International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2017 IJSRCSEIT | Volume 2 | Issue 5 | ISSN : 2456-3307

A Survey on Secure Clustering Approaches for VANET

Venkatatamangarao Nampally*1, Dr. M. Raghavender Sharma2, Arun Ananthanarayanan3

*1 *Department of Computer Science, University College of Science, Osmania University, Hyderabad, Telangana, India*
2 *Department of Statistics, University College of Science, Osmania University, Saifabad, Hyderabad, Telangana, India*
3 *Department of Network Systems and Information Technology, University of Madras, Guindy Campus, Chennai, Tamil Nadu, India*

ABSTRACT

Secure achievements are not only reliable data delivery but also the fast authenticity and reliability in security. The invasion of wireless communication technology has revolutionized human lifestyles in providing the most convenience and flexibility over accessing internet services and reliable services offered for privacy and security. Security is an important issue in deployment of ad hoc networks; secure clustering is necessary when there is a time of collecting and aggregating data from other nodes. In order to provide a comprehensive understanding of security techniques, which designed for VANETs and pave the way for the further research, a survey of the secure clustering techniques are discussed in detail in this paper.

Keywords: Invasion, Security, VANET, Cryptographic, Simulation and RHCN.

I. INTRODUCTION

VANET is a term used to describe the spontaneous Ad hoc network formed over vehicles moving on the roadside. The challenges in VANET are located especially in the aspects of security and privacy. To prevent unauthorized access to a service fabric cluster, one must secure the cluster. A group of VANET nodes within a radio range can form a cluster environment. In general, Clustering is a mechanism of grouping of vehicles based upon some predefined metrics such as density, velocity, and geographical locations of the vehicles to delivery of the efficient data in VANETs and securing a cluster means that to apply secure protocols and actions on the clusters that it is not exposed to any attacker, malware etc. In particular, clustering main goal is to categorize data into clusters such that objects fall into groups in the same cluster. Security is especially important when the cluster runs production workloads. Nodes present in the clusters will work more efficiently and the message passing within the nodes get more authentication from the cluster heads. Securing actually belongs to the robustness of the system to certain attacks. Vehicular Ad hoc networks (VANETs) are a kind of mobile Ad hoc network developed to enhance traffic safety and provide comfort applications to drivers as well as passengers. Each node in the cluster structure plays one of three roles: Cluster Head (CH), Cluster Gateway (CG), and Cluster Member (CM). A CH is a leading node of a cluster is responsible to coordinate all CMs in its cluster and is responsible for gathering data from any node of that cluster and sends them to another cluster head. A CG is a border node of a cluster that can communicate nodes belonging to different clusters. A CM does receive data from cluster coordinator CM. In VANET system, we consider two kinds of topology controls: cluster based topology control, and distributed topology control. This article describes how to configure node-to-node and client-to-node security. In order to implement security in VANET system by using clustering approach, symmetric algorithms as well as asymmetric algorithms are used. In a symmetric algorithm there is a shared secret key for both encryption and decryption, whereas in an asymmetric algorithm there is a requirement of secure mapping of public keys with the user's identities using public key infrastructure. PKI is often used in certification where a digitally signed certificate is issued to every authenticated user so that they can get their public key. The onboard units (OBUs) are used in the vehicles to communicate with one other directly or through roadside units (RSUs) located at various points on the road. Hence it becomes essential to provide security services such as authentication, non-repudiation, confidentiality, access control, integrity, and availability. In VANET, system common communication standards are IEEE 802.11p, IEEE1609. Internet Engineering Task force (IETF) defined MIPv4/v6 (Mobile Internet Protocol version4/6) and FMIPv6 (Fast) as mobility techniques.

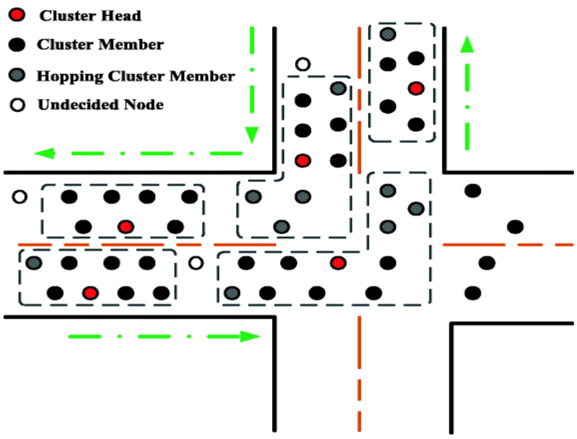


Figure 1. Clustering approaches in VANET

VANET system domains categorized into, the vehicle domain, the mobile device domain and the infrastructure domain. The vehicle domain comprises all kinds of vehicles such as cars and buses. Using the on-board unit i.e. node, vehicles can communicate among themselves and with roadside units. In VANET system, vehicles divided as an LE, a MV and a TV. The mobile device domain comprises all kinds of portable devices like personal navigation devices and smartphones. Communication types in VANET system divided as: V2I, and V2V.

A. Security Requirements

Security is a state of being or feeling protected from harm. Security Requirements for VANETs are:

1) *Authentication:* An authentication framework is necessary to enable receivers of broadcast data to verify that the received data really originates from the claimed node without modification. Authentication methods categorized into two groups: message authentication and entity authentication.

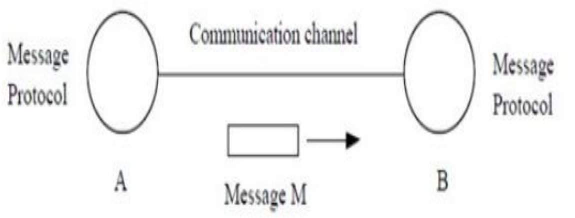


Figure 2. Authentication in VANET

2) *Integrity:* Integrity is required between two communicating nodes to protect data accuracy, which is main security issue desirable in VANETs.
3) *Confidentiality:* The challenge to protect data content from the adversaries is confidentiality.
4) *Non-Repudiation*: To repudiate means to deny. Nonrepudiation is the assurance that someone cannot deny something. Typically, nonrepudiation refers to the ability to ensure that a party to a contract or a communication cannot deny the authenticity of their signature on a document or the sending of a message that they originated.
5) *Pseudonymity:* Pseudonymity is the state of describing a disguised identity. A holder that is one or more human beings are identified but do not disclose their true names.
6) *Privacy*:The protection of personal information of drivers within the network from other nodes but extracted by authorities in case of accidents is a major privacy issue which is desirable for VANETs.

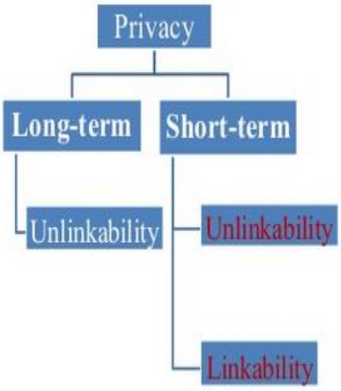


Figure 3. Privacy in VANET

7) *Scalability:* The ability of a network to handle growing amount of work in a capable manner securely is Scalability, which is the main challenge in VANETs.
8) *Mobility:* The nodes communicating in VANETs constantly change their locations with different directions and speeds making the network dynamic in nature. Therefore, in order to make

communication successful, it is challenging to establish security protocols.

9) *Key-Management:*The key is used to encrypt and decrypt information during communication process. When designing security protocols for networks like VANET, the issue of key management must be resolved.
10) *Location-verification:*This is necessary to prevent many attacks and is helpful in data validation process. Thus to improve the security of VANETs, a solid method is required to verify the nodes positions.
11) *Data Encryption:*Encryption is the act of encoding text so that others not privy to the decryption mechanism (the "key") cannot understand the content of the text.

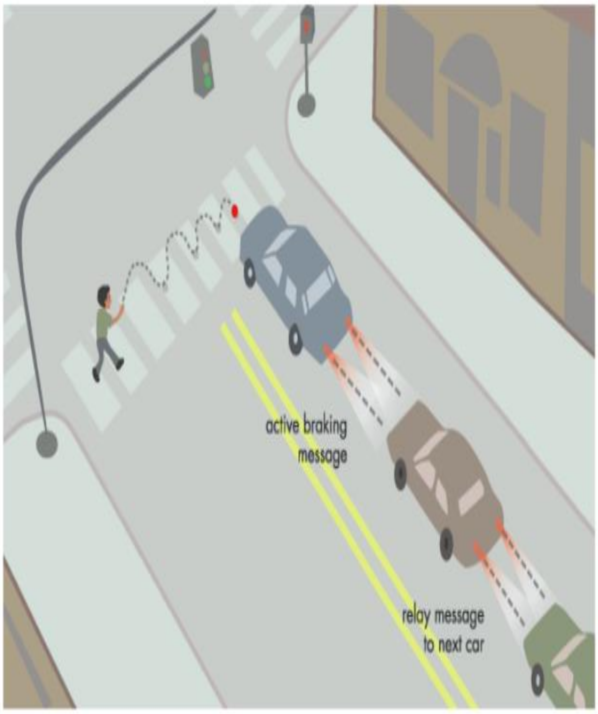


Figure 4. Safety application in VANET

B. Applications of VANETs

The three major classes of applications categorized in VANET as safety oriented, convenience oriented and commercial oriented.

1) *Safety Application:* Safety applications would be Slow/Stop Vehicle Advisor (SVA) in which a slow or stationary vehicle will broadcast warning message to its neighbourhood. Another similar type of application is emergency electronic brake-light (EEBL). In Post-Crash Notification (PCN), a vehicle involved in an accident would broadcast warning messages about its position to trailing vehicles so that it can take decision with time in hand as well as to the highway patrol for tow away support. Road Hazard Control Notification (RHCN) deals with cars notifying other cars about road having landslide. Another related application would be road feature notification, which deals with notification due to road curve, sudden downhill etc. Cooperative Collision Warning (CCW) alerts two drivers potentially under crash route so that they can mend their ways. Safety applications will monitor the surrounding road, approaching vehicles, surface of the road, road curves etc. . . . They will exchange messages and co-operate to help other vehicles out under such scenario. Though reliability and latency would be of major concern, it may automate things like emergency braking to avoid potential accidents.
2) *Convenience Application:* Congested Road Notification (CRN) detects and notifies about road congestions, which are used for route and trip planning. TOLL is yet another application for vehicle toll collection at the tollbooths without stopping the vehicles. Parking Availability Notification (PAN) helps to find the availability of slots in parking lots in a certain geographical area. Convenience application will be mainly of traffic management type. Their goal would be to enhance traffic efficiency by boosting the degree of convenience for drivers.
3) *Commercial Applicat* Commercial applications will provide the driver with the entertainment and services as web access, streaming audio and video Remote Vehicle Personalisation/ Diagnostics (RVP/D) helps in downloading of personalized vehicle settings or uploading of vehicle diagnostics from/to infrastructure. Service Announcements (SA) would be of particular interest to roadside business like petrol pumps, highways restaurants to announce their services to the drivers within communication range. Content Map Database Download (CMDD) acts as a portal for getting valuable information from mobile hotspots or home stations. Using Real Time Video Relay (RTVR), on-demand movie experience will not be confined to the constraints of the home and the driver can ask for real time video relay of his favourite movies.

The remainder of this paper organized as follows: Section II contains a review of related work. Section III explains methodology, section IV gives some results in simulator. In Section V, we give the conclusion. In section VI, we give acknowledgment and at last, references given in Section VII, which used for preparing this paper.

II. RELATED WORK

In recent years, various secure clustering techniques with distinguishing feature have been n proposed. Existing vehicle-to-vehicle safety systems together with new cooperative systems using wireless data communication. In [2] key management in ad hoc networks addressed. Key management was very difficult in ad hoc networks. In VANET system, key management technique- the public key infrastructure is used as a centralized approach in similar clusters and a distributed key is used between the cluster heads. In VANETs, key management achieved by key distribution, key certification, and key revocation. Schemes which were explained in [3], [4], [5], [6] , and [7] depend on certificate-based cryptography in which public-key certificates are used to authenticate public keys by binding public keys to the users' identities. Identity-based key management schemes have simple key management process, and reduced memory storage cost compared to other methods. However, they are easy to attack. Another approach is providing keying material through a web of trust [8], [9]. In these schemes, each node generates the public/private key pair by the node itself, issues certificates to its neighboring nodes and holds these certificates in its certificate repository. Key authentication performs via chains of certificates. In the distributed key generation, a set of n servers jointly generate a pair of public and private keys in a way that the public key is known to all nodes in the network while the private key is divided between the n servers via a threshold secret sharing scheme such as Shamir's (t, n) threshold cryptography [10]. It is observed in [11] that in ad hoc networks, it was easy to launch worm, man in the middle, denial of service attacks and to inoculate a malicious node, this was all done due to the lack of data integrity. In the [12] architecture was proposed for securing the clusters in ad hoc networks. The aim of [13] was to achieve trust based on keys in mobile ad hoc networks. The trust based physical logical domains was introduced for grouping nodes and getting distributed control over the network. In [14] the basic parameters, which were derived for deploying secure clustering algorithm, were max value, min value, d-hop clusters, identity ID and weight these parameters were involved in the election criteria. In [15] three suitable scenarios that are mainly for highway traffic were discussed. The first was that was used for choosing the cluster heads giving different parameters, which could improve stability, connectivity and security of VANETS. The second technique was the Adapter allocation of transmission range, which used hello messages and ensured connectivity among the vehicles. The third scenario was Monitoring of malicious vehicles to detect abnormal vehicles in the system. In [16] a concept of dynamic key distribution was observed in which there were multiple central certificate authorities present at their respective geographical areas and an asymmetric key distribution algorithm was used. Tim Leinmuller in 2006 [17] aimed to define a consistent & future proof solution to the problem of V2V/V2I security by focusing on SEVECOM (Secure Vehicle Communication). Lin et al. [18] proposed a secure and privacy preservation protocol using group signature scheme, named GSIS, to resolve the requirement of a large number of public key certificates. Lu et al. [19] proposed a system model for efficient privacy preservation protocol, named ECPP, which also uses a group signature scheme. Perrig et al. [20]. It is widely used in areas of sensor networks. It uses one-way hash chain where the chain elements are the secret keys to compute message authentication code (MAC). Boneh t al. [21] Proposd a mechanism on ring signature which was based on anonymity and spontaneity. Huand Laberteaux applied TESLA (an appropriate authentication mechanism for VANET. It uses time to provide asymmetric signature properties with symmetric functions. TESLA is an efficient and message-loss tolerant protocol for broadcast authentication with low communication and computation overhead. With TESLA, a sender sends data packets at a predefined schedule, to the receivers as well as the commitment

III. METHODOLOGY

Generally, in a secure clustering approach in VANET all vehicles inside a cluster are before communication, should be authenticate by a LE. Then only nodes can able to authenticate the nearby vehicle. This process establishes VANET environment quickly and gives short communication time among vehicular nodes in VANET thus results in increasing the communication capability.

A. Software Implementation

In implementing secure clustering algorithms, commonly used software is simulation software. There are many types of simulators available for both wired and wireless networks. A network simulator predicts the behaviour of a computer network environment and it gives accurate understanding of system behaviour. Moreover, the network simulator is the bank of different network and protocol objects. notepad++ for editing code, inside windows operating systems and XWin Server instead of bash shell. NS2 is one of the most popular simulators used in network research. It is open source and freely available software and developed at the University of Berkeley. It is available for platforms FreeBSD, Linux, SunOS/Solaris, MAC OSX and all windows versions. In ns2 simulator, network protocol stack is written in C++ language for fast to run, OTCL for fast to data write in order to differentiate control and data path implementations. TCL scripting language writes for specifying scenarios, traffic patterns and events. Simulations of VANET often involve large and heterogeneous scenarios.

B. Routing Protocol

AODV built upon DSDV routing protocol. DSDV is required to maintain a complete list of routes, whereas AODV creates routes on an on-demand basis; i.e., only when desired. This approach considerably reduces the number of required broadcast messages. When a source node desires to send data to a destination node, it checks if it already has a route to that particular destination node. If no valid route is present, it initiates a route discovery process to locate the other node. The source node sends out a Route Request (RREQ) to its neighbors, which then is forwarded to its neighbors until the destination node is reached or an intermediate node with a route to the destination is found. Figure shows the propagation of the RREQ packet within the network.

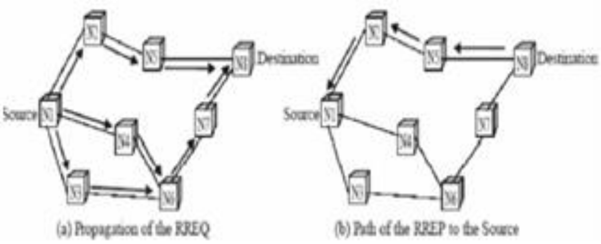


Figure 5. AODV route discovery

All the nodes receiving the route failure notification message forward the message up to the source node.

C. Cryptography Models

Encryption is the concern of the protection of electronic transmissions and digitally stored data. Standard encryption methods usually have two basic flaws, (1) A secure channel must establish at some point so that the sender may exchange the decoding key with the receiver; and (2) There is no guarantee that who sent a given message. Vehicle Safety Communications Consortium (VSCC) defined security approaches for a security architecture in vehicular networks that is under standardization so far. It defines a public-key-infrastructure (PKI)-based approach for securing messages sent in a vehicle-to-vehicle and vehicle-to-infrastructure fashion.

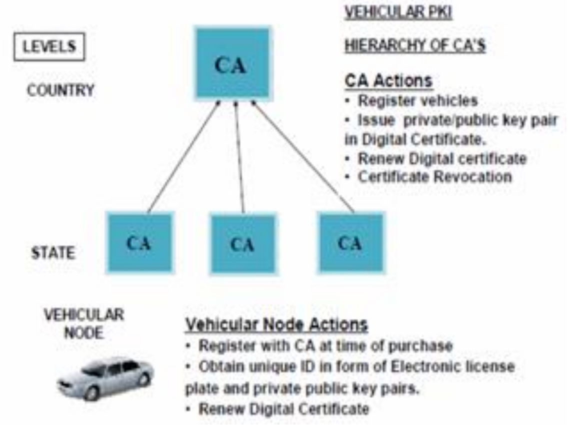

VEHICULAR PKI
HIERARCHY OF CA'S
LEVELS
COUNTRY
CA
CA Actions
• Register vehicles
• Issue private/public key pair in Digital Certificate.
• Renew Digital certificate
• Certificate Revocation
STATE
CA
CA
CA
VEHICULAR NODE
Vehicular Node Actions
• Register with CA at time of purchase
• Obtain unique ID in form of Electronic license plate and private public key pairs.
• Renew Digital Certificate

Figure 6. VANET security architecture

We can categorize cryptography techniques into two models:

1) *Conventional Techniques:* conventional techniques are categorized as:

a) *Tamper-proof device :* Each vehicle carries a tamper-proof device.

- Contains the secrets of the vehicle itself
- Has its own battery

- Has its own clock (notably in order to be able to sign timestamps)
  - Is in charge of all security operations
  - Is accessible only by authorized personnel

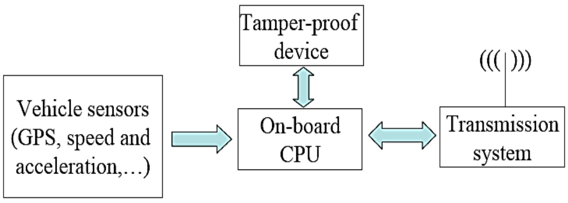


Figure 7. Tamper proof device in VANET

b) *V-PKI (vehicular PKI):* Each vehicle carries in its Tamper-Proof Device (TPD).

- A unique and certified identity: Electronic License Plate (ELP)
- A set of certified anonymous public/private key pairs

Mutual authentication can be done without involving a server authority (national or regional) are cross certified

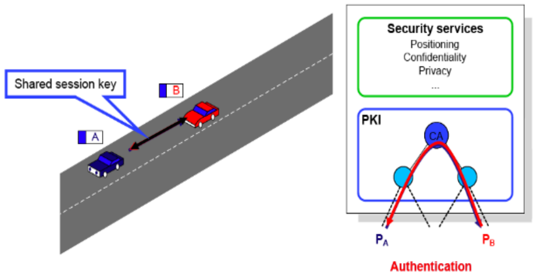


Figure 8. PKI in VANET

c) *Anonymous keys :* Preserve identity and location privacy.

- Keys can be preloaded at periodic checkups
- The certificate of *V*'s *ith* key:
- Keys renewed according to vehicle speed (e.g., ≈1 min at 100 km/h)
- Anonymity is conditional on the scenario
- The authorization to link keys with ELPs is distributed (say, police + court)

d) *Secure Localization:*This becomes more challenging in the context of vehicular networks, where the topology changes frequently and quickly. Whenever a new GeoUnicast communication has to be initiated, and the location information of the destination node is either unknown or outdated, the LS is used to determine the most updated location of the destination node.

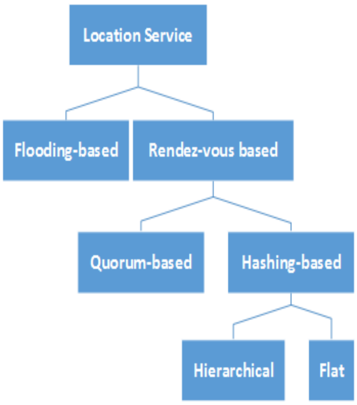


Figure 9. Location services taxonomy in VANET

e) *Certificate Revocation:*Certificate Revocation: Certificate revocation is done when any misbehaving vehicle having VC is discovered, where RSU replaces the old VC with new IC, to indicate that this vehicle has to be avoided and this happens when more than one vehicle reporting to RSU that a certain vehicle has a VC and broadcasting wrong data. See figure 5, this report must be given to RSU each time that any receiver receives information from sender and finds that this information is wrong.

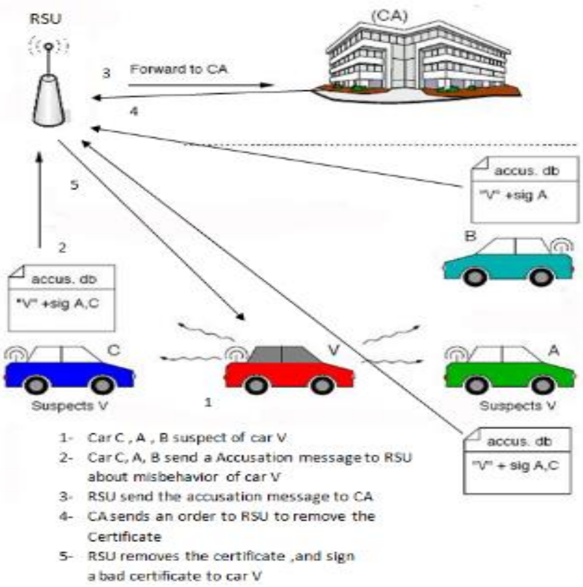

RSU
(CA)
3 Forward to CA
4
5
2
accus. db
"V" +sig A,C
accus. db
"V" +sig A
B
C
V
A
Suspects V
1
Suspects V
accus. db
"V" + sig A,C
1- Car C , A , B suspect of car V
2- Car C, A, B send a Accusation message to RSU about misbehavior of car V
3- RSU send the accusation message to CA
4- CA sends an order to RSU to remove the Certificate
5- RSU removes the certificate ,and sign a bad certificate to car V

Figure 10. Certificate revocation process in VANET

f) *Certificate revocation procedure:*The revocation will be as follows. A sender can sends a message to receiver; this message may be from untrusted vehicle, then receiver sends a message to RSU to acquire Session Key (SKA), RSU replay message

Containing SK Reply (SKR), this message contains the SK assigned to the current connection, this key is used to prevent attackers from fabrication of messages between two vehicles. Receiver sends a message to check validity, this message called “Validity Message”, the message job is to indicate if the sender vehicle has a VC or not. Afterwards, RSU reports to the receiver that the sender has a VC, so receiver can consider the information from the sender with no fear.

2) Classical Security Mechanisms

a) *Electronic license plates:* Electronic licence plates (ELP), which are cryptographically verifiable numbers equivalent to traditional license plates and help in identifying stolen cars and keeping track of vehicles crossing country border.

b) *Asymmetric Encryption using PKI:*A public-key cryptosystem is based on the assumption that it might be possible to find a system where it is computationally infeasible to determine the decryption rule given its encryption rule.vehicular public key infrastructure (VPKI) in which a certification authority manages security issues of the network like key distribution, certificate revocation etc. To keep a tap on bogus information attack, data correlation techniques are used. To identify false position information, secure positioning techniques like verifiable multilateration is commonly used. Public key encryption has rapidly grown in popularity because it offers a very secure encryption to information. In a public-key cryptosystem, the sender encrypts a message with the recipient's public key. This key is usually posted in a directory similar to a phone book. Upon receiving the message, the recipient uses his/her own private key to decrypt the message. For example, Alice encrypts a message using Bob's public key and sends it to him over an insecure channel. Bob then decrypts the message with a private key that is known only to him. RSA is a public-key cryptosystem that supports both encryption and digital signatures (authentication).Like all public key cryptography models, the RSA cryptosystem encrypts and decrypts a message using a pair of keys known as public key and private key. Its security is based on the difficulty of factoring large integers. Presently, most implementations of the RSA algorithm employ the use of 512-bit numbers. Cracking such a system requires the ability to factor the product of two 512-bit prime numbers. Factoring a number of this size is well beyond the capability of the best current factoring algorithms.

IV. SIMULATION RESULTS

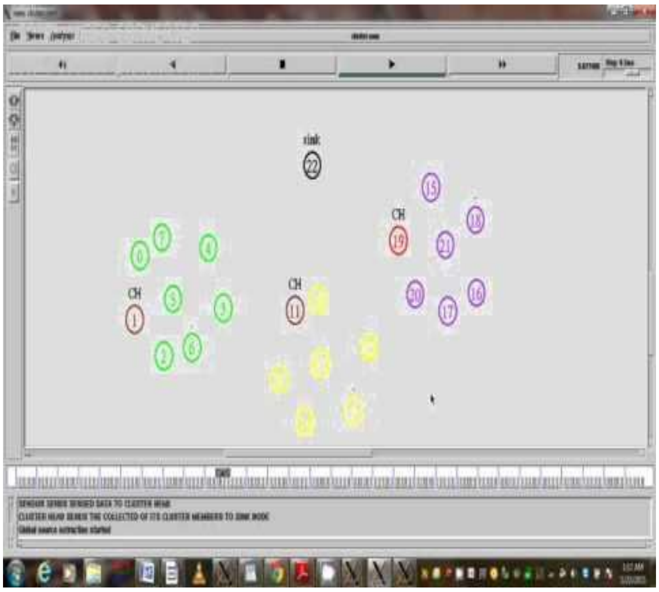
A. Parameters

In order to implement one of the security clustering algorithms, we used some parameters in NS2 simulator. These parameters and some output screenshots are given below.

Table 1: Simulation parameters

Parameters	Values
Network Size	4000m x 4000m
Number of Vehicle Nodes	112
Packet_ Size	1000bytes
Simulation Time	10 sec.
MAC protocol	IEEE 802_11
No. of AS	1
Number of LEs	16
Number of OBUs	86

B. Simulation Results



SENSOR SENDS SENSED DATA TO CLUSTER HEAD
CLUSTER HEAD SENDS THE COLLECTED OF ITS CLUSTER MEMBERS TO SINK NODE
Global source extraction started

Figure 11. Secure clustering output in NAM

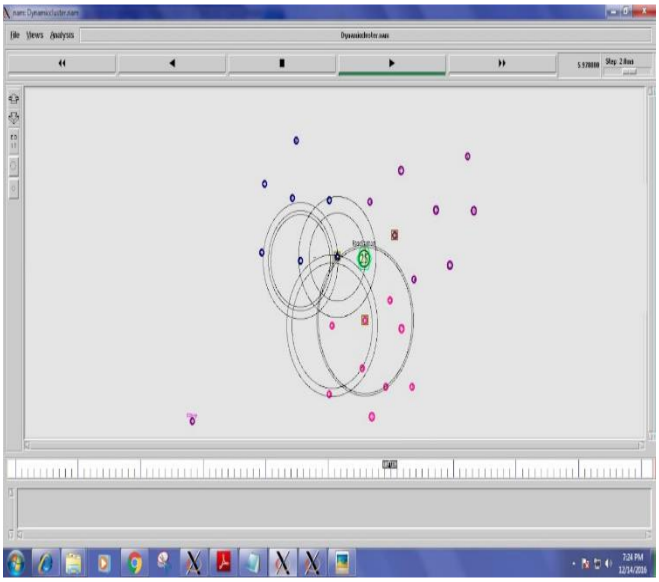


Figure 12. Communication process in clustering

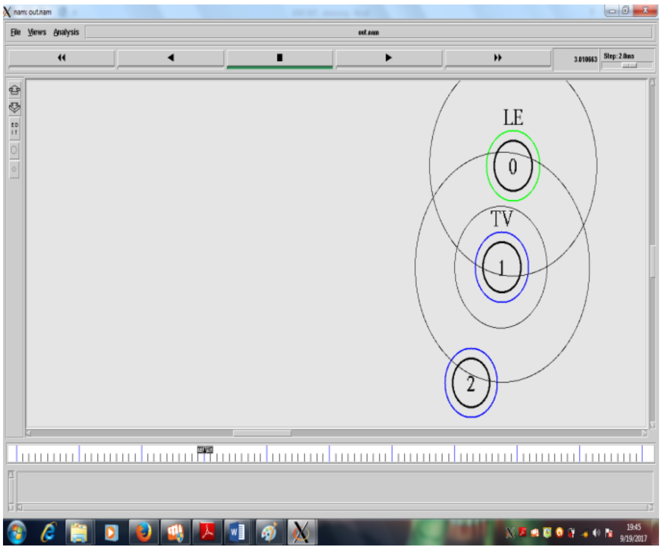


Figure 13. Trust process

V. CONCLUSION

There is a considerable improvement in the data communication between the nodes when secure clustering techniques employed. Without security, the delivery ratio becomes meaningless. These secure clustering techniques can be used in security sensitive applications like police and government agencies where VANETs are increasingly being used. Security measures guarantees that the transmissions of data are authentic that is data is accessible only by authorized parties. In general, confidentiality is not required in the VANET because generally packets on the network do not contain any confidential data.

VI. ACKNOWLEDGMENT

I will be thankful forever to the LORD BAJARANGBALI for his boundless blessings showered on me. I am very grateful and express my heartfelt countless Namaste to most respectable and my M.Phil. guide and supervisor who are **Dr. S. Anathi madam ji, B.E.,M.Tech.(IISC),Ph.D., Associate Professor, Department of Network Systems and Information Technology, University of Madras, Guindy Campus, Chennai** for their constant support, invaluable and inspiring guidance to the progress of my paper work. Without madam ji, and Sir K. Padmanabhan inspiration, definitely this paper work would not have been possible.

I would like to express my heartfelt special thanks to most respectable, emeritus and senior **Prof. (ret.) K.Padmanabhan, Former Head, CISL and Emeritus Professor in AC Technology College, Anna University** for their kind support to me for carrying out this paper work.

I would like to express special thanks to **Prof. (ret.) Ramana Murthy M. V., Department of Mathematics & Computer Science, University College of Science, Osmania University, Hyderabad, Telangana, Prof. (ret.) Shankar B., Department of Mathematics, University College of Science, Osmania University, Hyderabad, Telangana** and **R.K.sir** for clarifying my doubts On NS2 software to run on windows 7.

And I take this opportunity to express my heartfelt thanks to **Dr. K.R.Balaji (Guest lecturer in department of NS & IT, University of Madras, Guindy Campus, Chennai) M.Sc.,M.Phil.,Ph.D., Arun Ananthanarayanan, UGC research scholar, Department of NS & IT, University of Madras, Guindy Campus, Chennai** for giving their constant support and valuable help.

Finally, thank you very much **Dept. of NS & IT Scholars**!

VII. REFERENCES

[1] M. Raya and J. P. Hubaux, “Securing Vehicular ad hoc networks ,”HVVVJVVV J. Compute. Security, vol. 15, no. 1, pp. 39-68, 2007.

[2] Mohamed Elhoucine Elhdhili, Lamia Ben Azzouz and Farouk Kamoun:A Totally Distributed Cluster Based Key Management Model for Ad hoc Networks

[3] X. Lin, R. Lu, C. Zhang, H. Zhu, P.H. Ho, and X. Shen, "Security in Vehicular Ad Hoc Networks", IEEE Communications Magazine, Vol. 46, No. 4, 88-95, 2008

[4] Nai-Wei Lo and Hsiao-Chien Tsai, "Illusion Attack on VANET Applications", IEEE Globecom Workshops, pp. 1–8 (2007).

[5] IEEE Std. 1609.2-2006, “IEEE Trial-Use Standard forWireless access in Vehicular Environments-Security Services for Applications and Management Messages,” 2006.

[6] P. Wohlmacher, “Digital Certificates: A Survey of Revocation Methods,” Proc. ACM Wksp. Multimedia, Los Angeles, CA, Oct. 2000, pp. 111–14.

[7] M. Raya and J. P. Hubaux, “Securing Vehicular ad hoc networks ,” J. Compute. Security, vol. 15, no. 1, pp. 39-68, 2007.

[8] Pradeep B, Manohara Pai M.M and M. Boussedjra, J.Mouzna, Global Public Key Algorithm for secure location service in VANET, IEEE 2009

[9] P. S. L. M. Barreto et al., “Efficient and Provably-Secure Identity-Based Signatures and Signcryption from Bilinear Maps,” Proc. Advances in Cryptology — ASIACRYPT 2005, Taj Coromandel, Chennai, India, Dec. 2005, pp. 515–32

[10] Xiaodong Lin, Student Member, IEEE, Xiaoting Sun, Pin-Han Ho Member, IEEE, and Xuemin (Sherman) Shen, Senior Member, IEEE “GSIS: A Secure and Privacy Preserving Protocol for Vehicular Communications”, IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, VOL. 56, NO. 6, NOVEMBER 2007

[11] Rajaram Ayyasamy and Palaniswami Subramani: An Enhanced Distributed Certificate Authority Scheme for Authentication in Mobile Ad-hoc Networks, The International Arab Journal of Information Technology, Volume 9, pages 291-298, 2012.

[12] M. Bechler, H.-J. Hofi, D. Kraftt, E Pmket and L. Wolf: A Cluster-Based Security Architecture for Ad Hoc Networks, Twenty-third AnnualJoint Conference of the IEEE Computer and Communications Societies, Volume 4, pages 2393 – 2403, 2004

[13] Maxim Raya, Adel Aziz and Jean-Pierre: Efficient Secure Aggregation in VANETs, Proceedings of the 3rd international workshop on Vehicular ad hoc networks, Pages 67-75, 2006

[14] B. Kadri, A. M’hamed, M. Feham: Secured Clustering Algorithm for Mobile Ad Hoc Networks, IJCSNS International Journal of Computer Science and Network Security, volume 7, pages 27-34, 2007

[15] Ameneh Daeinabi, Akbar Ghaffar Pour Rahbar and Ahmad Khademzadeh: VWCA: An efficient clustering algorithm in vehicular ad hoc networks, Journal of Network and Computer Applications, Volume 34, Pages 207–222, 2011

[16] Tahani Gazdar, Abderrahim Benslimane, Abdelfettah Belghith and Abderrezak Rachedi: A secure cluster-based architecture for certificates management in vehicular networks, 2013

[17] Leinmuller T, Buttyan L et al (2006) SEVECOM-Secure Vehicle Communication. Proc of IST Mob Summit.

[18] Lin, X., Sun, X., Shen, X.: GSIS: a secure and privacy preserving protocol for vehicular communications. IEEE Transaction on Vechicular Technology 56(6), 3442–3456 (2007)

[19] Lu, R., Lin, X., Zhu, H., Ho, P.-H., Shen, X.: ECPP: Efficient conditional privacy preservation protocol for secure vehilce communications. In: Proceedings of The IEEE INFOCOM 2008, pp. 1229–1237 (2008)

[20] D. Boneh and H. Shacham. (2004). Group signatures with verifier-local revocation, in Proc.ACM CCS’ 04, pp. 168-177

[21] http://media.springernature.com/full/springerstatic/image/art%3A10.1186%2Fs13638-016-0573-9/MediaObjects/13638_2016_573_Fig1_HTML.gif

[22] https://www.researchgate.net/profile/Chaudhary_Muhammad_Asim_Rasheed/publication/315512136/figure/fig1/AS:476526849335296@1490624262514/Fig-1-Categorization-of-VANET-Attacks.ppm

[23] https://cdn.intechopen.com/pdfs-wm/42787.pdf

[24] www.roadtraffic-technology.com

[25] https://www.researchgate.net/profile/Raik_Aissaoui/publication/305149984/figure/fig5/AS:382635986702342@1468238936844/Figure-25-Location-service-taxonomy.ppm

Authors Biographies

[1]**Mr. Venkatamangarao Nampally (n.venkat018@gmail.com)** pursed Bachelor of Science in Computer Science, Master of Science in Computer Science and Master of Technology in Computer Science & Engineering from Osmania University, Hyderabad, Telangana, India and pursed Master of Philosophy from University of madras, Chennai, Tamil Nadu, India. He is currently persuing Ph.D. in Computer Science from Osmania University, Hyderabad, and Telangana, India. His main research work focuses on Cryptography Algorithms, Network Security, and Privacy. He has 7 years of teaching experience and 2 year of Research Experience.

[2] **Dr. M. Raghavender Sharma(drmrsstatou@gmail.com)** got his Ph.D. from Telangana State, India and currently he is an Assistant Professor and Head of the Department, Department of Statistics at University College of Science,Saifabad, Osmania University, Hyderabad, Telangana, India. He is the author of several papers. He is supervisingd many Ph. D.'s. He has excellent teaching track record.

[3] **Arun Ananthanarayanan (*aarun_84@yahoo.co.in*) has** finished his M.S from University at buffalo, New York, USA. Currently he is pursuing Ph. D. from Univerity of Madras, Department of NS & IT, Guindy campus, **Chennai,** Tamil Nadu, India. He is expert in Image Processing and Speech Recognition.