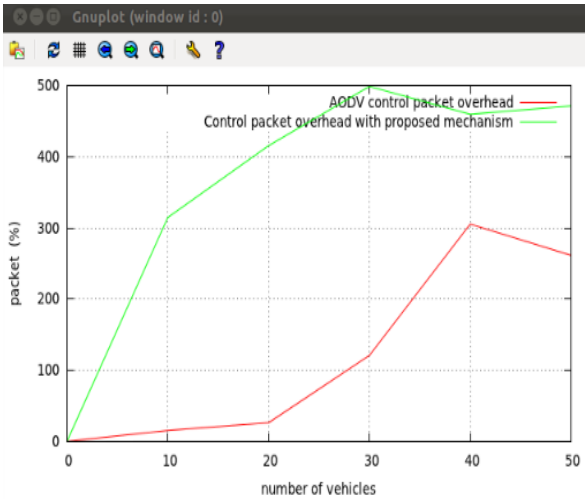

Fig.6 Control packet overhead analysis

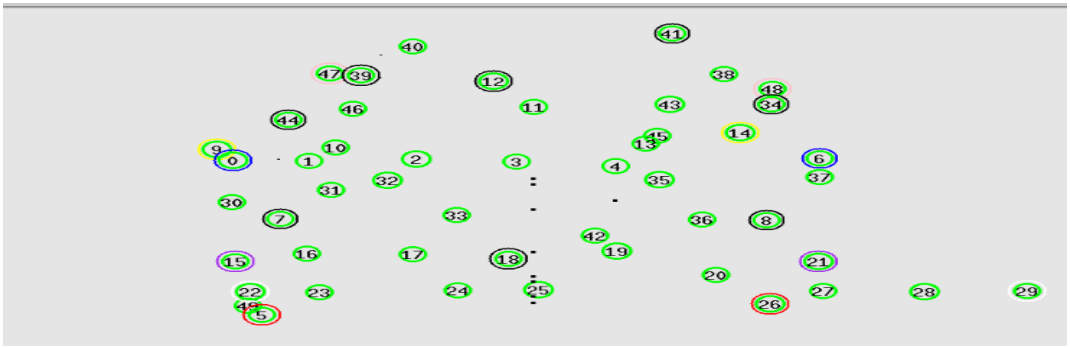

Fig.7 ns2 nam simulating the scenario

The Fig.7 the NS2 network animator is shown depicting the vehicular nodes, RSU nodes and Sybil attacker nodes. Also the storage requirement for RSU is mandatory in the proposed approach since the RSU maintains the mapping for the random number Krand and KID. The data structure used is hashmap which is highly efficient and provides quick access reducing the access time.

V. CONCLUSION AND FUTURE WORK

In this paper, a novel approach to prevent Sybil attack in VANET based cloud is proposed. The cryptographic approach employed between RSUs and Vehicle units is simulated. In future, the cryptographic security between RSU and cloud as proposed in the approach will be simulated and the results of the same will be compared with existing approaches.

REFERENCES

1. C.Sivaram Murthy and B.S Manoj, "Ad Hoc wireless Networks", Pearson Education, 2nd Edition India, 2001.
2. Demirbas, M. and Song.Y, "An RSSI-based scheme for sybil attack detection in wireless sensor networks," Proc. WOWMOM, 2006.
3. B. Xiao, B. Yu, and C. Gao, "Detection and localization of Sybil nodes in VANETs", Proceedings of the Workshop on Dependability Issues in Wireless Ad Hoc Networks and Sensor Networks (DIWANS '06), Los Angeles, CA, USA, pp. 1–8.
4. Erdogan, S. and Hussain, S,"Using received signal strength variation for energy efficient data dissemination in Wireless Sensor Networks", Proc. DEXA workshop, 620-624.

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 3, March 2015

5. S. Goel, M. Robson, M. Polte, and E. G. Sirer. Herbivore, "A Scalable and Efficient Protocol for Anonymous Communication", Technical Report 2003-1890, Cornell University, February 2003
6. G. Yan, S. Olariu, and M. C. Weigle, "Providing VANET security through active position detection", Computer Communications, 31(12), 2883–2897,2008
7. Park S, Aslam B, Turgut D, Zou C.C, "Defense against sybil attack in vehicular ad hoc network based on roadside unit support", MILCOM, pp. 1–7,2009.
8. M. Raya and J.-P. Hubaux, "Securing vehicular ad hoc networks". Journal of Computer Security, 15(1), 39–68.
9. A. Khalili, J. Katz, and W. Arbaugh, "Toward secure key distribution in truly ad-hoc networks", In Proceedings of the IEEE Workshop on Security and Assurance in Ad hoc Networks, in Conjunction with the 2003 International Symposium on Applications and the Internet, Orlando, FL, January 28 2010.
10. H. Fusslur, M. Transier, S. Schnaufer, and W. Effelsberg, "Vehicular ad hoc network:From vision to reality and back", The Fourth IEEE/IFIP Annual Conference on Wireless On demand Network Systems and Services, Vol. 4, 80–83,2007
11. J. Newsome, E. Shi, and D. Song, "The SybilAttack in Sensor Network: Analysis & Defenses," The Third Intl. Symposium on Information Processing in Sensor Networks (IPSN'04), Berkeley, California, USA: CAN Press, pp.185-191,2009
12. Francisco J. Martinez, Chai Keong Toh, Juan-Carlos Cano, Carlos T. Calafate and Pietro Manzoni, "A survey and comparative study of simulators for vehicular ad hoc networks (VANETs)",Wireless Communications and Mobile computing (2009), DOI: 10.1002/wcm.859
13. Md Whaiduzzaman, MehdiSookhak, AbdullahGani ,RajkumarBuyya, A survey on vehicular cloud computing",Journal of Network and Computer Applications, ELSEVIER, 325–344,2014.
14. Rasheed Hussain, Fizza Abbas, Junggab Son, and Heekuck Oh, "TIaaS: Secure Cloud-assisted Traffic Information Dissemination in Vehicular Ad hoc NETworks",13th IEEE/ACM International Symposium on Cluster, Cloud, and Grid Computing,2013.
15. Vinh Hoa LA, Ana CAVALLI, "Security Attacks and solutions in Vehicular Adhoc networks:A Survey", International Journal on AdHoc Networking Systems (IJANS) Vol. 4, No. 2, April 2014.

BIOGRAPHY

Vandana CP is currently working as Assistant Professor in Information Technology Department, New Horizon College of Engineering. She has 6 years of software industry experience in telecom domain mainly on network management systems (NMS) and storage area networks (SAN) domain. Her research interest includes security issues in MANET, network management systems and functionalities. She has done B.Tech in computer Science and M.Tech in Computer Networks.

Nitty Sarah Alex is currently working as Senior Assistant Professor in Information Technology Department, New Horizon College of Engineering. She has total 9 years of teaching experience. Her research interest includes wireless sensor network and cryptography. She has attended various international conference and published several international papers. She completed her Btech and Mtech in computer science.