ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 9, September 2016

An Effective Review on Attacks in Vehicular Ad Hoc Networks

Priyanka Mittal[1], Babita Yadav[2]

M.Tech. Student, Department of CSE, MVN University, Palwal, Haryana, India.[1]

Asst. Professor, Department of CSE, MVN University, Palwal, Haryana, India.[2]

ABSTRACT: In last few years, the VANET has gained a higher attention among researchers in academia and industry because of its powerful safety application and non safety application. Malicious subscribers are one of the types of intruders in VANET and generate the security issues. Confidentiality, integrity and availability (CIA) are important elements of security objectives. The increasing research interest, powerful applications, and security issue in VANET lead to the requirements to review the attacks on security objectives. In this paper, the goal is to present the review of attacks on security goals and to explain in details the nature of attacks and the behaviour of attackers through various scenarios in the network. The paper also offers a better understanding of security objectives and finally it offers an analysis and categorizes the attacks based on security goals into different attack levels that can support in the VANET implementation in real life.

KEYWORDS: Vehicular ad-hoc network (VANET) · Security goals · Confidentiality integrity availability (CIA) · Attacks

I. INTRODUCTION

Road accidents are one of the most critical attacks to human lives that can lead to complete or partial disability and results in death. Intelligent transportation system (ITS) is one of the techniques that have enhanced traffic systems by forwarding in safety information known as road to vehicle communication (RVC) to its clients on the highway [1]. Vehicular ad-hoc network (VANET) is a type of mobile ad-hoc network (MANET) and is regarded a promising method for future ITS. VANET monitors directly vehicular traffic issues utilizing its safety and non safety applications. Generally, VANET comprises of two kinds of communications: vehicle-to vehicle (V2V) and vehicle-to-roadside (V2R). The subscriber is the primary component of the vehicular network and the aim of this network is to support the user and give the right information about the road to the subscriber. Intruders are one of the kinds of users and those who intentionally generate problems for other clients of a network by launching various kinds of attacks (passive or active) [2]. In a vehicular network, they become more significant because they can powerfully change life critical message or flood a wrong message to other network users. Security is a significant factor and confidentiality, integrity, availability (CIA) are the important security needs in vehicular network [3, 4]. It is needed that all components [users, vehicle, and road side unit (RSU)] of vehicular network should be secure and work suitably to serve the subscribers and obtain the security objectives. Fig 1 represents the relationship of intruder with security goals (CIA) in VANET and Figure 2 represents all the possible attacks associated to the security goals in VANET. Detailed descriptions of all the attacks are provided in the upcoming sections with some scenarios. The remaining paper is categorized into five sections; Sections 2–4 discuss in detail the basic idea of security goals (CIA) and all possible attacks in VANET. Section 5 shows the conclusion of this review work.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 9, September 2016

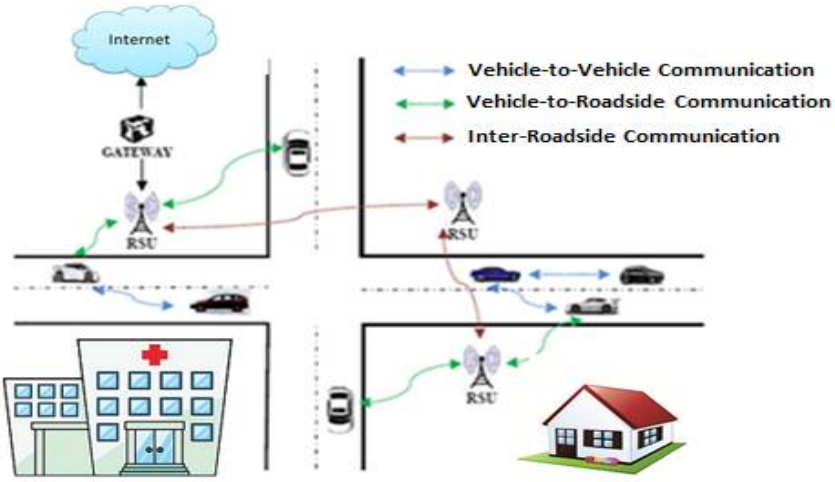

Figure-1 Vehicular Ad-hoc network

II. ATTACKS ON CONFIDENTIALITY IN VANET

Confidentiality [5, 6] is a significant security need in vehicular communication. A vehicle forwards and obtains safety and no safety messages from V2V and vehicle to infrastructure (V2I). The data of the message should be secure and should not be accessible to non authorized users (attackers). Another aspect of confidentiality is to build the analysis of the traffic flow from vehicle to RSU or V2V communication. This is a passive-type threat, in which intruders are just monitors, the communication between vehicles and collects obtained information. All possible attacks associated to confidentiality are provided below through various scenarios [7, 8].

A. MONITORING ATTACK

The intruder in a monitoring attack [9] simply monitors the entire network, hearing to the whole communication occurs in V2V and vehicle to roadside unit (V2R). When he/she listens any data that is pertinent to his/her requirements then he/she relays this data to the person of interest. One instance, in the case of a police operation, the police have planned an operation against a specific criminal to take place in a particular region. To conduct the operation, the police must interact with one other to pass on the details, such as the exact position and time that the operation is planned. Intruders hear to all of the interaction and inform the criminals about the impending police operation. Fig 2 shows the entire scenario where intruder X simply monitors other vehicles communications.

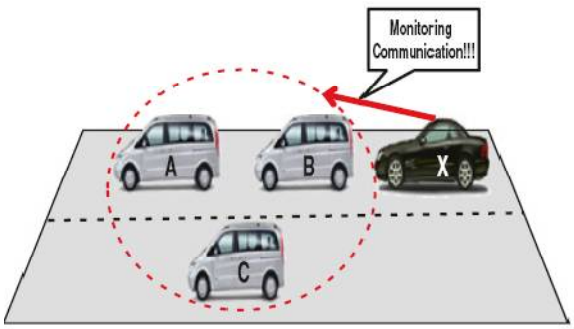

Fig. 2 Monitoring attack in V2V comm.

B. TRAFFIC ANALYSIS ATTACK

The traffic analysis attack [10] is a serious level attack to client privacy in vehicular communication. A traffic analysis attack is against the communication anonymity between vehicle to a roadside unit (V2R) and (V2V). In this attack, the

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 9, September 2016

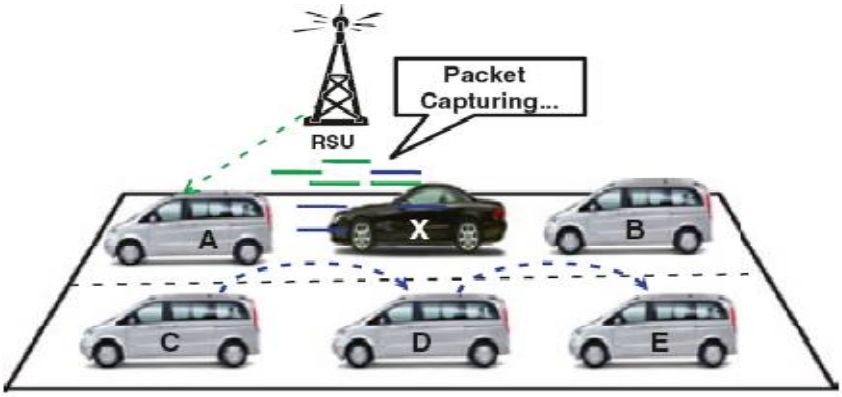

Fig. 3 Traffic analysis attack in V2V and V2R

intruder describes some objective and achieves the objective through capturing different kinds of traffic information packets. This involves the user location, the vehicle ID, the travelling route of the subscriber or some other of the user's traffic information; the intruder requires this information to utilize for its attacks. In Figure 3, the intruder captures packets from V2V communication and vehicle for RSU communication. Intruder X examines these captured packets and utilizes them to extract the needed information.

C. MAN IN THE MIDDLE ATTACK

Man in the middle (MiMA) attack [11] is a general attack on the communication that takes place among subscribers. The intruder is often situated between a minimum of two persons. The intruder is actively eavesdrops and links independently to the vehicle of the victim.

In a MiMA attack, there are two actions that can be conducted by the intruder.

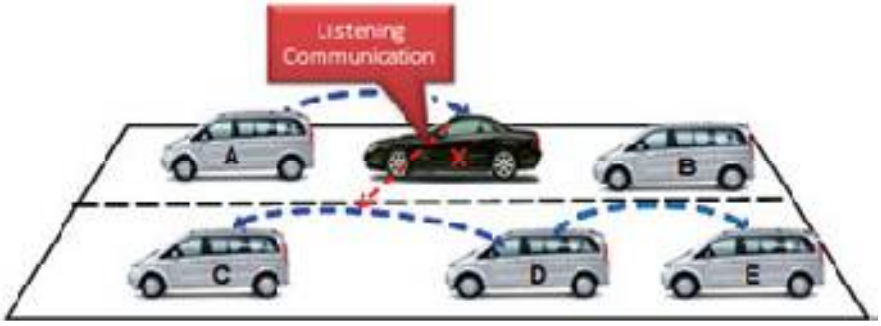

Fig. 4 Man in the middle (MiMA) attack

• Eavesdropping on communication between vehicles

In this situation, both the receiver and the sender think that they are in direct interaction with one other but in reality; their communication is being over listened by an intruder. The explanations of the MiMA attack can be viewed in Figure 4. In this scenario, interaction is occurring between vehicle C and vehicle D, and vehicle X is an intruder. Both vehicles C and D think that their interaction is not only direct but also secure. The intruder simply eavesdrops on their communication and then utilizes the data gained for his/her own requirements.

III. ATTACKS ON INTEGRITY IN VANET

In vehicular network, data integrity [5, 6] is one of the most significant security objectives and it should be manage while interacting V2V or vehicle to road side unit (V2R). The data of the message should not be changed as it goes from sender to recipient. If the source is authorized user of the network but message contents has been altered then there is no requirement to examine the authorization of the source user. Message content is very significant whereas

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 9, September 2016

communicating in safety and non safety applications of vehicular network. All possible attacks associated to integrity are provided below.

A. MESSAGE ALTERATION ATTACK

Malicious Attackers modify the messages, and the wrong messages are forwarded to other subscribers. Attackers simply alter the data of the safety or non safety messages that they have obtained from other users or from the RUS, then forward these modified message to other network users [12].

Fig 5 represents the example in which intruder X launches the attack on the safety message. Intruder X obtains one warning message *Break down Warning* from vehicle A. So, the intruder changes the message content and forwards this message *Road is Clear* to vehicle B.

Fig. 5 Message alteration attack in V2V

B. MESSAGE FABRICATION ATTACK

In a message fabrication attack [12], intruders broadcast wrong data in a network. Such types of attacks are started by greedy drivers. The greedy drivers fabricate messages utilizing broadcast methods and then launch the attack by forwarding these messages into the network. Messages fabrication has two possible forms.

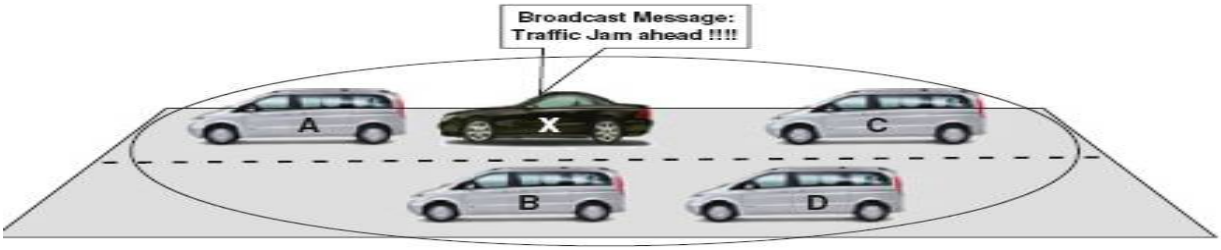

Fig. 6 Message fabrication attack

Wrong information about an attacker's ID, location and speed of vehicle is forwarded to other vehicles or RSU. Another possibility is that the intruder will represent himself/ herself as an emergency vehicle, so that he/she can drive at a faster speed. Fig 6 describes the condition in which intruder X floods the false message into the network.

C. INCORRECT DATA INJECTING ATTACK

In this attack, intruder X controls communication by adding alternative data into the original message (blue lines) from vehicle C to vehicle D. Fig 7 shows the attacker behaviour who is adding bogus data into vehicle to vehicle communication in network.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 9, September 2016

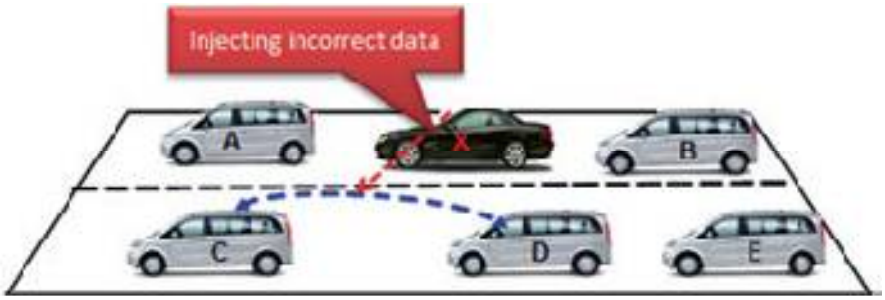

Fig. 7 Attacker injecting incorrect data

IV. ATTACKS ON AVAILABILITY IN VANET

Availability of network is one of the primary modules of security objectives. The basic goal of a vehicular network is to support the subscribers through its powerful applications and the network should be existed each time. But, if the network is not existed for communication then the primary objective of the network has become waste. All possible attacks associated to availability are provided below through various scenarios [7, 8, 13].

A. DENIAL OF SERVICE ATTACK

Denial of service (DoS) [14] attack is one of the significant attacks in relation to the network availability. Channel jamming in wireless atmosphere is also a part of attack and the intruder objective is to prevent the authorized vehicles from accessing the network facilities. The attack may jam the entire channel or may generate some problems directly or indirectly to use the network resources. The attacker forwards high frequency signals and jams the communication channel among the vehicles. These vehicles cannot forward or obtain safety or non-safety messages on the network. The intruder launches the attacks close to the RSU and jams the communication channel between the RSU and the vehicles. Fig 8 shows this scenario in which vehicle A could not interact with the other vehicle B because of a DoS attack.

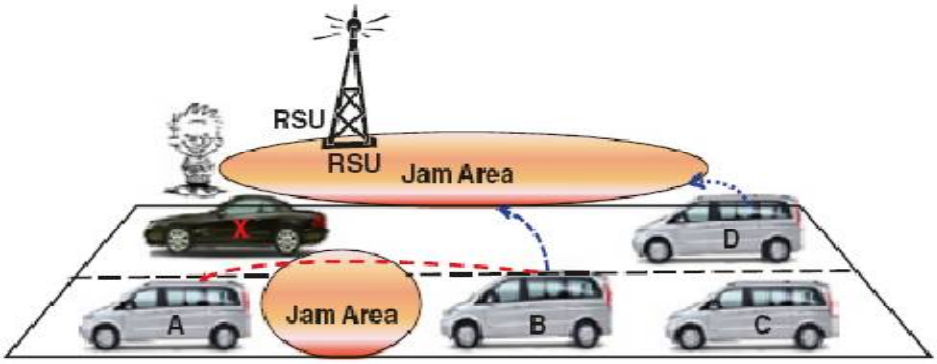

Fig. 8 DoS attack in V2V and V2R comm

B. DISTRIBUTED DENIAL OF SERVICE ATTACK

A DoS attack is critical in vehicular atmosphere but a Distributed Denial of Service (DDoS) [14, 15] attack is even more critical because the technique of the attack in it is in a distributed way. In this case, intruders launch attacks from various locations. They may utilize different time slots for establishing attacks. The behaviour of the attack and time slots may be changed from V2V of that specific attacker. Fig 9 describes the scenario in which a group of intruder's vehicles (C, D, and G) launches a DDoS attack on authorized user vehicle F. After some time, the victim user vehicle F cannot interact with other network vehicles.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 9, September 2016

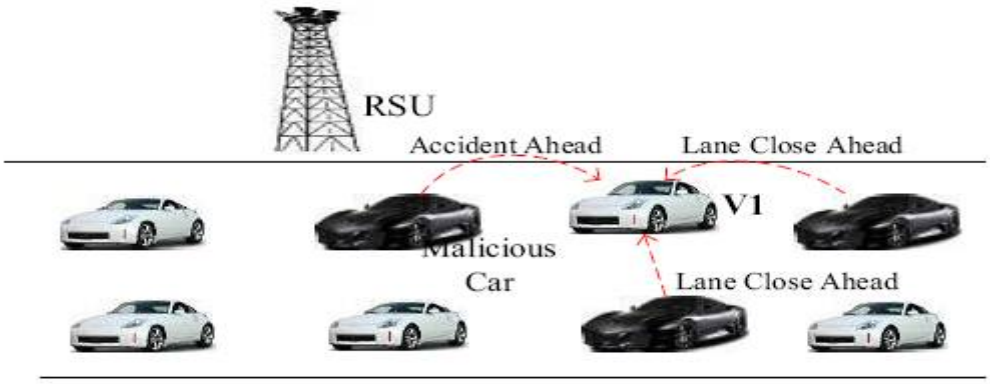

Fig. 9 DDoS attack in V2V communication

C. BROADCAST TAMPERING ATTACK

Safety messages are flooded in the network and inform other subscribers about current safety situations of any particular region. In this case, an intruder tampers with the flooded safety message and possibly adds wrong safety message. The objective of this is to cause road accidents or change the traffic flow on some particular route. Fig 10 represents the attacker X behaviour where the intruder broadcasts two different types of messages to two different users groups.

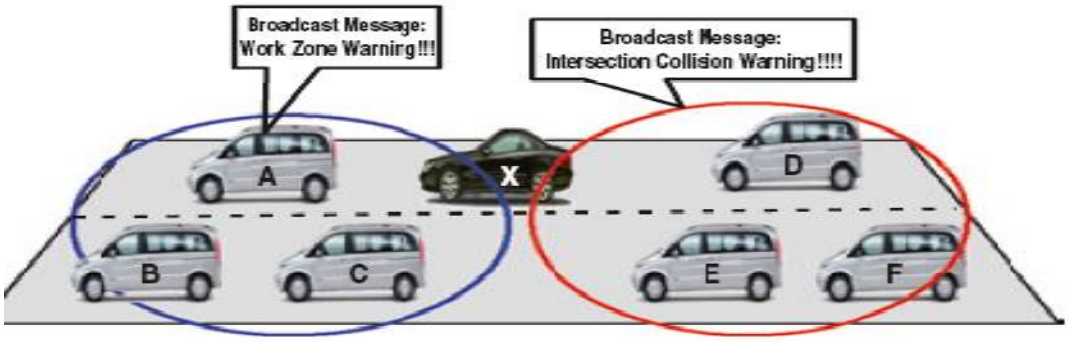

Fig. 10 Broadcast tampering attack

D. MALWARE ATTACK

A vehicle has its own software and application unit (AU) which performs its own task and interacts with other subscribers as well as the RSU. There is some possibility to enter a worm and virus into the vehicle and interfere the network operation. Fig 11 shows the scenario in which a user forwards a request to the RSU for software updates. The RSU is already managed by an intruder, so the intruder downloads the malicious software into the vehicle which built the request. Now this software generates problems for the subscribers.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 9, September 2016

Fig. 11 Malware attack in V2R communication

E. SPAMMING ATTACK

In this situation, the sole objective of the intruder is to increase the transmission latency and utilize the network bandwidth. So, no service is existed to other network users and this is obtained by forwarding spam messages through the network. Fig 12 explains the situation when intruder X broadcasts spam messages to a specific group of users. RSU also forward spam messages, which are most usually just advertisements, to the users group.

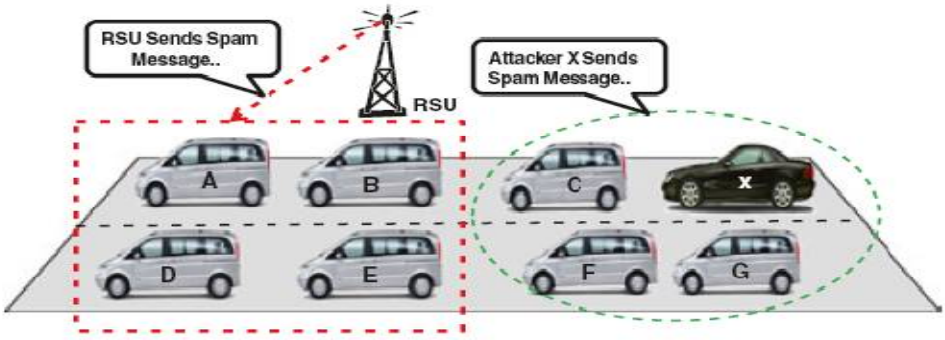

Fig. 12 Broadcast spam message attack

F. BLACKHOLE ATTACK

Blackhole attack is a different type of attack, and there are following two possible cases in vehicular network. • When any new user wishes to initiate communication with other users or simply participate in a network, then other users simply deny it. In Figure 14, user D wishes to initiate communication with user X, but user X Denys it and simply forwards a response with “SORRY.” So now user D attempts to interact with any other network user.

• One user initiates communication with other network users and it is suddenly dropped out of the communication. Fig 13 describes the situation in which user B interacting with user A and user C. User B plays the role of router and forwards and obtains messages from user A to user C. Intruder X drops the interaction of user B and the other neighbouring vehicles are interfered because this vehicle was performing the routing task and some vehicles were linked through it as the router client. In this manner, all possible connections are down because of the dropping of the connection with this intermediate vehicle.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 9, September 2016

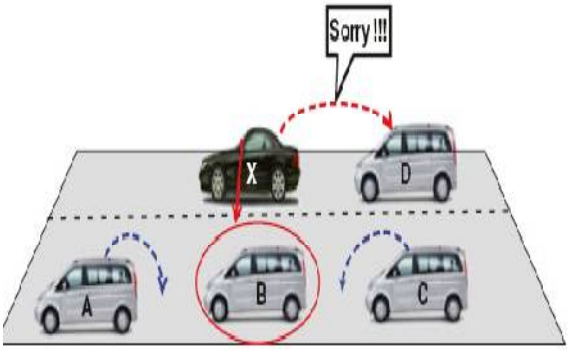

Fig. 13 Black hole Attack In V2V Communication

V. CONCLUSION

Depending on the literature review, it is understood that intruders launch different kinds of attacks while communication is in progress in the network. These threats break the security objectives like CIA in the VANET atmosphere. These goals have equal significance to support the users but the existence leads to high priority. It is realized that the attacks associated to the availability have more attack level as compare to the confidentiality and integrity. The accomplishment of the security goals by addressing the attacks nature and the attackers behaviours will support to successfully implement the VANET in real atmosphere.

REFERENCES

[1] Fatima Ameza, Nassima Assam and Rachid Beghdad, "Defending AODV Routing Protocol Against the Black Hole Attack", International Journal of Computer Science and Information Security, Vol. 8, No.2, 2010, pp.112-117.

[2] Nital Mistry, Devesh C. Jinwala and Mukesh Zaveri, "Improving AODV Protocol against Blackhole Attacks", International Multiconference of Engineers and Computer Scientists 2010, vol. 2, March 2010.

[3] Payal N. Raj and Prashant B. Swadas,"DPRAODV: A dynamic learning system against black hole attack in AODV based Manet", International Journal of Computer Science Issues, Vol. 2, Issue 3, 2010, pp: 54-59.

[4] Hoang Lan Nguyen and Uyen Trang Nguyen, "Study of Different Types of Attacks on Multicast in Mobile Ad Hoc Networks", International Conference on Networking, International Conference on Systems and International Conference on Mobile Communications and Learning Technologies, April 2006, pp. 149-149

[5] Rutvij H. Jhaveri, Ashish D. Patel, Jatin D. Parmar and Bhavin I. Shah, "MANET Routing Protocols and Wormhole Attack against AODV", International Journal of Computer Science and Network Security, vol. 10 No. 4, April 2010, pp. 12-18.

[6] N. Shanthi, Dr. Lganesan and Dr.K.Ramar, "Study of Different Attacks on Multicast Mobile Ad hoc Network", Journal of Theoretical and Applied Information Technology, December 2009, pp. 45-51.

[7] Abhay Kumar Rai, Rajiv Ranjan Tewari and Saurabh Kant Upadhyay , "Different Types of Attacks on Integrated MANET-Internet Communication", International Journal of Computer Science and Security, vol. 4 issue 3, July 2010, pp. 265-274.

[8] Jakob Eriksson, Srikanth V. Krishnamurthy, Michalis Faloutsos, "TrueLink: A Practical Countermeasure to the Wormhole Attack in Wireless Networks", 14th IEEE International Conference on Network Protocols, November 2006, pp.75-84.

[9] Mahdi Taheri, Dr. majid naderi, Mohammad Bagher Barekatain, "New Approach for Detection and defending the Wormhole Attacks in Wireless Ad Hoc Networks", 18th Iranian Conference on Electrical Engineering,, May 2010, pp. 331-335.

[10] Dang Quan Nguyen and Louise Lamont, "A Simple and Efficient Detection of Wormhole Attacks", New Technologies, Mobility and Security, November 2008, pp. 1-5.

[11] Viren Mahajan, Maitreya Natu, and Adarshpal Sethi, "Analysis of Wormhole Intrusion Attacks in MANETs", Military Communications Conference, November 2008, pp.1-7.

[12] Maria A. Gorlatova, Peter C. Mason, Maoyu Wang, Louise Lamont, Ramiro Liscano, "Detecting Wormhole Attacks in Mobile Ad HocNetworks through Protocol Breaking and Packet Timing Analysis", Military Communications Conference, October 2006, pp. 1-7.

[13] Mani Arora, Rama Krishna Challa and Divya Bansal, "Performance Evaluation of Routing Protocols Based on Wormhole Attack in Wireless Mesh Networks", Second International Conference on Computer and Network Technology, 2010, pp. 102-104.

[14] Yih-Chun Hu, Adrian Perrig,and David B. Johnson, "Wormhole Attacks in Wireless Networks", IEEE Journal on Selected Areas in Communications, vol. 24 no. 2, February 2006, pp. 370-380.

[15] W. Weichao,B. Bharat, Y. Lu and X. Wu, "Defending against Wormhole

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 9, September 2016

[16] Attacks in Mobile Ad Hoc Networks", Wiley Interscience, Wireless Communication and Mobile Computing, January 2006.

[17] L. Qian, N. Song, and X. Li, "Detecting and Locating Wormhole Attacks in Wireless Ad Hoc Networks Through Statistical Analysis of Multipath," IEEE Wireless Commuunication. and Networking Conference,

[18] I. Khalil, S. Bagchi, N. B. Shroff," A Lightweight Countermeasure for the Wormhole Attack in Multihop Wireless Networks", International Conference on Dependable Systems and Networks, 2005.

[19] L. Lazos, R. Poovendram, C. Meadows, P. Syverson, L.W. Chang, "Preventing Wormhole Attacks on Wireless Ad Hoc Networks: a Graph Theoretical Approach", IEEE Communication Society, WCNC 2005.

[20] L. Hu and D. Evans, "Using Directional Antennas to Prevent Wormhole Attacks", 11th Network and Distributed System Security Symposium, pp.131-141, 2003.

[21] L.Lazos, R. Poovendran, "Serloc: Secure Range-Independent Localization for Wireless Sensor Networks",ACM Workshop on Wireless Security, pp. 21-30, October 2004.

[22] W. Wang, B. Bhargava, "Visualization of Wormholes in sensor networks", ACM workshop on Wireless Security, pp. 51-60, 2004.

[23] Mohammad Al-Shurman, Seong-Moo Yoo and Seungjin Park, "Black Hole Attack in Mobile Ad Hoc Networks", ACMSE, April 2004, pp.96-97.

[24] Anu Bala, Munish Bansal and Jagpreet Singh, "Performance Analysis of MANET under Blackhole Attack", First International Conference on Networks & Communications, 2009, pp. 141-145.

[25] Latha Tamilselvan and Dr. V Sankaranarayanan, "Prevention of Blackhole Attack in MANET", The 2nd International Conference on Wireless Broadband and Ultra Wideband Communications, 2007, pp. 21-26.

[26] Geng Peng and Zou Chuanyun,"Routing Attacks and Solutions in Mobile Ad hoc Networks", International Conference on Communication Technology, November 2006, pp. 1-4.

[27] S. Lee, B. Han, and M. Shin, "Robust Routing in Wireless Ad Hoc Networks", International Conference on Parallel Processing Wowrkshops, August 2002.

[28] Satoshi Kurosawa, Hidehisa Nakayama, Nei Kato1, Abbas Jamalipour, and Yoshiaki Nemoto1," Detecting Blackhole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method", International Journal of Network Security, vol..5 no..3, Nov. 2007, pp.338–346.

[29] Nadia Qasim, Fatin Said, and Hamid Aghvami, "Performance Evaluation of Mobile Ad Hoc Networking Protocols", Chapter 19, pp. 219-229.

[30] G.S. Mamatha and S.C. Sharma, "A Robust Approach to Detect and Prevent Network Layer Attacks in MANETS", International Journal of Computer Science and Security, vol. 4, issue 3, Aug 2010, pp. 275-284.

[31] Preetam Suman, Dhananjay Bisen, Poonam Tomar, Vikas Sejwar and Rajesh Shukla, "Comparative study of Routing Protocols for Mobile Ad-Hoc Networks", International Journal of IT & Knowledge Management, 2010.