An Analytical Study of Routing Attacks in Vehicular Ad-hoc Networks (VANETs)

Priyanka Sirola
M.Tech Scholar, Computer Science & Engineering
Graphic Era Hill University
Dehradun, Uttarakhand-India
E-mail: priyanka.sirola@gmail.com

Amit Joshi
M.Tech Scholar, Computer Science & Engineering
Graphic Era Hill University
Dehradun, Uttarakhand-India
E-mail: joshiamit93@gmail.com

Kamlesh C. Purohit
Assistant Professor, Department of Computer Applications
Graphic Era University
Dehradun, Uttarakhand-India
E-mail: kamleshpurohit80@gmail.com

Abstract— ***Vehicular Ad-hoc Network (VANET) is a rising & most challenging research area to provide Intelligent Transportation System (ITS) services to the end users. The implementation of routing protocols in VANET is an exigent task as of its high mobility & frequent link disruption topology. VANET is basically used to provide various infotainment services to each and every end user; these services are further responsible to provide an efficient driving environment. At present, to provide efficient communication in vehicular networks several routing protocols have been designed, but the networks are vulnerable to several threats in the presence of malicious nodes. Today, security is the major concern for various VANET applications where a wrong message may directly or indirectly affect the human lives. In this paper, we investigate the several security issues on network layer in VANET. In this, we also examine routing attacks such as Sybil & Illusion attacks, as well as available solutions for such attacks in existing VANET protocols.***

Keywords- Vehicular Ad-hoc Network (VANET), Intelligent Transportation System (ITS), On-board Unit (OBU), security attacks, privacy.

I. INTRODUCTION

With the rapid improvements in the wireless technologies & the importance of Internet as an essential part of our lives, a new expectation of a Wi-Fi environment is emerging rapidly. This has results to the development of a special category of wireless ad hoc networks called Vehicular Ad-hoc Network (VANET). VANET is an evolved from of Mobile Ad-hoc Network (MANET) where each node (vehicle) moves freely within the network coverage area & provides various types of communications such as Inter Vehicular communication, Vehicle to Roadside Communication & Inter Roadside Communication.

As per the report given by the U.S Federal Communication Commission (FCC) in 1999, it has been decided that the 75*MHz* of Dedicated Short Range Communication (DSRC) spectrum at 5.9*GHz* will be exclusively used for VANET. DSRC is based on the 802.11p amendment, which adds Wireless Access in Vehicular Environments (WAVE) & is used for ITS. The IEEE has provided various standards such as IEEE 1609.1, 1609.2, 1609.3, 1609.4, 802.11p & 802.16e for the efficient deployment of vehicular networks. VANET is a self organized network in which every vehicle consists of an On-board Unit (OBU) & a Temper Proof Device (TPD). An OBU connects each vehicle with RSUs via DSRC radios, that enables communication between vehicles & RSUs and a TPD is used to hold the vehicles safety information like keys, speed, routes, identities, etc… [1] [2] [3]. In VANET, vehicles share their traffic situations or information with one another after sensing their traffic environment to enable road safety, efficient driving & infotainment. Figure 1 illustrates the architecture of Vehicular Ad-hoc Network.

Routing in VANET has been studied & discussed widely in the past few years. Routing protocols in VANET can be categorized as unicast, multicast, broadcast & geocast. Routing in VANET is a challenging task due to its high mobility & frequent link disruption topology [4]. For the above said reasons vehicular communication is critically insecure to various threats; so security is an important aspect for the deployment of VANET to make available Intelligent Transportation System (ITS) services to each and every end user.

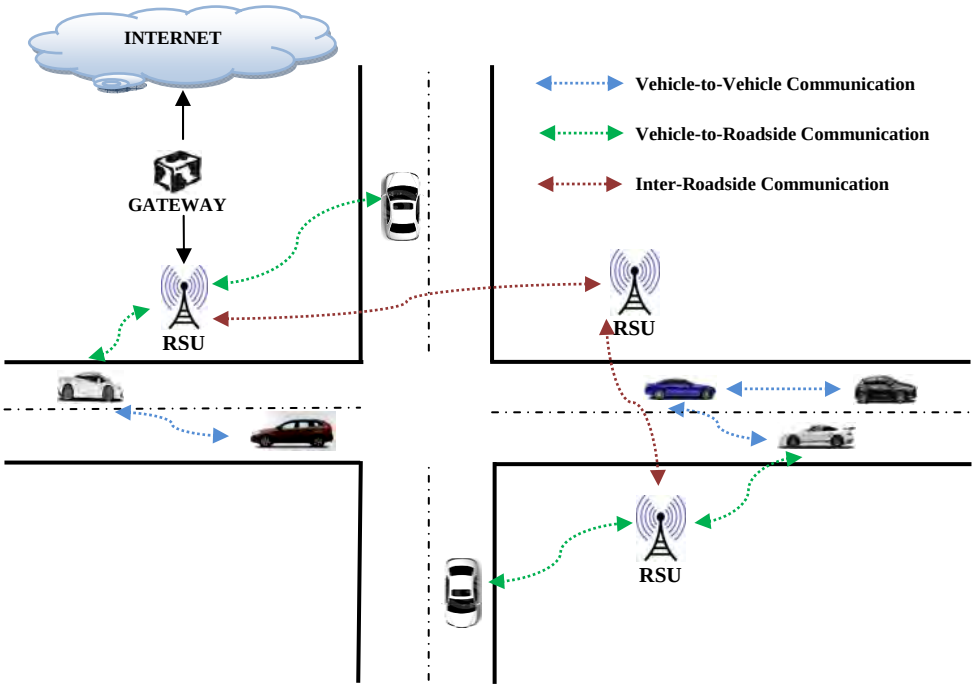

Figure 1: Vehicular Ad-hoc Networks (VANETs)[5]

ITS services consist of three broad applications such as safety, non-safety & infotainment. The safety application is one of the most important application in ITS. Most VANET based applications such as, lane change warning, blind spot warning, collision warning, congested road notification, parking availability notification etc… need the cooperation of vehicles [6]. For this reason, routing attacks are serious threats for VANET. VANETs should follow the security requirements such as integrity, confidentiality, authentication, availability & non-repudiation to deal with life critical information and to provide secured communication against malicious nodes [7]. To provide crash avoidance safety system programs, the U.S Department of Transportation (USDOT) is working cooperatively with major automobile manufacturers such as Ford, Honda, General Motors, Hyundai Kia, Nissan, Toyota, Mercedes-Benz, & Volkswagen-Audi.

After studying various literatures, we have analyzed that most of the existing work mainly discussed about effective approaches that provide protection to the routing protocols in VANET. These approaches are mainly based on cryptography & key management schemes to avoid the malicious nodes from joining the network. But, the main disadvantage of these approaches is that they are too heavy & expensive to deploy, therefore it is very difficult to use these schemes in real world due to VANET characteristics. In [8], the author provides a survey on security attacks in VANETs. However some attacks such as Denial of Service (DoS) attack, Black Hole attack & their countermeasures have not been discussed properly in it. In this paper, we provide a survey of attacks on the network layer, that is, routing attacks such as Denial of Service (DoS), Black Hole & Sinkhole attacks, as well as countermeasures in VANET. Then, we give a brief overview of available approaches for each routing attack.

The rest of the paper is organized as follows. Section 2 presents several security attributes in VANETs. In section 3, we provide an analytical study of routing attacks against VANETs. In section 4, we provide a brief overview of countermeasures against routing attacks. Then we summarize the paper in section 5 and the conclusion & future work is depicted in section 6.

II. SECURITY ATTRIBUTES

There are several essential requirements to achieve security in VANETs. In this section, we provide several security attributes that should be followed by VANET [7].

- **Authentication:** In vehicular communication, it is very essential to authenticate the sender of a message to prevent impersonation.
- **Confidentiality:** It is necessary that the privacy of each entity must be sheltered. Directional antennas & encrypted data should be use to provide confidentiality.
- **Integrity:** Intactness for all messages must be protected to prevent intruders from altering the message contents so that the information can be trusted.

- **Non-repudiation:** Through it, we will be able to induce the ability to identify the attacker even after its occurrence. It prevents deceivers from denying their crimes.
- **Availability:** It will insure that the network resources must be available to the authorized users even if the communicating entities are under an attack by using alternative mechanisms without affecting the network's performance.

III. ROUTING ATTACKS AGAINST VANET

A. Denial of Service (DoS) Attack

Denial of Service (DoS) attack [9] can be done by the network insiders & outsiders. An insider attacker may jam the channel after transmitting dummy messages & thus, stops the network connection. An outsider attacker can launch a DoS attack by repeatedly disseminating forged messages with invalid signatures to consume the bandwidth or other resources of a targeted vehicle. The impact of this attack is that, VANET losses its ability to provide services to the legitimate vehicles. Figure 2 illustrates a Denial of Service (DoS) attack in which a malicious vehicle transmits a dummy message to an RSU & also to a legitimate vehicle behind it in order to create a jam in the network.

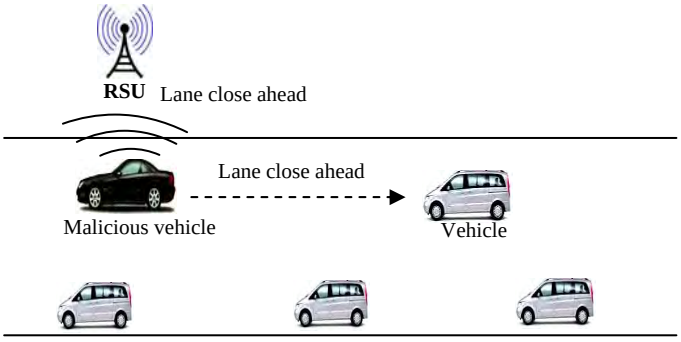

Figure 2: Denial of Service (DoS) Attack

B. Black Hole Attack

In Black Hole attack [8], a malicious node pretends to have an optimum route for the destination node and indicates that packet should route through this node after transmitting the fake routing information. The impact of this attack is that the malicious node can either drop or misuse the intercepted packets without forwarding them. Figure 3 illustrates a Black Hole attack where a Black Hole region is created by a number of malicious vehicles & they refuse to broadcast the received messages from the legitimate vehicles to the other legitimate vehicles behind them.

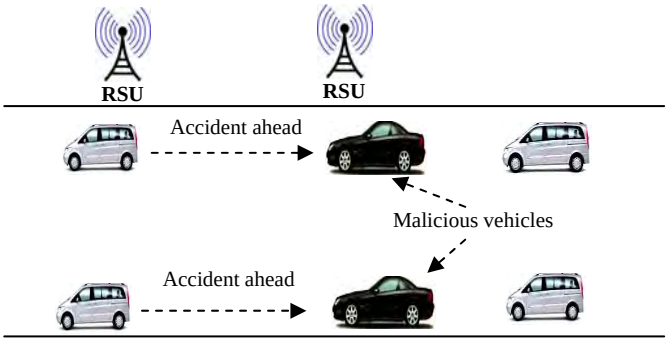

Figure 3: Black Hole Attack

C. Wormhole Attack

In Wormhole attack [10], a malicious vehicle receives the data packets at a point in the network and replays them to another malicious vehicle by using a wormhole high speed link (tunnel) & hence a source to destination communication proceeds through these malicious vehicles. The impact of this attack is that it prevents the discovery of valid routes & threatens the security of transmitting data packets. Figure 4 illustrates a Wormhole attack where two malicious vehicles use a tunnel to broadcast privacy information.

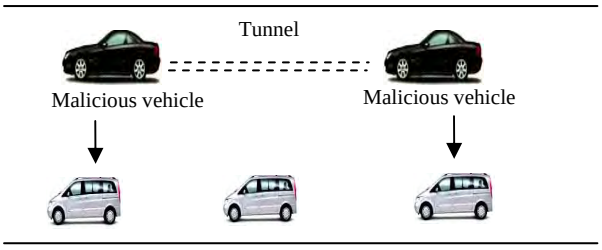

Figure 4: Wormhole Attack

D. Sinkhole Attack

In Sinkhole attack [11], a malicious vehicle broadcasts the fake routing information so that it can easily attract all the network traffic towards it. The impact of this attack is that it makes the network complicated & degrades the network performance either by modifying the data packets or by dropping them. Figure 5 illustrates a Sinkhole attack in which a malicious vehicle drops the data packets received from a legitimate vehicle & broadcasts fake routing information to the legitimate vehicles behind it.

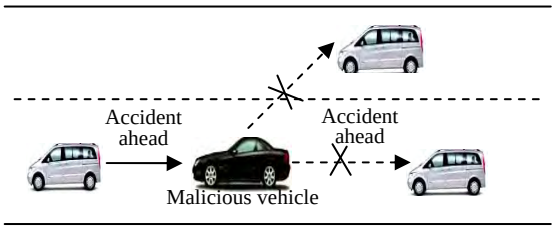

Figure 5: Sinkhole Attack

E. Illusion Attack

In Illusion attack [8] [12], attacker tries to purposely manipulates his/her sensor readings for giving falsify information about his/her vehicle. As a result, the system reaction invokes and false traffic warning messages are broadcast to neighbours. The impact of this attack is that it can easily change the driver's behaviour by spreading the wrong traffic information & can cause accidents, traffic jams and reduce the vehicular network efficiency by dropping the bandwidth consumption. Existing message authentication & message integrity approaches cannot secure networks against this attack as the malicious vehicle directly manipulates & misleads the sensors of its own vehicle to produce & broadcast the wrong traffic information. Figure 6 illustrates an Illusion attack where a malicious vehicle broadcasts the wrong traffic warning messages to vehicles at their neighborhood.

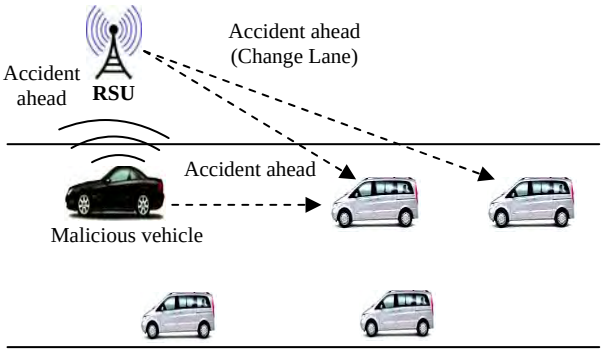

Figure 6: Illusion Attack

F. Sybil Attack

In Sybil attack [13], a malicious vehicle creates a large number of false identities in order to take over the control of whole VANET & inject fake information in the network to harm the legitimate vehicles. Sybil attack puts a great impact on the performance of the VANET by creating an illusion of existence of multiple vehicles in the network. The impact of this attack is that after spoofing the identities or positions of other vehicles in vehicular network, this attack may lead to other types of attack. Figure 7 illustrates a Sybil attack in which a malicious vehicle creates a number of false identities of many vehicles & produces an illusion of extra number of vehicles on the road.

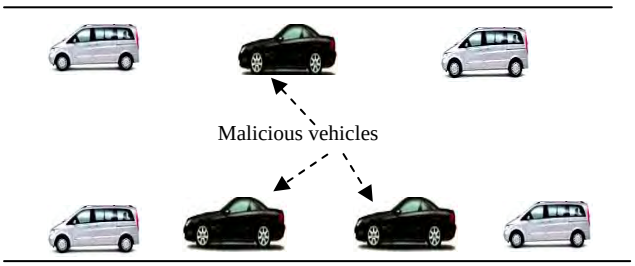

Figure 7: Sybil Attack

IV. COUNTERMEASURES AGAINST ROUTING ATTACKS IN VANET

A. Solutions to the Denial of Service (DoS) Attack

A pre-authentication scheme is an approach that detects Denial of Service attack launched by an outsider attacker [14]. This scheme is very efficient & robust because it can effectively mitigate such DoS attacks in VANETs, which are not in favor of signature based authentication. This scheme provides a pre-authentication process before signature verifying process. The pre-authentication process makes use of the one-way hash chain & a group rekeying scheme. In this scheme, if the message has passed the one-way hash chain-based authentication, the signature verification process of the message will be carried out by the receiver. Otherwise, it rejects to verify it.

An efficient approach is proposed to detect & defend against UDP flooding which is a common class of DoS attacks in different types of IP spoofing [15]. This approach can detect random as well as subnet spoofing. This approach uses an efficient data structure for storage & a Bloom filter based IPCHOCKREFERENCE (BFICR) detection method. An efficient data structure needs a table of fixed length to record applicable traffic information. A Bloom filter based IPCHOCKREFERENCE (BFICR) method is then used to discover sudden variations in the features of traffic which represent the flooding attack presence. After examine the hash table for the features of source IP, this approach can further categorize the detected malicious events into random, subnet spoofing. The detection rate of this approach is high & it is very effective, unique & robust which requires lesser amount of storage and computational costs.

An Attacked Packet Detection Algorithm (APDA) is another approach that detects DoS attacks before verification time [16]. This algorithm is used to detect the invalid requests & attacked packets. In this approach, RSUs play an important role; vehicles can send messages to RSU through APDA mechanism. This mechanism is used to store the vehicle information in the RSUs after detecting the data packets send by the vehicles & the position of the vehicles. If the data packet is not attacked, vehicle will not track. Otherwise, it will track. The benefit of this approach is that it minimizes the delay overhead for processing & enhances the security in VANET.

B. Solutions to the Black Hole Attack

A Detection, Prevention & Reactive AODV (DPRAODV) protocol [17] is proposed to defend against security threats of Black Hole attack. In DPRAODV protocol, a node detects the black hole (malicious) node & isolates it; so that the malicious node can't performs the data forwarding & routing. An ALARM packet is used to inform all other legitimate nodes about the malicious node. This ALARM packet consists of an identity of a black list node as its parameter. If the reply is sent from the blacklisted node, no processing is carried out. The advantages of this protocol are that it provides a safe scheme to prevent black hole attack in the network as well as upgrades the overall AODV protocol performance.

An efficient technique called BAMBi [18] is proposed to detect malicious (Black Hole) nodes in the network. This technique can be easily applied after the successful deployment of several base stations in the network architecture. This technique is used to eliminate the impact of malicious (black hole) nodes in the data transmission. This technique also route the copied data packets to these multiple base stations. This technique is very effective with higher detection rate & with negligible false positive rate. But due to the high mobility of vehicles, this technique is too heavy to deploy & is not realistic in VANET.

A security protocol is proposed [19] to recognize many Black Hole nodes in the network and to discover a secure & an optimal route from a source to a destination node. This proposed mechanism modifies the AODV protocol by introducing two new concepts in it named as data routing information (DRI) table scheme and cross checking scheme, which provide protection against a black hole attack. In first scheme (data routing information), during the route discovery process, additional information of two bits are transmitted by the nodes that respond to the RREQ message sent by a source node. In it, every node holds an extra data routing information (DRI) table. The second scheme (cross checking) relies on reliable nodes to transfer data packets. This protocol is very effective & provides a secure network for data transmission.

C. Solutions to the Wormhole Attack

An efficient technique called, HEAP [20] is proposed to defend against Wormhole attack in the network. This technique is based on AODV protocol. This technique is an improvement of previously proposed packet leashes method [10]. It is a packet authentication technique, which is responsible to authenticate packets at each & every hop by using an algorithm which is a modified form of HMAC-based algorithm. This algorithm uses two keys for packet authentication purpose & neglects those packets that originate from outsiders. The HEAP uses geographical leashes instead of temporal leashes for the detection of malicious nodes. But, geographical leashes limit the packets travel distance; therefore to eliminate this problem, the packets should be dropped from the HEAP whenever their travel distances are more than the claimed value. Otherwise, the packets are accepted. The benefits of this technique are that it doesn't need any additional or special hardware, it has low overhead and it is more secure as compare to other techniques.

A set of plausibility checks [21] is proposed to eliminate the influence of Wormhole attack on the position-based routing (PBR) and to assure the PBR reliability in Vehicular Ad-hoc Networks. A set of plausibility checks consists of the following checks in it: spatial checks (communication range, speed & density, moved distance, map location), temporal checks, strategy checks, overhearing checks & content checks. The advantage of this scheme is that it doesn't need any additional hardware to be added to the vehicles as the plausibility checks are logical rules.

A Wormhole Attack Detection Protocol using Hound Packet (WHOP) [22] is proposed to detect Wormhole attack in the network. It is based on AODV protocol. In this protocol, after the route discovery process, the wormhole detection process is initiated with the transmission of a hound packet by the source node. In the proposed solution, the Hound packet is being processed by each and every node other than those that are involved in the route discovery process from source node to destination node. Hound packet counts the difference of hops between the neighboring nodes which are located one hop away in the current path. If the hop difference between neighboring nodes exceeds the threshold value then the destination node identifies it as a wormhole. The advantage of this protocol is that it does not use any special hardware such as directional antennas & it is also free from physical medium of wireless network. This protocol has higher detection rate but the problem is that it also maximizes the processing delay of the packets.

D. Solutions to the Sinkhole Attack

A distributed model is designed [23] called Intrusion Detection System (IDS) to detect an ongoing Sinkhole attack. It is made up of the same IDS clients, which operate in every node in the network. These IDS clients are responsible to communicate with one another so that they can easily get a conclusion on an intrusion event. An IDS client consists of the following functionality: Network monitoring, Intrusion detection, Decision making & Action. Based on these functions, architecture of the IDS clients is built by using five conceptual modules & every conceptual module is responsible for a particular type of function such as local packet monitoring, cooperative detection engine, local detection engine, etc… This scheme is robust & provides a secure network. But it is too heavy to deploy in a realistic environment.

A mechanism [24] is proposed that uses Link Quality Indicator (LQI) based routing in wireless sensor network which is used to detect Sinkhole attack. This mechanism consists of mainly two types of phases in it; first phase is Network Initialization phase & second phase is Attack Detection phase. In first phase, the information is gathered which is used for the detection of sinkhole attack in the network. In it, general nodes are responsible for gathering lowest link cost in between each & every neighborhood node and detector nodes are responsible for computing minimum path cost & also link cost with each & every neighborhood node. In second phase, detector nodes are used to detect forgery of path cost in RREQ message & as a result abnormal signal strength is detected concerning minimum neighbor link cost table. This mechanism is very effective to detect sinkhole attack in the network but it is based on various assumptions, which are not realistic.

A mechanism [25] is proposed to detect & prevent Sinkhole attacks in the network. This mechanism consists of four types of phases or modules in it: Initialization, Storage, Investigation and Resumption. In Initialization module, AODV broadcasts the RREQ packets to all the neighbors & starts its route discovery process so that it can easily get the optimal shortest path from source to destination. In Storage module, essential information of each RREQ packet is stored in the routing table like destination sequence number, hop count, source address & destination address. In Investigation module, they are calculating the sequence numbers difference of current and previous requests for a source. If newly founded source sequence number for the present route request is very large than the previous request then the node from which we have received the current route request is believed as a faulty node & this RREQ packet is dropped from the current routing table. In Resumption module, SendRequest method of default AODV is called & as a result AODV starts behaving normally.

E. Solution to the Illusion Attack

To resolve the security threats of illusion attack, a new security model i.e. Plausibility Validation Network (PVN) model is proposed [12]. It is basically used to identify whether the message coming from the sensor is

valid or not. PVN takes two types of input data: incoming data from antennas & data collected by sensors. Data Type header is responsible to categorize the input data. The proposed PVN model consists of a checking module called Plausibility Network (PN) & a rule database, which are used to check the validity of input data & take necessary action accordingly. A message is reasonable if it passes all verifications. Otherwise, it is described as an invalid message and dropped automatically. PVN model requires that the messages (input data) should be cross verified efficiently.

F. Solutions to the Sybil Attack

To detect Sybil attack in VANET, a timestamp series approach is proposed [26] which is based on Road Side Unit (RSU) support. According to this approach, it is find in very few cases that two vehicles are passing by multiple RSUs at the same time. By following above said reason, if two or more messages have common timestamp series provided by the RSUs, then these messages will be taken as Sybil attack released by a vehicle. This approach is very efficient & cheap as it does not use any public key infrastructure (PKI). But this approach can not detect the Sybil attack in the scanerio where two vehicles coming from opposite sides, as both vehicles may receive same series of certificates from same RSU for some significant period of time.

A distributed security scheme is proposed [27] in which all nodes contribute for the detection of Sybil nodes in VANET. This scheme is totally based on the difference in movement patterns of Sybil nodes & normal nodes. In this approach, RSUs play an important role for detecting Sybil attack & for this each RSU follows four types of detection steps: collects the beacon packets from vehicles, calculate distance & angle of vehicles, calculate the difference values, identification & grouping of Sybil nodes. This approach works well in a large network but in small scale networks, it gives more false positive rates.

A distributed & robust approach is proposed [28] to defend against Sybil attack. In this approach, each node keeps a record of its neighboring nodes & also exchange groups of its neighboring nodes periodically & performs the intersection of these groups. If some nodes observed that they have similar neighbors for a significant duration of time i.e. a predefined threshold value (σ), these similar neighbors are identified as Sybil nodes. This approach consists of four phases in it to detect the Sybil nodes: periodic communication between vehicles, group construction of neighboring nodes, exchange groups with other nodes in vicinity, identify the vehicles comprising similar neighboring nodes. But this approach cannot detect the Sybil nodes in the scenario where the attack duration is shorter than the predefined threshold value (σ).

V. SUMMARY

Table 1 lists different types of routing attacks with their effects in the network & respective security requirements.

Table 2 provides a summary and offers a comparative analysis between the above described approaches and protocols for providing security in VANET.

Table 1: Comparison of routing attacks with their effects & security requirements

Attacks on Network Layer (Routing Attacks)	Impact/Effect	Security Requirements
Denial of Service (DoS) Attack	Reduce the performance & efficiency of the network	Availability
Black Hole Attack	Cause data packets to be lost & misuse or discard the traffic	Availability
Wormhole Attack	Prevent the discovery of valid routes & cause data packets to be lost	Authentication & Confidentiality
Sinkhole Attack	Make the network complicated, either by modifying the data packets or by drooping them.	Availability
Illusion Attack	Cause car accidents, traffic jams & reduce the performance of the network in terms of bandwidth utilization	Authentication
Sybil Attack	Take over the control of whole network & inject false information in it like traffic congestion, accident etc	Authentication

Table 2: Summary of various kinds of proposed approaches & their features

Proposed Approach/Protocol	Solution to	Based on	Node Density	PDR	Delay	Overhead	Throughput	Detection Rate	FPR	FNR	Evaluation Platform
Pre-authentication Approach [14]	DoS Attack	ND	L	ND	Authentication Delay (L)	ND	ND	ND	ND	ND	Simulation
BFICR Approach [15]	DoS Attack	UDP	H	ND	ND	Data storage Overhead (L)	ND	H	L	ND	Real Environment
APDA [16]	DoS Attack	ND	L	ND	ND	Delay Overhead (L)	ND	ND	D	ND	Simulation
DPRAODV Protocol [17]	Black Hole Attack	AODV	M	H	End-to-End Delay (M)	Normalized Routing Overhead (M)	ND	ND	D	ND	Simulation
BAMBi Approach [18]	Black Hole Attack	ND	H	H	ND	ND	ND	H	L	ND	Simulation
Modified AODV Protocol [19]	Black Hole Attack	AODV	L	M	ND	ND	ND	ND	ND	ND	Simulation
HEAP Approach [20]	Wormhole Attack	AODV	H	H	Delivery Delay (H)	Network Overhead (H)	M	ND	ND	ND	Simulation
Plausibility Check Approach [21]	Wormhole Attack	GPSR	H	H	ND	ND	ND	ND	ND	ND	Simulation
WHOP Protocol [22]	Wormhole Attack	AODV	H	ND	Processing Delay (M)	ND	ND	H	ND	ND	Simulation
IDS Model [23]	Sinkhole Attack	ND	H	ND	ND	ND	ND	H	ND	L	Simulation
LQI based Approach [24]	Sinkhole Attack	ND	H	ND	ND	ND	ND	H	L	ND	Simulation
Modified AODV Protocol [25]	Sinkhole Attack	AODV	M	H	End-to-End Delay (L)	ND	H	ND	ND	ND	Simulation
PVN Approach [12]	Illusion Attack	ND	H	ND	Check Delay (L)	Communication Overhead (M), Data Storage Overhead (M)	ND	ND	ND	ND	Simulation
Approach based on Movement patterns [27]	Sybil attack	ND	H	ND	ND	Computation Overhead (L)	ND	H	L	ND	Simulation
Approach based on Neighboring nodes [28]	Sybil attack	ND	M	ND	ND	ND	ND	H	L	L	Simulation

ND: Not determined, L: Low, M: Medium, H: High, PDR: Packet Delivery Ratio, FPR: False Positive Rate, FNR: False Negative Rate

VI. CONCLUSION & FUTURE WORK

Vehicular Ad-hoc Network (VANET) is most challenging & promising research area to provide Intelligent Transportation System (ITS) services to the end users. VANET applications can be categorized as safety applications, convenience applications & commercial applications. However, implementation of VANET poses a great challenge due to its high mobility, frequent link disruption topology & several security attacks. The main weakness of Vehicular Ad-hoc Network is that it doesn't have any centralized infrastructure in it; therefore it is susceptible to different security attacks.

In this paper, we reviewed several routing attacks & their countermeasures in VANET. For countermeasures, we described their advantages as well as their drawbacks. Most of the available approaches support cryptography & key management schemes. But, the major drawbacks of these available approaches are that they are too heavy & expensive to deploy, therefore it is very difficult to use these schemes in real world due to VANET characteristics. Some solutions works well in a large network but in small scale networks, it gives more false positive rates.

Future research work should be focused on improving the effectiveness of the security mechanisms so that they prevent all possible attacks in VANET and make it secure and reliable network & also on minimizing the implementation cost that makes them desirable for VANET.

REFERENCES

[1] Toor, Y., P. Muhlethaler, and A. Laouiti, Vehicle ad hoc networks: Applications and related technical issues. Communications Surveys & Tutorials, IEEE, 2008. 10(3): p. 74-88.

[2] Jiang, D. and L. Delgrossi. IEEE 802.11 p: Towards an international standard for wireless access in vehicular environments. in Vehicular Technology Conference, 2008. VTC Spring 2008. IEEE. 2008: IEEE.

[3] Qian, Y., K. Lu, and N. Moayeri. A secure VANET MAC protocol for DSRC applications. in Global Telecommunications Conference, 2008. IEEE GLOBECOM 2008. IEEE. 2008: IEEE.

[4] Lin, Y.-W., Y.-S. Chen, and S.-L. Lee, Routing Protocols in Vehicular Ad Hoc Networks A Survey and Future Perspectives. Journal of Information Science & Engineering, 2010. 26(3).

[5] Lin, X., et al., Security in vehicular ad hoc networks. Communications Magazine, IEEE, 2008. 46(4): p. 88-95.

[6] Mishra, B., et al. Security in vehicular adhoc networks: a survey. in Proceedings of the 2011 International Conference on Communication, Computing & Security. 2011: ACM.

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

[8] Al-kahtani, M.S. Survey on security attacks in Vehicular Ad hoc Networks (VANETs). in Signal Processing and Communication Systems (ICSPCS), 2012 6th International Conference on. 2012.

[9] Sumra, I.A., et al. Classes of attacks in VANET. in Electronics, Communications and Photonics Conference (SIECPC), 2011 Saudi International. 2011: IEEE.

[10] Hu, Y.-C., A. Perrig, and D.B. Johnson. Packet leashes: a defense against wormhole attacks in wireless networks. in INFOCOM 2003. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications. IEEE Societies. 2003: IEEE.

[11] Ngai, E.C.H., L. Jiangchuan, and M.R. Lyu. On the Intruder Detection for Sinkhole Attack in Wireless Sensor Networks. in Communications, 2006. ICC '06. IEEE International Conference on. 2006.

[12] Lo, N.-W. and H.-C. Tsai. Illusion attack on VANET applications-A message plausibility problem. in Globecom Workshops, 2007 IEEE. 2007: IEEE.

[13] Douceur, J.R., The sybil attack, in Peer-to-peer Systems. 2002, Springer. p. 251-260.

[14] He, L. and W.T. Zhu. Mitigating DoS attacks against signature-based authentication in VANETs. in Computer Science and Automation Engineering (CSAE), 2012 IEEE International Conference on. 2012: IEEE.

[15] Verma, K., H. Hasbullah, and A. Kumar. An efficient defense method against UDP spoofed flooding traffic of denial of service (DoS) attacks in VANET. in Advance Computing Conference (IACC), 2013 IEEE 3rd International. 2013: IEEE.

[16] RoselinMary, S., M. Maheshwari, and M. Thamaraiselvan. Early detection of DOS attacks in VANET using Attacked Packet Detection Algorithm (APDA). in Information Communication and Embedded Systems (ICICES), 2013 International Conference on. 2013: IEEE.

[17] Raj, P.N. and P.B. Swadas, DPRAODV: A DYANAMIC LEARNING SYSTEM AGAINST BLACKHOLE ATTACK IN AODV BASED MANET. International Journal of Computer Science Issues (IJCSI), 2009. 7(4).

[18] Misra, S., K. Bhattarai, and G. Xue. BAMBi: blackhole attacks mitigation with multiple base stations in wireless sensor networks. in Communications (ICC), 2011 IEEE International Conference on. 2011: IEEE.

[19] Sen, J., S. Koilakonda, and A. Ukil. A mechanism for detection of cooperative black hole attack in mobile ad hoc networks. in Intelligent Systems, Modelling and Simulation (ISMS), 2011 Second International Conference on. 2011: IEEE.

[20] Safi, S.M., A. Movaghar, and M. Mohammadizadeh. A novel approach for avoiding wormhole attacks in VANET. in Internet, 2009. AH-ICI 2009. First Asian Himalayas International Conference on. 2009: IEEE.

[21] Alsharif, N., A. Wasef, and X. Shen. Mitigating the effects of Position-Based Routing Attacks in Vehicular Ad Hoc Networks. in Communications (ICC), 2011 IEEE International Conference on. 2011: IEEE.

[22] Gupta, S., S. Kar, and S. Dharmaraja. WHOP: Wormhole attack detection protocol using hound packet. in Innovations in Information Technology (IIT), 2011 International Conference on. 2011: IEEE.

[23] Krontiris, I., et al., Intrusion detection of sinkhole attacks in wireless sensor networks, in Algorithmic Aspects of Wireless Sensor Networks. 2008, Springer. p. 150-161.

[24] Choi, B.G., et al. A sinkhole attack detection mechanism for LQI based mesh routing in WSN. in ICOIN. 2009.

[25] Gandhewar, N. and R. Patel. Detection and Prevention of Sinkhole Attack on AODV Protocol in Mobile Adhoc Network. in Computational Intelligence and Communication Networks (CICN), 2012 Fourth International Conference on. 2012: IEEE.

[26] Park, S., et al. Defense against sybil attack in vehicular ad hoc network based on roadside unit support. in Military Communications Conference, 2009. MILCOM 2009. IEEE. 2009: IEEE.

[27] Grover, J., M.S. Gaur, and V. Laxmi. A novel defense mechanism against sybil attacks in VANET. in Proceedings of the 3rd international conference on Security of information and networks. 2010: ACM.

[28] Grover, J., et al. A sybil attack detection approach using neighboring vehicles in VANET. in Proceedings of the 4th international conference on Security of information and networks. 2011: ACM.