IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 10, Issue 9, September 2021

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.569

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 10, Issue 9, September 2021 ||

| DOI:10.15680/IJIRSET.2021.1009086 |

Review of Techniquesof Black Hole Attacks in Mobile AD HOC Networks

Himanshu Gaurav[1], Prof. Navneet Kaur[2]

M. Tech. Scholar, Department of Electronics and Communication, SIRT, Bhopal, India[1]

Professor, Department of Electronics and Communication, SIRT, Bhopal, India[2]

ABSTRACT: Secure communication is an important aspect in any networking environment. But in ad hoc networks it is a significant challenge due to its unique characteristics like unreliable wireless links, dynamic topology, limited physical protection of wireless nodes, and absence of certificate authority and lack of centralized administration point. These characteristics make ad hoc networks vulnerable not only to the existing attacks of wired networks like IP Spoofing, Denial Of Service attack, eavesdropping and message distortion but also to new kind of attacks specifically targeting ad hoc networks like black hole attack, gray hole attack and worm hole attack. The traditional security mechanisms of infrastructure networks are not fully applicable to ad hoc networks because of its limited resources such as memory, bandwidth and energy.

KEYWORDS: - MANET, Black Hole, Attack

I. INTRODUCTION

The design of wireless devices such as cellular phones, laptops, Personal Digital Assistants (PDAs), and micro-sensors have enabled the development of Mobile Ad hoc Networks (MANETs) in which a group of wireless nodes, form a network among themselves [1]. In contrast to wired and cellular networks, an ad hoc wireless network does not depend on any established infrastructure or centralized administration such as a base station or router for communication. Hence it is also called as infrastructureless networks. MANET is an autonomous system of wireless mobile nodes that moves freely and randomly, organizing itself arbitrarily. Therefore, its network topology is dynamic in nature and changes rapidly and unpredictably. These networks have no fixed infrastructure for end to end delivery of packets. Hence the nodes act both as a host and as a router for forwarding packets in the network. In recent years, ad hoc wireless networks have found applications in vehicular networks, military, during natural disasters, business conferences, educational environments and smart home [2].

Since the functioning of MANET requires cooperation from the participating nodes in the network, security is a primary concern in MANET. Many applications, especially military and emergency rescue, are based on ad hoc networks, where enforcing security requirements are harder than traditional wired networks. Secure routing is also difficult here because of the absence of centralized administration in the network and each node has to trust other nodes for routing their packets. So the presence of any misbehaving nodes in the network can easily disrupt the network operation and damage the communication within the network. Thus, secure routing is one important aspect that has to be incorporated with ad hoc networks for successful commercialization of such networks, and to support secure applications.

II. BLOCK HOLE ATTACK

A black hole attack is a kind of DOS attack where a malicious node can attract all packets by falsely claiming a fresh route or shortest route to the destination and then absorbs them without forwarding them. The black hole nodes follow a pattern for launching the attack. Initially, the nodes exploit the property of reactive routing protocols such as DSR and AODV, to advertise itself as having the short and recent route to reach the destination. Then, the black hole nodes drop the packets without forwarding to destination. To avoid the risk of overhearing by neighbor nodes, as in case of DSR protocol due to promiscuous overhearing, the black hole nodes launch a subtle form of this attack called gray hole attack, where the nodes selectively drops and selectively forwards some packets.

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 10, Issue 9, September 2021 ||

| DOI:10.15680/IJIRSET.2021.1009086 |

2.1 Classifications of Black Hole Attack

The black hole attack can be classified as follows: Single Black Hole Attack: A single black hole attack easily occurs in the mobile ad hoc networks. This attack is launched by single malicious node present along the data forwarding path in the network. Cooperative Black Hole Attack: It is also known as colluding or collaborative black hole attack. Here a group of black hole nodes cooperate with each other and drops data packets between them. The cooperative black hole nodes exhibit this behavior to avoid themselves from being detected by the upstream nodes present in the data forwarding path through promiscuous monitoring. Gray Hole Attack: It is also known as selective black hole attack. In this attack, the malicious node participates correctly in route discovery process. Once a route is selected involving the malicious node, the node then partially drops the data packets. Since the gray hole node selectively drops the data packets, it is difficult to differentiate whether the packet drop occurs due to congestion in the network, or due to black hole attack. Hence gray hole attack is even harder to detect than black hole attack.

III. LITERATURE REVIEW

Sharma et al. [1], mobile Ad hoc Network is a very important key technology for device to device communication without any support of extra infrastructure. As it is being used as a mode of communication in various fields, protecting the network from various attacks becomes more important. In this research paper, we have created a real network scenario using random mobility of nodes and implemented Black hole Attack and Gray hole Attack, which degrades the performance of the network. In our research, we have found a novel mitigation technique which is efficient to mitigate both the attack from the network.

Aaroud A et al. [2], the nature of VANET networks makes the network vulnerable to several attacks such as the black hole attack which is part of Denial of Service attacks (DOS). The aim of these attacks is to prohibit users from using one or more services by making the communication unavailable. In this sense and during the routing process, the malicious node tries to acquire the route by forging routing information in order to receive the data and then drops it without transferring it to its destination. In this paper, we propose a novel detection method of such attack during communication in a VANET network. This method is based on a variable control chart which is widely used in the industrial field to monitor the quality of a given process. This method can identify malicious nodes in real time by deploying the monitoring system in each receiving node within the network. Our method is easy to implement and does not require any modification to the 802.11p standard or the routing protocol as we will demonstrate by NS-2 simulations and SUMO microscopic and continuous road trafc simulator using a real map.

Arathy K et al. [3], the special characteristics of the VANETs, that we have mentioned earlier, influence directly on the topology of the network which makes managing very difficult. The most common threats directly afect the routing protocols. This is due to the cooperation between the different nodes of the network in order to establish a route between the transmitter and the receiver. Therefore, the network is exposed to several vulnerabilities such as Distributed Denial of Service attack (DDOS). Among these attacks, the black hole attack is the best known for disrupting a network communication. This attack occurs during the routing process to acquire the route illegally. The routing information is falsified by the malicious node.

Baadache A et al. [4], the information packaged within the RREQ is the source IP address, the destination IP address and the number of sequences. Each node with a route to the destination indicated on the RREQ responds to it by a Route Response (RREP). Unlike the RREQ, the RREP is a unicast request. The RREP is sent via the reverse route through the intermediate nodes until it gets at the source node. The chosen path is the shortest path with a minimum number of jumps as well as the highest number of sequences. When the road is no longer maintained, a route error (RERR) is sent to the transmitter so that it canfnd another alternative by the same mechanism as we explained earlier.

Baiad R et al. [5], external attacks can be prevented by using any standard security mechanism. However internal attacks are very hard to detect, because it is launched by compromised nodes that have been authorized by the victim network. Depending on whether the attacker tries to hide his misbehaving actions, the attacks are classified into stealthy and non-stealthy attacks. Also, the attacks can be classified as cryptography and no cryptography related attacks. In cryptography related attacks the attacker tries to break the cryptographic protocols, for example, using brute force attack to find the key used in an encryption system. In non-cryptography related attacks the attacker will try to make use of the faults in routing protocol design without breaking the encryption system.

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 10, Issue 9, September 2021 ||

| DOI:10.15680/IJIRSET.2021.1009086 |

Carie A et al. [6], the black hole attack is part of the family of Denial of Service attacks. The principle of this attack is to disrupt communication and put the network out of service. The attacker is waiting for a route request (RREQ) to be sent over the network. Afterwards, the attacker responds to this request by a false RREP that contains a minimum number of jumps to the destination and the highest sequence number to acquire the route. Once it is done, the sending node begins to send the data believing that they were sent to the appropriate destination while these data are intercepted by the attacker and this latter destroys them instead of transferring them to their destination.

Chavan A A et al. [7], in order to eliminate the black hole attack in its two forms: single and cooperative. This method is based on a double verification procedure done at the source node and also at the destination node. A verification packet is sent to the destination node via the route designated by the routing process. If the ID of this packet is identical in the both sides (the destination node and the source node) then we admit that the route is verified. A final verification packet is sent as a confirmation tool. If the latter arrives at its destination, a data transfer starts afterwards. A modification of the AODV protocol is made to make this method work. Additional steps are added to the routing protocol which can negatively influence the overall time of the routing, and therefore the overall time of the communication.

Delkesh T et al. [8], this modified version of the AODV can mitigate the effect of the black hole attack according to the authors. The changes are made at the level of the RREQs and the RREPs. A destination node is checked using the sequence number and the encryption/decryption function. The structure of the RREQ and RREP packets is modified by adding an Encrypted Random Number which will be verified by the said function at the source and the destination. Simulation and validation of this method is done via the NS-2 and SUMO simulators. The used version of SUMO is old (v0.12.3) to generate a fairly real mobility model. Changes to the AODV protocol must be reviewed and approved by the IEEE standard. The global response and interference time of the protocol may decrease as a consequence of the binged modifications.

El Houssaini MA et al. [9], proposed an improvement of the AODV routing protocol standard. This modification aims to detect the black hole attack by concocting a timeline of the RREQs and also for the RREPs. A correspondence is made between the two times lines. The time is split into observation intervals of fixed length. These observation intervals are used in the correspondence process to detect the false RREP. The experimental results obtained show that the method gives a performance close to that of an environment without attack.

Hasrouny H et al. [10],designed a method for real-time detection of black hole attack based on Statistical Process Control. These statistical methods, which are widely used in the industrial feld, are initiated by the authors in the field of black hole attack detection in a VANET environment. This solution acts in real time by monitoring the Packet Drop Ratio metric with this control chart by the graphic representation of network activities. This does not require modifications of the IEEE standards

IV. METHODOLOGY

IDS Technique to eliminated Black Hole Attack

In this section, the brief explanation of overall process of proposed methodology is described.

The exhibition of hybrid intrusion detection system (HIDS) is improved by characterizing the recognition aftereffects of Packet Header Anomaly Detection (PHAD) and Application Layer Anomaly Detector (ALAD) utilizing Semi Supervised ML method and a ultimate conclusion making measure is improved by presenting improved proof hypothesis. As in the past work of the exploration, the highlights are extricated from the info dataset utilizing PLS strategy.

At that point the individual choice consequences of PHAD and ALAD are grouped based Semi Supervised ML procedure. In the AI method, SVM has gotten one of the famous calculations utilized for interruption discovery because of the capacity to defeat the scourge of dimensionality and their great speculation nature. At that point the arranged outcomes are consolidated utilizing Dempster-Shafer evidence theory(ET) for ultimate choice making. Anyway the proportion of contention issue in Dempster-Shafer ET corrupts the general presentation by bringing about more bogus positives. Subsequently an improved ET is proposed. The improved ET at first builds proof uniqueness network utilizing the weighted Euclidean distance. The divergence between the confirmations is estimated and afterward at long last utilizing the disparity network, supporting degree, validity and weight of proof are determined, and the first confirmations are altered. Subsequently the proposed HIDS method with SVM and improved ET improves the identification precision.

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 10, Issue 9, September 2021 ||

| DOI:10.15680/IJIRSET.2021.1009086 |

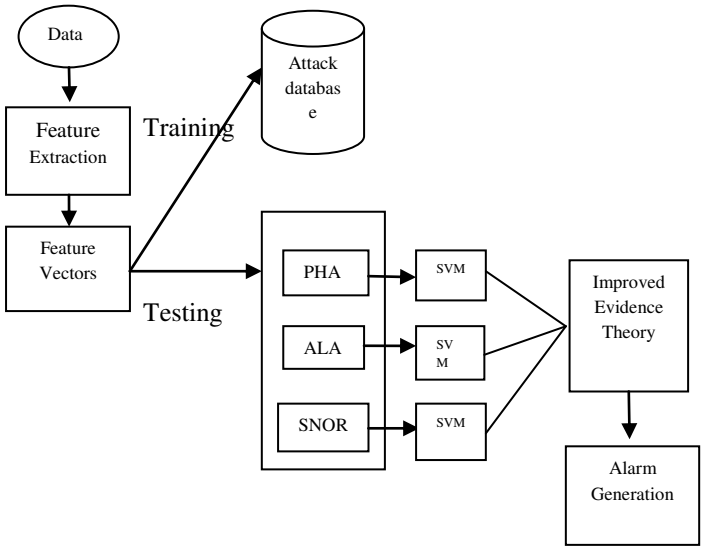

Fig. 1: Overall process flow

Input: Dataset, Evidence vector E=E_1, E_2.....En
Output: detect attacks
Step 1- Collect the dataset from the network
Step 2- Detect the intrusions in data using PHAD, ALAD and SNORT
Step 3- Classify the results using SVM
Step4- Begin
Step 5- Calculate dissimilarity matrix using equation

$$d_{i,j}(E_i, E_j) = \begin{cases} 0, & C_1 = C_2 \\ (w_1|A_1 - B_1|^2 + w_2|A_2 - B_2|^2 + \\ \ldots + w_n|A_n - B_n|^2)^{1/2}, & C_1 \neq C_2 \end{cases}$$

Where $E_i$and E_j are two instances evidences of the detection results if discrement Θ, $w_i$is the evidences, C_1 and C_2 and are the preposition values. There are n evidences for attack detection, then the above formula is used to compute the dissimilarity between E_i and E_j.

Step 6- for i=1 to n//n is the number of evidences
Step 7- Calculate entropy of evidences using equation

$$Entropy_i = Supporting\ Degree\ (m_i)_i$$
$$\ln(\ Supporting\ Degree\ (m_i))$$

The data entropy of proof is corresponding to its disparity supporting degree. The validity of the proof is calculated by normalizing the entropy value of the evidence.

Step 8- Calculate credibility of evidence using equation

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 10, Issue 9, September 2021 ||

| DOI:10.15680/IJIRSET.2021.1009086 |

$$Credibilit\,y_{m_i} = \frac{1/Entropy_i}{\sum_{i=1}^{n} 1/Entropy_i} \quad i = 0,1,2,....n$$

The sum of the credibility$_{mi}$ is equal to 1, which means credibility$_{mi}$can be viewed as the heaviness of mi. In the wake of getting the heaviness of proof, the proof can be weighted and the acquired essential certain task estimations of improvedE_i which is given in equation

Step 9- Calculate the weight of evidences using

$$m'(A) = Credibilty_{m_i}.m(A), m'(\theta) = 1 - \sum_{i=1}^{n} m'(A)$$

Step 10- end for
Step 11- for i=1 to n
Step 12- if n>2
Step 13- $e_x=e_i$
Step 14- $e_y=e_{i+1}$
Step 15- Apply improved combination rule of evidence theory using previous equation
Step 16- if i== n-1
Step 17- return result
Step 18- end if
Step 19- i=i+1
Step 20- end if
Step 21- end for
Step 22- End

V. CONCLUSION

HIDS with include choice and extraordinary classifier technique is proposed which improves exactness of interruption location measure by information decrease. At first, the applicable highlights are extricated and those highlights are given to HIDS framework. The greater part of the IDS looks at all the highlight that is excess for interruption recognition. This methodology thinks about the significant highlights in the info traffic for interruption discovery framework that is computationally proficient and viable. The most significant highlights of PHAD, ALAD and SNORT are chosen by utilizing LDA method. At that point the chose highlights are given to SVM classifier. This classifier groups the identification results. At long last, the arranged recognition consequences of every IDS are consolidated by utilizing improved proof hypothesis. Through element choice and SVM characterization measure the interruption location with higher review and exactness values are accomplished.

REFERENECS

[1] Sharma Hitesh, Omprakash and Margam K. Suthar, “Mitigation Technique for Black hole Attack in Mobile Ad hoc Network”, ICCCNT 2020.
[2] Aaroud A, El Houssaini MA, El Hore A, Ben-Othman J (2017) Real time detection of mac layer misbehavior in mobile ad hoc networks. ApplComputInf 13(1):1–9. https://doi.org/10.1016/j. aci.2015.11.001.
[3] Arathy K, Sminesh CN (2016) A novel approach for detection of single and collaborative black hole attacks in MANET. Proc Technol 25:264–271. https://doi.org/10.1016/j.protcy.2016.08.106.
[4] Baadache A, Belmehdi A (2014) Struggling against simple and cooperative black hole attacks in multi-hop wireless ad hoc networks. ComputNetw 73:173–184. https://doi.org/10.1016/j.comne t.2014.07.016.
[5] Baiad R, Alhussein O, Otrok H, Muhaidat S (2016) Novel cross layer detection schemes to detect blackhole attack against QoSOLSR protocol in VANET. VehCommun 5:9–17. https://doi. org/10.1016/j.vehcom.2016.09.001.
[6] Carie A et al (2019) Cognitive radio assisted WSN with interference aware AODV routing protocol. J Ambient Intell Hum Comput. https://doi.org/10.1007/s12652-019-01282-6.

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 10, Issue 9, September 2021 ||

| DOI:10.15680/IJIRSET.2021.1009086 |

[7] Chavan AA, Kurule DS, Dere PU (2016) Performance analysis of AODV and DSDV routing protocol in MANET and modifcations in AODV against black hole attack. Procedia ComputSci 79:835–844. https://doi.org/10.1016/j.procs.2016.03.108.

[8] Delkesh T, Jamali MAJ (2019) EAODV: detection and removal of multiple black hole attacks through sending forged packets in MANETs. J Ambient Intell Hum Comput 10(5):1897–1914. https ://doi.org/10.1007/s12652-018-0782-7.

[9] El Houssaini MA, Aaroud A, El Hore A, et al (2014) Analysis and simulation of MAC layer misbehavior in mobile ad-hoc networks. In: WCCCS 2014 - proceedings; 2014 5th workshop on codes, cryptography and communication systems pp 50–54.

[10] Hasrouny H, Samhat AE, Bassil C, Laouiti A (2017) VANet security challenges and solutions: a survey. VehCommun 7(January):7–20. https://doi.org/10.1016/j.vehcom.2017.01.002.

[11] Lee BK, Jeong EH (2016) A black hole detection protocol design based on a mutual authentication scheme on VANET. KSII Trans Internet InfSyst 10(3):1467–1480.

[12] Mahshid R, Mansourvar Z, Hansen HN (2018) Tolerance analysis in manufacturing using process capability ratio with measurement uncertainty. Precision Eng 52:201–210. https://doi.org/10.1016/j. precisioneng.2017.12.008.

[13] Montgomery DC (2005) Stastical quality control. Wiley, Hoboken Von Mulert J, Welch I, Seah WKG (2012) Security threats and solutions in MANETs: a case study using AODV and SAODV. J NetwComputAppl 35(4):1249–1259. https://doi.org/10.1016/j. jnca.2012.01.019.

[14] Robinson YH et al (2018) FD-AOMDV: fault-tolerant disjoint adhoc on-demand multipath distance vector routing algorithm in mobile ad-hoc networks. J Ambient Intell Hum Comput. https:// doi.org/10.1007/s12652-018-1126-3.

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor:
7.569

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details