International Journal of Engineering Research ISSN:2319-6890)(online),2347-5013(print)
Volume No.5, Issue No.7, pp : 572-577 1 July 2016

Mitigation of Grayhole Attack in Vanet Using Clustering and Neighbour Node Information

Alla Rang, Lalit Mann Singh
Dept. of CSE ,Sri Guru Granth Sahib World University
Kingbleem2@gmail.com, Lalitmann19@gmail.com

Abstract: VANET is the field of networking that deals with vehicles. In VANET it is a vehicular and ad-hoc network that works same as MANET, In VANET two types of communication occur between vehicles that is Vehicle to vehicle communication and vehicle to road side communication. In this paper to overcome this issue of malicious nodes available in VANET neighboring information of the nodes have been utilized. The attack nodes create fraudulent identities of other nodes to disrupt network, transmission and topologies. To remove the neighboring nodes information is collected and compared with the threshold values for detection of malicious node.

Keywords: VANET, RSU, Grey hole attack, PDR with PMOR.

1. INTRODUCTION

1.1 VANET

Vehicular ad-hoc network (VANET) is sub class of mobile ad-hoc network (MANET). MANETS are ad-hoc networks and those types of networks which can alter their location and configure it. They use wireless channel, satellite channel and cellular transmission for communication because these are mobile networks which change their position after every interval. In VANETs vehicles can communicate with road side equipment which is also called as vehicle to roadside communication. In VANETs or MANETs it is not necessary that nodes have internet connection. Roadside equipment can have wireless connection by which vehicles can send data.

1.2 ROUTING IN VANET

For communication Ad-hoc networks are used. Ad-hoc Network is initially used for the MANETs but now they are used for the VANETs also.VANET utilizes these location based and topology-based steering conventions obliges that each of the partaking hubs be allocated a novel location. This intimates that we require an instrument that can be utilized to appoint interesting locations to vehicles yet these conventions don't promise that the copy locations are doled out in a system or not. Consequently, existing circulated tending to calculations utilized as a part of versatile specially appointed systems are significantly less suitable in a VANET environment. Particular VANET-related issues, for example, system topology, portability designs, thickness of vehicles at diverse times of the day, fast changes in vehicles arriving and leaving the VANET and the way that the width of the street is regularly littler than the transmission run all make the utilization of these routine specially appointed directing conventions lacking.

1.3 SECURITY

It is basic that data can't be embedded or altered by a noxious individual. Somebody orders aggressors as having three measurements: "insider versus outcast", "noxious versus objective", and "dynamic versus inactive" (G., 2010). The sorts of assaults against messages, can be depicted as takes after: "False Information", "Conning with Positioning Information", "ID divulgence", "Disavowal of Service", and "Masquerade". The unwavering quality of a framework where data is accumulated and imparted among elements in a VANET raises worries about information legitimacy. Case in point, a sender could distort perceptions further bolstering increase good fortune (e.g., a vehicle erroneously reports that its coveted street is stuck with activity, in this manner urging others to evade this course by changing course and giving a less congested outing).
There are various threats in VANET like threats to availability, threats to authenticity, threats to confidentiality (A. G. F., 2013). These threats include denial of service attack, malware attack, spamming, black hole attack, masquerading, reply-back attack, GPS spoofing, tunneling, position faking attack.

1.4 GRAY HOLE ATTACK

In gray hole attack, a node that is a member of the network, gets RREQ packets and creates a route to destination. After creating route, it drops some of data packets. This kind of dropping against Gray hole, does not drop all data packets. Attacker drops occasionally packets. It means attacker sometimes acts like a normal node and other times as a malicious node. [4]The Gray Hole attack has two phases. Initially, a malicious node exploits the AODV protocol to advertise itself as having a valid route to a destination node, with the intention of intercepting packets, even though the route is spurious. Next, the node drops the intercepted packets with a certain probability. This attack is more difficult to detect than the Gray Hole attack where the malicious node drops the received data packets with certainty. A Gray Hole may exhibit its malicious behavior in various techniques. It simply drops packets coming from (or destined to) certain specific node(s) in the network while forwarding all the packets for other nodes. Another type of Gray Hole attack is a node behaves maliciously for some particular time duration by dropping packets but may switch to normal behavior later. A Gray Hole may also exhibit a behavior which is a combination of the above two, thereby making its detection even more difficult.

2. RELATED WORK

Swati Verma et.Al [1] "Impact of Gray Hole Attack in VANET" Vehicular Ad Hoc Network (VANET) is a technology

which accommodates the vehicle to interconnect with each other through a wireless network. So that it can track and locate other vehicles to provide road safety. Any fixed infrastructure is missing so effective route for transporting data communication is established. Security is a major issue in VANET as it can be life threatening. V ANET is a subclass of ad hoc network and it is almost same as Mobile Ad Hoc Networks (MANET) but in V ANET nodes are vehicles. It is a challenging topic because of frequent link disruptions caused by vehicle mobility. We have used AODV routing protocol in VA NET for proper communication between nodes by forwarding data packets. We have implemented the gray whole attack on routing protocol AODV and shown its impact on implementation of VA NET. We have analyzed variable parameters like a packet delivery ratio (PDR), normalized routing load (NRL), delay and throughput.

Faisal Khan et. al. [2] "Recovering VANET Safety Messages in Transmission Holes" in this paper The core concern in vehicular ad hoc networks (VANETs) is the reliable transfer of safety-related messages to all endangered vehicles on the road. The recent discovery of the presence of transmission holes in the VANET communication range poses a serious challenge in the reliable safety-message dissemination. In this work, a technique for recovering the safety message for vehicles located in transmission holes is proposed. Each vehicle that successfully receives the safety message actively estimates propagation loss for its immediate neighbors. When the receiving vehicle determines a neighbor located in a coverage hole, the safety message is rebroadcast by the receiving vehicle. The propagation-loss estimation makes use of the topology information appended in the periodic beaconing messages. Contention among multiple rebroadcasts is resolved by using the relay schedule mechanism. The proposed technique is evaluated using a detailed implementation in the ns-3 network simulator. The simulation results suggest that the proposed technique guarantees the safety-message dissemination with a minimal overhead delay of five milliseconds even in the dense-urban traffic scenario.

Ambuj Kumar ET.Al[3] "An Efficient Group-Based Safety Message Transmission Protocol for VANET" Vehicular Ad-hoc Network (VANET) is a type of mobile communication in which topology changes dynamically due to high mobility of vehicles. Vehicles use two types of messages to update their status and to communicate with other vehicles. First is Periodic Safety Message (PSM) which gives us information about position, speed etc. and second is Event Driven Safety Message (ESM) which occurs when emergency situation like hard breaking, sudden lane change, etc. When vehicle movement is abnormal either due to change in speed or direction, vehicles generate event-driven safety alert messages. Safety alert messages are needed to be very fast and reliable for VANET applications. In this paper, we propose a novel approach to improve safety alert message communication in VANET using grouping of vehicles. Firstly, vehicles form a group and select their Group Leader to communicate with other Group Leaders. Secondly, we send the safety alert message by using priority in the messages and context-based communication. The priority is set according to various types of accidents and by using context-based communication the ESM messages are send to those groups which are endangered by the accidents. Simulation of proposed scheme is performed on multi-lane roads by considering vehicles movement in a single direction. Performance is evaluated in terms of packet delivery ratio and back-off counter for multi-hop broadcast communication.

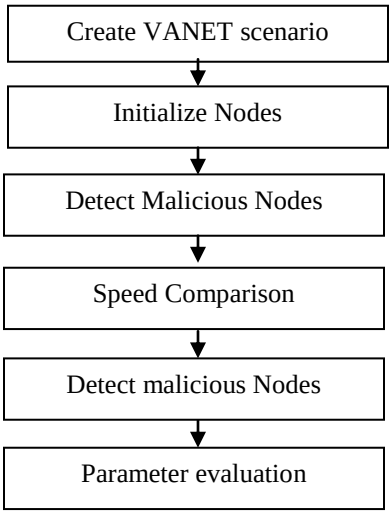
Ikechukwu K. AzoguET.Al[4] "A New Anti-Jamming Strategy for VANET Metrics-Directed Security Defense" As Vehicular Ad-hoc Network (VANET) becomes a critical infrastructure for road safety and traffic efficiency, its standardization and deployment face serious security challenges. The nature of VANET hinders ineffective most of existing defense schemes for wireless/mobile networks. This paper studies the impact of jamming on 802.11p, the standard of vehicle-to-vehicle (V2V) communications. Jamming, a category in Denial-of-Service (DoS) attack is a legacy in wireless communications. Although some detections and countermeasures of jamming-style DoS attacks have been proposed for generic 802.11 wireless local area networks, few is tested for 802.11p. Specifically, retreat strategies fail to mitigate jammers in VANET as geography may prohibit escaping from a jammed area, and the only one control channel for safety critical messages in 802.11p excludes channel hopping. Likewise, competition strategies such as tuning the carrier sense threshold does not respond fast enough to high-speed mobility. This work proposes a hideaway strategy, suitable for anti-jamming in VANET. The new strategy is perceived with a novel security metrics to measure the effectiveness of jammers, directing the design of defense mechanisms. The strategy utilizes Roadside Equipment's to shoulder off computation and communication tasks from Onboard Equipment's. A simulationstudy measures VANET efficiency protected by the new strategy compared to traditional schemes such as channel surfing. The study validates the VANET security metrics and the metrics directed approach of design for security schemes.

Claudia Campolo et.al[5] "Modeling Broadcasting in IEEE 802.11p/WAVE Vehicular Networks" IEEE 802.11p/WAVE (Wireless Access in Vehicular Environments) is an emerging family of standards intended to support wireless access in Vehicular Ad Hoc Networks (VANETs).Broadcasting of data and control packets is expected to be crucial in this environment. Both safety-related and non-safety applications rely on broadcasting for the exchange of data or status and advertisement messages. Most of the broadcasting traffic is designed to be delivered on a given frequency during the control channel (CCH) interval set by the WAVE draft standard. The rest of the time, vehicles switch over to one of available service channels (SCHs) for non-safety related data exchange. Although broadcasting in VANETs has been analytically studied, related works neither consider the WAVE channel switching nor its effects on the VANET performance. In this letter, a new analytical model is designed for evaluating the broadcasting performance on CCH in IEEE 802.11p/WAVE vehicular networks. This model explicitly accounts for the WAVE channel switching and computes packet delivery probability as a function of contention window size and number of vehicles.

ISSN:2319-6890)(online),2347-5013(print)
1 July 2016

3. PROPOSED METHODOLOGY

In the proposed work various steps have to be carried out for achieving the desired objective. In the completion of these objectives the phases have been described below:



Phase 1: In the first phase of the proposed work VANET scenario has been designed by initializing Lanes, vehicles and RSU. These lanes have different speed structure and RSU sense the coordinates of the vehicles available on the road.

Phase 2: In the second phase the malicious node has been introduced in the network that creates the duplicate ID of the other nodes available in the network and the position of the origin al node representing them on the other location that breaks the communication of the node.

Phase 3: In third phase the detection of the malicious node has been done by using the neighboring information. The speed of each node is compared with other nodes available in the neighbor. If the speed of the node is compared with its threshold value that has been defined by RSU. On the basis of comparison, legitimate and malicious nodes have been detected. After detection of malicious node, RSU broadcast message to all nodes available. Various parameters have been computed for performance evaluation of proposed work. These parameters are PDR, Packet loss, Collision avoidance and throughput.

4. RESULTS AND DISCUSSIONS

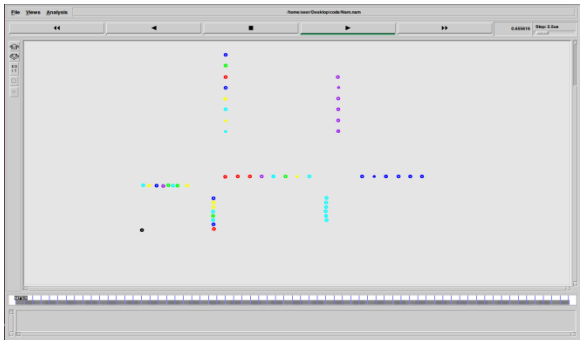


Fig 4.1: Initialization of nodes

This figure is use to represent the number of nodes in the network. The number of nodes in this network is 52.

Fig 4.2: Mobility between vehicles

This figure is use to represent the mobility between the vehicles. The nodes start moving from one location to other location.

Fig 4.3: Represent Clustering

This figure is use to represent the clustering between the nodes. The nodes have been divided into different cluster on the basis of their properties. After clustering cluster head selection has been done.

Fig 4.4: Cluster Head Selection

This figure is use to represent the selection of cluster heads. The cluster head is selected on the basis of distance from other cluster nodes.

ISSN:2319-6890)(online),2347-5013(print)
1 July 2016

Fig 4.5: Data Monitoring during Transmission

This figure is use to represent the monitoring of data during the data transmission. During data monitoring message has been monitor that provides information about whole route occupied by the message header format in the message.

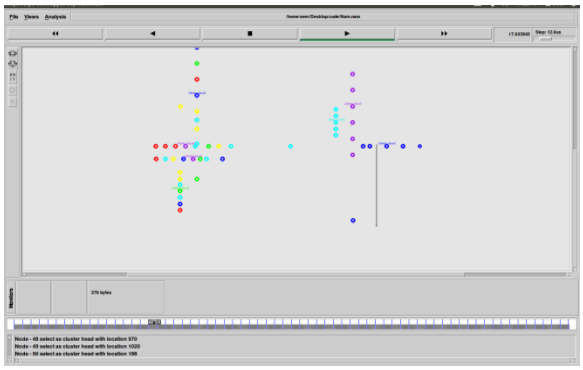


Fig 4.6: Data Monitoring during CBIR

This figure is use to represent the Data monitoring during CBIR i.e. component based image retrieval.

Fig 4.7: Gray Hole Attack Detection

This figure is use to represent the detection of Gray Hole Attack. The gray whole attack has two phases. In the first phase, a malicious node exploits the AODV protocol to advertise itself as having a valid route to a destination node, with the intention of intercepting packets, even though the route is spurious. In the second phase, the node drops the intercepted packets with a certain probability. This attack is more difficult to detect than the black hole attack where the malicious node drops the received data packets with certainty.

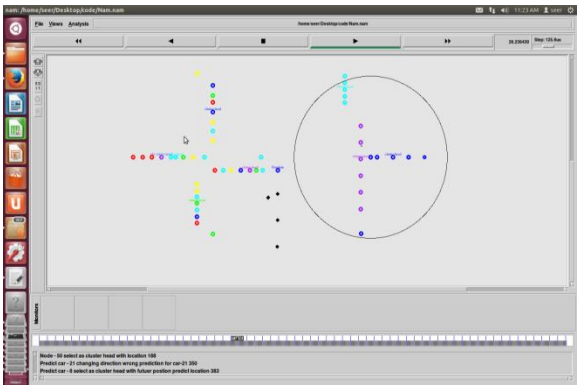


Fig 4.8: Broadcasting of Malicious Node on the network

The disrupting of the network by malicious nodes may cause problem in the transmission of valid information to the nodes available in the network. To detect the malicious nodes available in the network for avoiding the collision neighbor nodes information has been captured. For removing the malicious nodes available in VANET neighboring information of the nodes have been utilized.

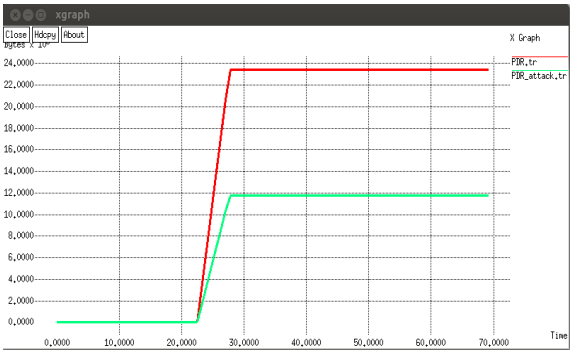


Fig 4.9:Loss

Loss is defined as the difference between total numbers of bytes sent and total number of bytes received. Figure 4.9 shows that there is very less loss which shows that network is performing well. But on the other hand loss for existing work which is represented by green line is much more as compare to existing one.

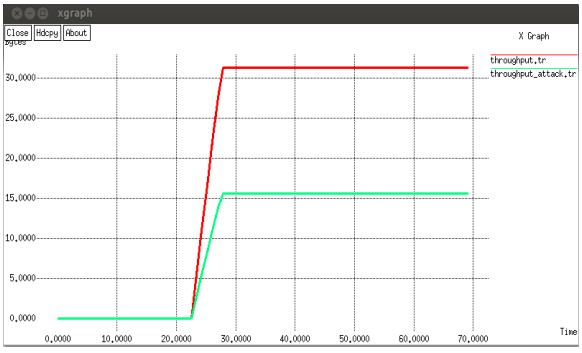


Fig 4.10:Throughput

Throughput is a total number of successful bytes received per unit time. So, figure 4.10 shows the calculated throughput for the

ISSN:2319-6890)(online),2347-5013(print)
1 July 2016

nodes. In this graph red line represents current work and green line is for existing work which is very less as compare to this work.

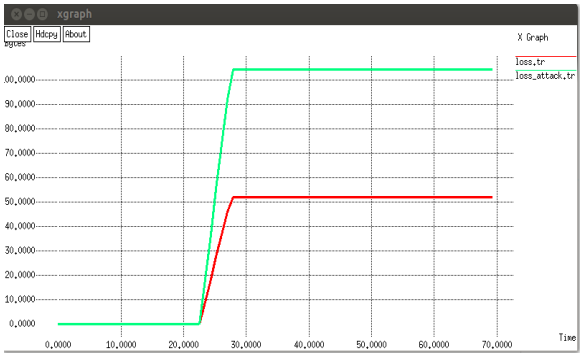


Fig 4.11: Packet Loss

Loss is defined as the difference between total numbers of bytes sent and total number of bytes received. Figure 4.11 shows that there is very less loss which shows that network is performing well. But on the other hand loss for existing work which is represented by green line is much more as compare to existing one.

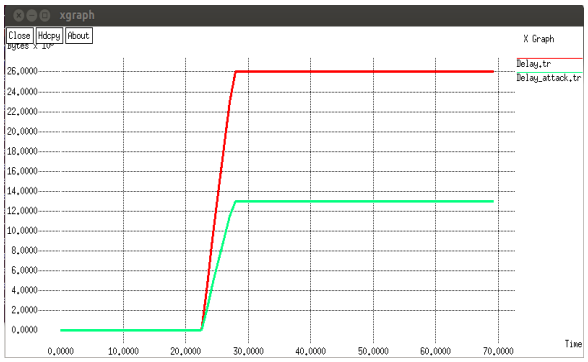


Fig 4.12: Delay

Delay is the time taken by bytes to reach its destination. Graph in picture shows that delay for this network is very less which means network performance is good but for existing work (represented by green line) delay is very high as compare to current work.

5. CONCLUSION AND FUTURE SCOPE

VANET is the field of networking that deals with vehicles. Various types of attacks are occurred in VANET. Environment safety message have to be transmitted in real time so that collision between different vehicles can be avoided. By performing attacks create an innumerable prudent identity for disturbing the network. The disrupting of the network by malicious nodes may cause problem in the transmission of valid information to the nodes available in the network. To detect the malicious nodes available in the network for avoiding the collision neighbor nodes information has been captured. To eliminate the issue of malicious nodes neighboring information of the nodes have been utilized. We used PDR, PMOR & neighboring information. At last we evaluate various parameters PDR, Packet loss, Collision avoidance and throughput for performance evaluation & on the basis of these parameters we conclude that our system gives us better results.

In the future gray hole attack can be detected by using encryption approaches that use key phase for a genuine node to transmit data.

REFERENCES

i. *Swati Verma "Impact of Gray Hole Attack in VANET"IEEE International Conference on Next Generation Computing Tecologies, 2015, pp-127-130.*

ii. *Faisal Khan "Recovering VANET Safety Messages in Transmission Holes" IEEE International Conference on Information and Communication Technology, 978-1-4799-2969-6/13/$31.00 ©2013.*

iii. *Ambuj Kumar "An Efficient Group-Based Safety Message Transmission Protocol for VANET" IEEE International Conference on Communication and Signal Processing, 2013, pp- 270-274.*

iv. *Ikechukwu K. Azogu "A New Anti-Jamming Strategy for VANET Metrics-Directed Security Defense" IEEE International Conference on vehicular network evolutlon,2013,pp-1344-1349.*

v. *Claudia Campolo "Modeling Broadcasting in IEEE 802.11p/WAVE Vehicular Networks" IEEE International Conference on COMMUNICATIONS LETTERS, 2011, pp- 1089-7798.*

vi. *Bertrand Ducourthial. "Conditional Transmissions: Performance Study of a New Communication Strategy in VANET" IEEE International Conference on TRANSACTIONS ON VEHICULAR TECHNOLOGY, 2007, pp-3348- 3357.*

vii. *Y. Bevish Jinila "A PRIVACY PRESERVING AUTHENTICATION FRAMEWORK FOR SAFETY MESSAGES IN VANET" IEEE International Conference on Sustainable Energy and Intelligent Systems, 2013, pp-446-461.*

viii. *F. A. Ghaleb, M. A. Razzaque, I.F. Isnin "Security and Privacy Enhancement in VANETs using Mobility Pattern," IEEE, 2013.*

ix. *G. Samara, A.H. Wafaa Al-Salihy, R. Sures "Security Issues and Challenges of Vehicular Ad Hoc Networks (VANET)," IEEE, 2010.*

x. *Seuwou. P, Patel. D, Protheroe.D, Ubakanma.G,"Effective Security as an ill-defined Problem in Vehicular Ad hoc Networks (VANETs)", IEEE Conf. on VANET, 2012, PP 34-43.*

xi. *Y. Qian, K. Lu, and N. Moayeri"Performance Evaluation of A Secure Mac Protocol for Vehicular Networks," IEEE, 2008.*

xii. *Hung.C.C, Chan.H "Mobility Pattern Aware Routing for Heterogeneous Vehicular Networks", IEEE Communications Society publication in the WCNC, 2008.*

xiii. *Dias .A.J. "Test bed-based Performance Evaluation of Routing Protocols for Vehicular Delay-Tolerant Networks" 45th Annual Simulation Symposium, IEEE.*

xiv. *Sumra A.I. et.al. Proposed "Trust Levels in Peer-to-Peer (P2P) Vehicular Network", 2012, PP 123-130.*

xv. *Lu Chen, Hongbo Tang, Junfei Wang "Analysis of VANET Security Based on Routing Protocol Information" ISSN 978-1-4673-6249-8, pp 134-138 2013 IEEE.*

xvi. *Irshad Ahmed Sumra, Halabi Hasbullah, Jamalul-lail Ab Manan"VANET Security Research and Development Ecosystem" ISSN NO. 978-1-4577-1884-7, 2011 IEEE*

xvii. *Jason J. Haas and Yih-Chun Hu, Kenneth P. Laberteaux "Real-World VANET Security Protocol Performance (Haas, 2009)" ISSN NO. 978-1-4244-4148-8, IEEE 2009.*

xviii. Josiane Nzouonta, Neeraj Rajgure, Guiling (Grace) Wang, Cristian Borcea "VANET Routing on City Roads Using Real Time Vehicular Traffic Information" VOL. 58, NO. 7, pp 3609-3626, SEPTEMBER 2009.

xix. Yen-Wen Lin "Optimal Next Hop Selection for VANET Routing" in International Conference on ICT Convergence (ICTC), 2011, pp. 737-741.

xx. Chia-Chen Hung, H. Chan, and Eric Hsiao-Kuang Wu "Mobility Pattern Aware Routing for Heterogeneous Vehicular Networks," IEEE WCNC 2008.

xxi. GMT Abdalla, SM Senouci "Current Trends in Vehicular Ad Hoc Networks," in proceedings of UBIROADS workshop, 2007.

xxii. Hoang Anh Nguyen et.al. "Opportunistic Networks (OPPNET)", International Journal of Ambient Computing and Intelligence.

xxiii. Muhammad A. Javed and Jamil Y. Khan " A Geocasting technique in an IEEE 802.11p based vehicular Ad hoc network for road traffic management" IEEE

xxiv. M.S. Al-Kahtani, "Survey on Security Attacksin Vehicular Ad hoc Networks (VANETs)," IEEE, 2012.

xxv. M Raya, P Papadimitratos, JP Hubaux, "Securing Vehicular Communications", IEEE Wireless Communications, vol 13, 2006

xxvi. M Raya, J Pierre Hubaux," The security of VANETs," in proceedings of the 2nd ACM international workshop on Vehicular ad hoc networks, 2005.

xxvii. M. A. Javed and J. Y. Khan "A Geocasting Technique in an IEEE 802.11p based Vehicular Ad hoc Network for Road Traffic Management," 2010.

xxviii. Mrs. Vaishali D. Khairnar, Dr. Ketan Kotecha "Simulation-Based Performance Evaluation of Routing Protocols in Vehicular Ad-hoc Network" Volume 3, Issue 10, ISSN 2250-3153, October 2013.

xxix. N. Sastry, U. Shankar and D. Wagner. "Secure Verification of Location Claims". In ACM Workshop on Wireless Security. WiSe 2003.