Strategical Comparison: Recognizing and Evicting Sybil Attack in Vehicular Ad Hoc Networks

Sagar Narang
Student
Lovely Professional University Punjab

Kundan Munjal
Assistant Professor
Lovely Professional University Punjab

ABSTRACT
Vehicular Ad-Hoc Networks (VANET) generalization of Mobile Ad Hoc Networks (MANET) are proclaimed for extreme mobility as compared to MANET. Motivation of VANET is Traffic Administration and Human Protection. Misuse of utilities provided by VANET is more prone to attacks like Black Hole Attack and Sybil Attack. This paper is fascinated towards recognition and eviction of Sybil Attack in VANET. In Sybil Attack evil-minded nodes known as Sybil nodes imitates multiple fraud identities of one vehicle at same time distorting behavior of right-minded nodes in network vulnerable to human lives. In this paper, different strategies of finding, locating and evicting Sybil Nodes in VANET are suggested and differentiated.

Keywords
Sybil attack recognition, eviction and localization, GPS, RFID, VANET, PKI, Observers, DTT, Privacy preserving, RF-GPS, Certificate and Key administration, Pseudonyms and RSU.

1. INTRODUCTION
MANET is generalization of Wireless Ad-Hoc Network (WANET) which is further generalization of Ad-Hoc networks. There is dissimilarity between Ad-Hoc network and MANET:

"MANETs are always Ad-Hoc but Ad-Hoc are not always MANETs"

MANET is architecture-less network sanctioning mobile devices associated in network for circulating information between them without any background architecture [1] [2]. MANETs are proclaimed for their high mobility. In MANET, mobile devices associated with each other through wireless link without any background architecture are sanctioned to move arbitrarily. MANET deliver aspects like Autonomous Terminal, Distributed Operation, Multi-hop Routing, Dynamic Network Topology, Fluctuating Link Capacity and Light Weight Terminals [3]. MANETs are employed in areas like military battlefields, emergency search, rescue sites, classroom and convention where instant utilization and effective reformation is necessary and wired network is inaccessible. This paper focuses on recognition and eviction of most commonly occurring Sybil attack in VANET vulnerable to human lives.

VANET generalization of MANET exerts moving vehicles as mobile nodes in MANET for inception of mobile network. Every moving vehicle in VANET can act as wireless router, access point or node for efficient communication among

vehicles and with nearby roadside units (RSU). Distance between two vehicles for communication is 100-300 metres approx. Any vehicle can join VANET for inception of vehicular network. Corps and fire vehicles are first approximated systems exerting this new emerging technology VANET for safety purposes and traffic related problems. The main difference between VANET and MANET is extreme mobility in VANET as compare to low mobility in MANET. Extreme mobility in VANET triggers vehicles to change their topology instantly as compare to mobile devices changing their topology slowly in MANET. In VANET, vehicles connect and move in structured pattern whereas in MANET, mobile devices connect and move in unstructured pattern. Wi-Fi IEEE 802.11p, WAVE IEEE 1609, WiMAX IEEE 802.16, Bluetooth, IRA, Zig Bee, Satellites, DSRC (Dedicated Short Range Communications) are technologies exerted in VANET. Intelligent Transportation System (ITS) is composed of VANETs. DSRC are unidirectional or bidirectional, short range to medium range communications channels exerted for automation. Its applications provides services regarding traffic management and sanctions assorted users to be informed, secured and synchronized.

There are three major classifications for grouping of VANET applications:

1. Safeguard Applications: Safeguard Applications are determined towards depleting the threats related to road accidents and loss of human lives. Collision Risk Warning, Control Loss Warning, Pre-Crash Warning and many more Applications are associated with Safeguard Applications.

2. Traffic Administration and Oversee Applications: Traffic Administration and Oversee applications are determined towards refinement of traffic co-operation, co-ordination and motion among vehicles. Speed Management and Co-operative Navigation Applications are associated with Traffic Administration and Oversee Applications.

3. Advertorial and Commercial Applications: Advertorial and Commercial Applications are determined towards offering entertainment associated messages like location of nearest shopping mall, cinema and many more. Co-operative Local Applications and Global Internet Applications are associated with Advertorial/Commercial Applications.

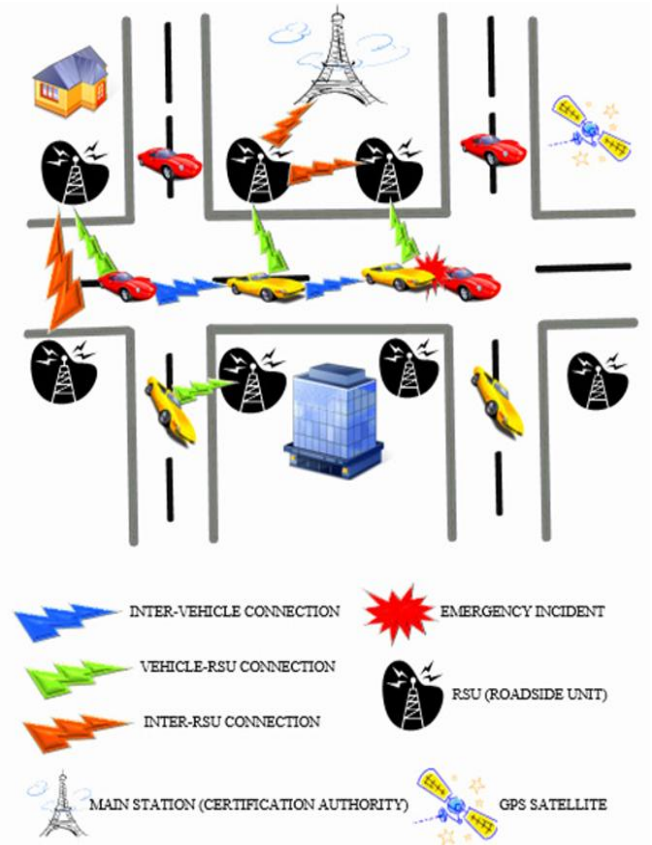

Figure-1: VANET ARCHITECTURE

VANET architecture incorporates vehicles associated with On-Board Unit (OBU), RSU and Certification Authority (CA) disposed along Highways, GPS satellites, various kinds of communication between vehicles, RSU and CA depicted above in Figure 1. Routing, security, reliability, Quality of Service (QOS), Internetworking and Power consumptions are numerous challenges of VANETs but security is major concern in VANET. Security is crucial concern in VANET. Numerous security threats have diminished effectiveness of VANET, human lives and traffic management applications. Sybil Attacks belongs to those threats diminishing effectiveness of VANET.

In Sybil Attack evil-minded nodes known as Sybil nodes imitates multiple fraud identities of one vehicle at same time distorting behaviour of right-minded nodes in network vulnerable to human lives. It is termed after case study of woman recognized with disjoint character disorder and recommended in or before 2002 by Brian Zill at Microsoft Research [4]. Different strategies of finding, locating and evicting Sybil Nodes in VANET are suggested and differentiated along with their flaws and strength in later sections.

Outline: After elementary section, in Section 2, literature review of different strategies has been considered. In Section 3, comparison of different strategies along with their adequacies and inadequacies has been examined. In Section 4, conclusion and future work has been suggested.

2. RELATED WORK

Sybil Attack was first depicted by Doucer in [4]. Different strategies for finding, locating and evicting Sybil Nodes and Sybil Attack have been proposed till now. Exerting Resource Testing [4] was fundamental direct validation strategy grounded on premise that proportion of enumerating resources like computation, storage and communication for each vehicle on network are minimal. In this strategy, verifier disseminates request instructing definite proportion of resource expenditure to acknowledge and manage vehicles that acknowledged back in given time interval. Evil-minded vehicles are furnished with numerous symmetric and asymmetric cryptographic strategies integrated tools. So, this strategy is impractical. Newsome et al. [5] suggested Radio Resource Testing strategy grounded on premise that each vehicle has only one radio vulnerable to concurrent transmission or reception on more than one channel. Intruder may exert different vehicles for transmission to multiple radio channels. This strategy is beneficial grounded on premise that intruder cannot exert one vehicle for transmission to multiple radio channels concurrently. Doucer [4] suggested Rationalized Trusted Certification strategy which employs Certification Authority (CA) subjected to ensure claimed identity of vehicle is authorized with assistance of Access Control List (ACL) and further circulate certificates to right-minded vehicles for communication. Vehicles identities are certified formerly connecting to network. CA are subjected to ensure preservation of certification list and one-to-one relationship between vehicles and identities. This strategy is inadequate in case of single point attack, potential congestion, scaling and dissemination cost. Demirbas and Song [6] suggested Received Signal Strength Indicator (RSSI) strategy consequence of dissemination power exerts receiver to collaborate RSSI of message with sender-id integrated in message without hampering network with symmetric and asymmetric keys. Receiver recognizes Sybil attack upon receiving another message with same RSSI but different sender-id. Sybil node may disseminate message with different ID's employing fluctuating dissemination power to deceive receiver. This strategy is inadequate due to erratic, time fluctuating and non-isotropic nature of RSSI.

Different strategies are grounded on Public Key Infrastructure (PKI) suggested by Raya and Hubaux [7] exerting CA to validate each vehicle with distinct public key and certificates organized by CA. Classical PKI grounded certificates employed only key information without any consideration to vehicles distinct physical knowledge provoking it defenceless to stolen authorized key pair and certificates utilized by malicious vehicle. Later Multifactor authentication strategy was suggested which exerts certificates to associate key pair information, radio coverage, transmitter coverage and so on as accomplished by CA. VANET is divided into zones. Each zone has one CA. CA of different zones oversee circulated certificates by disseminating with each other along certified channel as messages with authorized certificates are considered. In VANET, validating PKI for each vehicle at same time with different manufacturer, policies and countries or Vehicular Public Key Infrastructure (VPKI) including key dissemination and certificate administration incorporating circulation, preservation, revocation and elicitation of certificates possess prolong duration and memory. VPKI is inadequate to preserve privacy. Certificates should be changed from time to time for preserving privacy.

Guette and Bryce [8] suggested tamper proof hardware grounded strategy associated with cryptographic principles fabricated on Trusted Platform Module (TPM) integrated in vehicle. TPM certificates are certified by vehicle manufacturer and confidential information and protocols are preserved in Tamper proof hardware where replication and fabrication is impossible. So, dissemination between TPMs of vehicles are shielded from Sybil attack. TPM is enhanced

alteration of certificates but CAs are significant for administration of individual vehicles. This strategy is inadequate due to flaws of tamper proof hardware suggested by Anderson and Kuhn in [10]. Evil-Mined vehicles with exploitation of semiconductor test device can invade chip-sized tamper resistance hardware for fetching certificates components by inspection and utilization of chip's components. Eschenauer and Gligor [11] suggested Random Key Pre-distribution strategy employing each vehicle with arbitrary group of keys from huge key space prior to concur on distinct key or shared secret key between two different arbitrary groups of keys of two different vehicles for communication. Chan, Perrig and Song [9] suggested q-composite random key pre-distribution strategy grounded on above explained strategy which employs q-distinct keys (q>=1) instead of single key for reliable communication between two vehicles. This strategy certifies the key and integrates identity of vehicle with key circulated to vehicle. Sybil nodes will fail at key certification test due to irrelevant equivalence with compromised key set. This strategy is inadequate to preserve privacy due to association of vehicle's identity along keys, communication overhead when two vehicles are not straight associated and computational overhead.

Park, Aslam, Turgut and Zou [12] suggested Timestamp series strategy grounded on Roadside Unit Support (RSU) employs RSU incorporating certified timestamps to circulate certified Timestamps associated with vehicles self-initiated public key to each vehicle after moving along RSU. It is infrequent for arbitrary two or more than two vehicles to move along slightly numerous RSUs repeatedly at same time. Sybil attack is recognized if numerous messages disseminated by vehicles incorporates identical timestamp series. This strategy is inadequate to preserve privacy and unable to recognize Sybil attack if RSU are located at intersections and complex roadways in urban area. This strategy is unable to restrain vehicles from acquiring different timestamps from RSU. It is grounded on premise that VANET incorporates limited number of vehicles.

Zhou et al., Choudhury, Ning and Chakrabarty [13] suggested Privacy Preserving Strategy employing Department of Motor Vehicles (DMV) to circulate discrete pool of pseudonyms hashed with discrete value to vehicles and further exerted for obscuring vehicles distinct identity. Pseudonyms are exerted for disseminating traffic messages instead of vehicles real identities for privacy. Hashing restrains malicious vehicle from exploitation of pseudonyms. Hashed Values are preserved at RSU and DMV. Co-ordination of RSU and DMV association can recognize any deceptive pseudonym. Minimal knowledge about vehicles at RSU provokes it to transmit all deceptive pseudonyms upon intuition along with hashed value to DMV which further validates pseudonyms preliminary circulated to vehicles. This strategy preserves privacy but inadequate to mitigate false alarm over transmission of each deceptive pseudonym to DMV as overheads are fairly moderate which further provokes inflation in burden and time dissipation to DMV. Vehicles disseminating farther from consideration zone of RSU provokes termination of suggested strategy.

Mekliche and Moussaoui [14] suggested Location-grounded privacy preserving strategy almost identical to strategy suggested by Zhou et al., Choudhury, Ning and Chakrabarty [13] except dissimilarity that burden and false alarm on DMV is minimized due to co-ordination among nearby RSU in former strategy. Co-ordination diagnoses position of deceptive pseudonyms and further computes separable extent among position of malicious nodes. If separable extent is above threshold then RSU disseminates deceptive pseudonym to DMV for further certification where fine grained hash of deceptive pseudonym is computed for distinction among actual attack and false positive. Zhou and Chigan [15] suggested Dynamic Trust Token (DTT) strategy for assisting node co-ordination and preserving packets during dissemination by exerting both symmetric and asymmetric cryptography and further exerting Neighbourhood Watchdog to provoke Trust Token grounded on sudden performance for certification of packet exactness. Each vehicle in DTT is exerted as Predecessor, Relayer and Successor for per packet dissemination. Relayer is exerted for packet dissemination. Predecessor is exerted for fabrication of trust token with assistance of Watchdog. Successor is exerted for conclusion on accepting or discarding of packet. Each dissemination of packets incorporates four phases: Packet Relaying, Behaviour Evaluation, Token Relaying and Packet Acceptance. This strategy is inadequate to trace back actual packet dispatcher after packet disseminates through numerous hops and key administration including circulation, preservation, revocation and elicitation possess prolong duration and further fabricates burden to huge unrestrained VANET.

Triki, Rekhis, Chammem and Boudriga [16] suggested RFID grounded Privacy Preserving strategy exerting two forms of validation methods. First method exerts RFID tags associated within vehicles for acquiring short span certificates from RSU after validation of vehicles along RFID tags by RSU. RFID tags and RSU are associated with Vehicle Identification Number (VIN) and RFID reader respectively. Second method exerts acquired certificates for validation to neighbours. This strategy is grounded on premise that network is split into various regions. Each region incorporates numerous RSU moreover one RSU among them is appointed as controller or Road Side Controller (RSC) for that region further associated with CA. Different regions RSCs are associated together for interchange of information analogous to circulated certificates, accumulated surveillance and investigated reports. Vehicle's certificates are renewed on transition from one region to another restraining intruders against surveillance of vehicles. Exertion of RSU at road intersections may sanction vehicles to acquire numerous authorized certificates. During certificates revocation, precise and immediate recognition of vehicle is essential to restrain them from acquiring numerous identities from same RSU. False negatives analogous to vehicles disseminating farther from consideration region of RSU are minimized with assistance of observers associated within vehicles, RSU and RSC. Burden on RSU is minimized due to allocation of observers associated within vehicles, RSU and RSC. Ob servers are exerted for accumulation, substitution and evaluation of data analogous to volatile circumstances. This strategy preserves privacy as VIN associated within RFID tag is never disseminated inside VANET. Exerting RFID systems [17] is convenient interpretation regarding vehicles recognition and localization.

Numerous localization strategies like Global Positioning System (GPS), Differentiated Global Positioning System (DGPS), Map Matching, Dead Reckoning, RF-GPS RFID Assisted Localization, Cellular Localization, Image/Video Processing, Relative Distributed Ad-hoc Localization and Localization services have been suggested. GPS [18] comprises 24 satellites revolving in earth's orbit. GPS receiver associated within vehicles gathers continuous information disseminated by satellites for length approximation and location determination to at least four

familiar satellites exerting Time of Arrival (TOA) and trilateration strategy respectively. For precise operations of GPS receiver's estimation, at least 3 and 4 satellite signals for 2D and 3D positioning respectively are essential. ±10 to 30 m is localization flaw in GPS receivers. Adjacent GPS receivers have coordinated flaws. DGPS [18] exerts assistance of coordinated flaws by positioning GPS receivers in previously familiar established location. In DGPS variation among GPS receiver's estimated position and previously familiar physical location is disseminated to adjacent GPS receiver's for alteration of their estimated position. DGPS exerts fixed referral node whereas RF-GPS [17] [18] exerts any moving vehicle as referral node for alteration of estimated position.

Eun-Kyu Lee, Sungwon Yang, Soon Y. Oh, and Mario Gerla [17] suggested RF-GPS(RFID supported GPS systems) enhancing GPS position preciseness by utilizing approaches like RF-GPS and DGPS for recognition and localization of vehicles with cooperation of mobile referral nodes on network. It sanctions Non-GPS vehicles to estimate their location and travel information via RFID and IEEE 802.11 radio respectively by notifying GPS implemented neighbour vehicles. Vehicles interchange data among themselves using mobile RFID reader/tag set. RSU incorporates RFID reader exerted for certifying VIN from RFID tags associated within vehicles. Fragment of vehicles incorporates GPS systems but RFID reader/tag set is incorporated by all vehicles. Map matching strategy [18] exerts various locations acquired across continuous durations for organization of approximated path differentiated with familiar digital map information for exploration of path equivalent to approximated path. It is exerted for enhancing capabilities of GPS. Dead Reckoning strategy [18] explores current location of vehicle grounded on last familiar location acquired by GPS. It is exerted during short duration inaccessibility of GPS within tunnel or indoor parking area and associated with various localization strategies like Map matching. 10 to 20 m positioning flaw arises in 30 s with 100 km/h driving speed. Non-GPS vehicles approximate their locations grounded on adjacent GPS vehicles with assistance of distributed localization strategy [18] [19] exerting RSSI and information employed by optimization method. Communication with at least three GPS sanction vehicles is essential for approximating location of Non-GPS vehicles. Image/Video processing strategy [18] is exerted to contribute Data Fusion algorithms for approximation of vehicles location. It precisely determines vehicle's analytical specifications comprising lane width, road side curvature, camera inclination angle, vehicles distance against lane's left side and vehicles orientation angle.

Cellular localization strategy [18] necessitates establishment of communication architecture configured by cellular base stations circulated throughout covered area. Handoff is exerted during switching of vehicles between base stations due to larger signal power. It is exerted in association with various localization strategies like GPS, RSSI, TOA and Time difference of arrival (TDOA), Angle of arrival (AOA) for approximating vehicle's position. In TDOA approximated distance is grounded on variation among arrival time exerted by single signal to strike various base stations. In TOA approximated distance is grounded on arrival time of signal to strike various base station. In AOA angle is approximated by signal striking at base station associated with directed antennas. Approximation of position is grounded on AOA of three distinct base stations. This strategy is imprecise than GPS. Its preciseness rely upon considerations like current urban environment, signal recognizing base stations and positioning strategies with localization flaw of 90-250 m imprecise for VANET applications.

3. COMPARISON

In this section, different strategies for recognition and eviction of Sybil attack in VANET like Resource Testing, Radio Resource Testing, Trusted Certification, Received Signal Strength Indicator (RSSI), Public Key Infrastructure (PKI)/Public Key Cryptography, Trusted Platform Module (TPM), Random Key Pre-Distribution, q-composite Random Key Pre-Distribution, Timestamp Series, Privacy Preserving, Dynamic Trust Token (DTT), Location grounded Privacy Preserving, RFID grounded Privacy Preserving and RF-GPS (RFID supported GPS systems) Localization are compared with parameters like Essential Premise, Adequacies, Inadequacies and Simulation Outcomes. These strategies can be integrated with localization strategies like GPS, RF-GPS, DGPS, Map Matching, Dead Reckoning and Cellular Localization for preciseness of vehicles claimed location to restrain them from fabrication of forged identity by proclaiming from different locations.

Table 1. Comparison among numerous strategies

STRATEGIES	ESSENTIAL PREMISE	ADEQUACIES	INADEQUACIES
Resource Testing	Minimal proportion of enumerating resources.	Vehicles responding in threshold time duration are managed.	Malicious vehicles furnished with cryptographic strategy responds in threshold time duration.
Radio Resource Testing	Vehicle has one radio vulnerable for dissemination to multiple radio channels concurrently.	Vehicle disseminate to only one radio channel at a time.	Intruder may exert different vehicles for dissemination to multiple radio channel.
Trusted Certification	CA ensure claimed identity of vehicle formerly connecting to network with ACL. CA circulate certificates vehicles.	Certification list preserved at CA. One-to-One relation among vehicles and identities.	Only CA certifies vehicles identities. Single point attack and Potential Congestion at CA. Scaling and dissemination cost.
Received Signal Strength Indicator (RSSI)	No congestion on network with symmetric and asymmetric keys. RSSI of message integrated with sender id.	Sybil attack recognized if another message with same RSSI but different sender id is received. Can be integrated with localization strategies like dead reckoning, map matching, GPS, DGPS, RF-GPS for accuracy.	Erratic, time fluctuating and non-isotropic nature of RSSI. Receiver is deceived due to fluctuating dissemination power. Sybil node disseminates message with different id due to fluctuation.
RF-GPS(RFID supported GPS systems) Localization	Fragment of vehicle incorporates GPS systems. All vehicles incorporates RFID reader/tag set. RSU incorporates RFID reader.	Recognition and localization of vehicles with cooperation of mobile referral nodes in VANET. Non GPS vehicle estimate their position by notifying GPS implemented neighbour vehicle. Exerting RF-GPS and more.	Fixed referral nodes in DGPS provokes error for vehicles far from it. Localization capability dissipates with minimal RFID associated vehicles and RFID reference points

Trusted Platform Module (TPM)	Inbuilt cryptographic principles in Tamper proof hardware fabricated on TPM TPM integrated vehicles	TPM certificates preserved in Tamper proof hardware. Replication and fabrication unfeasibility in Tamper proof hardware. TPM certificates is enhanced alteration of certificates	Vehicles individual administration by CA takes prolong duration. Vehicles invade chip-sized tamper resistance hardware for fetching certificates components by inspection and utilization of chip's components
Random Key Pre-Distribution	Vehicles employed with arbitrary group of keys from huge key space	Prior to communication vehicles concur on single distinct key among two different group of keys. Compromised key set unfeasible due to administration of key space by trusted parties.	Intruder may easily recognize single distinct key provoking failure of strategy. Indirect association of vehicles provokes communication and computational overhead. Association of vehicle's identity along key provokes privacy issue.
q-composite Random Key Pre-Distribution	Vehicles employed with arbitrary group of keys from huge key space	Prior to communication vehicles concur on more than one distinct key among two different group of keys. Compromised key set unfeasible due to administration of key space by trusted parties.	Indirect association of vehicles provokes communication and computational overhead. Association of vehicle's identity along keys provokes privacy issue.
Timestamp Series	RSU circulate certified timestamps with vehicles self-initiated public key to vehicles moving along RSU. No vehicular PKI (VPKI) for distinct vehicles and few set of vehicles deployed on road. Restricted set of RSU lacking internet access.	Infrequent for two or more than two vehicles to move along RSUs at same time. Sybil attack recognized if disseminated messages have identical timestamp series. No need of administration of individual vehicle.	Association of vehicles self-initiated public key provokes privacy issue. Deployment of RSU at intersections and complex roadways provokes overlook of Sybil attack. Vehicles may acquiring different timestamp from RSU.

Privacy Preserving	DMV circulates pool of pseudonyms hashed with discrete value to vehicles. Hashed values preserved at RSU and DMV.	Privacy preserved due to dissemination of message with pseudonyms. Hashing prevents exploitation of pseudonyms. RSU and DMV coordination recognize deceptive pseudonym.	Minimal knowledge of vehicles at RSU provokes false alarm. Burden and Time dissipation due to transmission of each deceptive pseudonym to DMV. Incapable to recognize vehicles disseminating outside consideration zone of RSU.
Dynamic Trust Token (DTT)	Exertion of vehicles as Predecessor, Relayer and Successor for packet dissemination. Coordination among vehicles. Trusted initiator. One-to-one mapping among public key of vehicle and electronic identity.	Packet preservation by exertion of neighbourhood watchdog, symmetric and asymmetric cryptography. Recognize and evict vehicles hampering packet dissemination by trust token fabricated with neighbourhood watchdog assistance. Preservation of packet integrity.	Incapable to trace back actual dispatcher after dissemination through multiple hops. Key administration possess prolong duration and burden on VANET. Security and packet dissemination overhead.
Location grounded Privacy Preserving	DMV circulates pool of pseudonyms hashed with discrete value to vehicles. Hashed values preserved at RSU and DMV.	Privacy preserved due to dissemination of message with pseudonyms. Hashing prevents exploitation of pseudonyms. RSU and DMV coordination recognize deceptive pseudonym. False alarm on DMV minimized due to coordination among nearby RSU. Can be integrated with localization strategies like dead reckoning, map matching, GPS, DGPS, RF-GPS	Incapable to recognize vehicles disseminating outside consideration zone of RSU. Intruders may exert more computational power for alteration of dissemination signal strength. Intruders may exert more certified pseudonyms for dissemination of same message.
RFID grounded Privacy Preserving	RFID tags associated within vehicles incorporates VIN. RFID reader associated with RSU. Splitting of network in various regions. Each region has multiple RSU and one of them is RSC for that region. Observers associated within vehicles, RSUs and RSCs investigate data related to volatile events with assistance of Certificate revocation list (CRL).	Vehicles validated through RFID tags by RSU and acquire short span certificates. Validation of vehicles to neighbours. Different RSCs associate for investigation of information analogous to circulated certificates. False negatives analogous to vehicles outside consideration zone of RSU and burden on RSU is minimized with assistance of observers. Privacy preserved as VIN is never transmitted within VANET. Vehicles certificates renew on transition from one region to other restraining intruders against surveillance of vehicles	Precise and immediate recognition of vehicle is essential to restrain them from acquiring multiple identities from same RSU. RSU at road intersections sanction vehicles to acquire numerous authorized certificates. Vehicles may misuse assigned certificates after going back to previous region when timer of certificate is left and may acquire another certificates and becomes holder of two valid certificates.

4. CONCLUSION AND FUTURE WORK

In this paper different strategies for recognition and eviction of Sybil attack in VANET like Resource Testing, Radio Resource Testing, Trusted Certification, Received Signal Strength Indicator (RSSI), Public Key Infrastructure (PKI)/Public Key Cryptography, Trusted Platform Module (TPM), Random Key Pre-Distribution, q-composite Random Key Pre-Distribution, Timestamp Series, Privacy Preserving, Dynamic Trust Token (DTT), Location grounded Privacy Preserving, RFID grounded Privacy Preserving and RF-GPS (RFID supported GPS systems) Localization are compared with parameters like Essential Premise, Adequacies, Inadequacies and Simulation Outcomes. These strategies can be integrated with localization strategies like GPS, RF-GPS, DGPS, Map Matching, Dead Reckoning and Cellular Localization for preciseness of vehicles claimed location to restrain them from fabrication of forged identity by proclaiming from different locations. The main issue in various privacy preserving strategies, Timestamp series is deployment of RSU at intersections but timestamp series strategy analogous to low cost due to no need of unnecessary administration of individual vehicle. Main focus for strategy should be privacy preservation and precise recognition of evil minded vehicle. In future association of above explained strategies along with their adequacies will be sanctioned for efficient recognition, localization and eviction of evil minded vehicles along with Sybil attack.

5. ACKNOWLEDGMENTS

Foremost, I would like to express my sincere gratitude to my guide Prof. Kundan Munjal for continuous provision of my M.Tech study and research, for his patience, motivation, enthusiasm, and immense knowledge. His supervision helped me in writing of review paper. I could not have imagined having better guide and mentor for my M.Tech study.

Last but not the least, I would thank my family for supporting me spiritually throughout my life.

6. REFERENCES

[1] M. Frodigh, P. Johansson, and P. Larsson. “Wireless ad hoc networking: the art of networking without a network,” Ericsson Review, No.4, 2000, pp. 248-263.

[2] Joseph P. Macker, M. Scott Corson: “Mobile Ad-hoc Networks (MANET) and The IETF” Volume 2 Issue 1, January 1998, Pages 9-14.

[3] Jun-Zhao Sun, Machine Vision & Media Process Unit, Oulu Univ, Finland: “Mobile Ad Hoc Networking: An Essential Technology for Pervasive Computing”, pp. 316 - 321 vol.3, 2001

[4] J. Douceur “The Sybil Attack” In First International Workshop on Peer- to-Peer Systems, pages 251–260, 2002.

[5] J. Newsome, E. Shi, D. Song, and A. Perrig, “The Sybil Attack in Sensor Networks: Analysis & Defences.” Proc. Of International symposium on information processing in sensor networks, pp 259–268, 2004.

[6] Murat Demirbas, Youngwhan Song, “An RSSI-based Scheme for Sybil Attack Detection in Wireless Sensor Networks”, In Proceedings of WoWMoM 2006 International Symposium on a World of Wireless, Mobile and Multimedia Networks, 2006. 5 pp. – 570

[7] M. Raya and J.-P. Hubaux, (2007)” Securing vehicular ad hoc networks”. Journal of Computer Security, 15(1), 39–68.

[8] G. Guette and C. Bryce, “Using TPMs to Secure Vehicular Ad-Hoc Networks (VANETs),” Proc. of WISTP 08, LNCS 5019, pp. 106-116, 2008.

[9] H. Chan, A. Perrig, and D. Song “Random key pre-distribution schemes for sensor networks” . In IEEE Symposium on Security and Privacy, pages 197–213, Berkeley, California, May 11-14 2003.

[10] R. Anderson and M. Kuhn “Tamper resistance - a cautionary note” In Proceedings of the Second Usenix Workshop on Electronic Commerce, pages 1–11, November 1996.

[11] L. Eschenauer and V. D. Gligor “A key-management scheme for distributed sensor networks”. In Proceedings of the 9th ACM conference on Computer and communications security, November 2002.

[12] S. Park, B. Aslam, D. Turgut, Cliff C. Zou (2009)” Defense against Sybil attack in vehicular ad-hoc network based on roadside unit support”. In: MILCOM, pp. 1–7.

[13] T. Zhou, R.R. Choudhury, P. Ning and K. Chakrabarty, “Privacy-Preserving Detection of Sybil Attacks in Vehicular Ad Hoc Networks,” Proc. of International Conference on MobiQuitous 2007, pp. 1-8, 2007.

[14] Kenza Mekliche, Dr. Samira Moussaoui L-P2DSA, “Location-based privacy-preserving detection of Sybil attacks,” Programming and Systems (ISPS), 2013 11th International Symposium on Digital Object Identifier: 10.1109/ISPS.2013.6581485 Publication Year: 2013, Page(s): 187-192

[15] Zhou Wang, Chunxiao Chigan, “Countermeasure Uncooperative Behaviors with Dynamic Trust-Token in VANETs” Communications, 2007. ICC '07. IEEE International Conference on Digital Object Identifier: 10.1109/ICC.2007.652 Publication Year: 2007, Page(s): 3959- 3964

[16] Bayrem Triki, Slim Rekhis, Mhamed Chammem, and Noureddine Boudriga, “A Privacy Preserving Solution for the Protection Against Sybil Attacks in Vehicular Ad Hoc Networks” Wireless and Mobile Networking Conference (WMNC), 2013 6th Joint IFIP, Digital Object Identifier: 10.1109/WMNC.2013.6549051 Publication Year: 2013 , Page(s): 1-8

[17] LEE, E.-K., YANG, S., OH, S. Y., AND GERLA, M “RF-GPS: RFID assisted localization in vanets” Mobile Adhoc and Sensor Systems, 2009. MASS ’09. IEEE 6th International Conference on (October 2009).

[18] Azzedine Boukerche, Horacio A.B.F. Oliveira, Eduardo F. Nakamura, Antonio A.F. Loureiro: “Vehicular Ad Hoc Networks: A New Challenge for Localization-Based Systems” , Volume 31 Issue 12, July 2008, Pages 2838-2849

[19] R. Parker, S. Valaee: “Vehicle localization in Vehicular Networks” , in: Vehicular Technology Conference, 2006. VTC-2006 Fall. 2006 IEEE 64th, 2006, pp. 1–5.