Webology (ISSN: 1735-188X)
Volume 18, Number 6, 2021

Efficacy Of Two Competing Black Hole Detection Mechanism In Manets: ABIP And KNN Clustering With Fuzzy Inference

Dr. S. Sangeetha[1] , Dr. A. Kalaivani[2]

[1]Head & Assistant Professor, Information Technology, Sri Vasavi College (SFW), Erode.

[2]Assistant Professor, Department of Computer Applications, Nehru Arts and Science College, Coimbatore.

Abstract: Mobile ad hoc networks shared medium in wireless networks makes them inherently vulnerable to different kinds of attacks. It is important to make mobile ad hoc networks secure as the industry is finding more and more applications for this kind of network. The most dangerous attack on mobile ad hoc networks is called a black hole attack. Black hole attack can cripple a network at an alarming rate and the results can be disastrous. Here we had analyzed two different approaches to counter the black hole attack. Main features for each of these methods are described briefly, followed by a few observations.

1 Introduction

A mobile ad hoc network (MANET) is a group of nodes which constitutes a network of mobile nodes without predefined and pre-established architecture. Mobile nodes ad hoc networks can communicate without any dedicated access points. In MANETs, a node can act as a host as well asa router. Nodes in the network can send and receive packets through intermediate nodes.

MANETs are becoming more important because they can be used to extend a network beyond the physical infrastructure range. These are very useful for extending a network to remote locations where there is no infrastructure or where the network infrastructure is being destroyed due to natural calamity like flood or earthquake. MANETs not only have potential to be used in military but they basically originated from military. Other than military MANET scan also be used for search and rescue operations during natural or man-made calamity, to extend a network to remote locations, vehicular network, sensor networks, robot networks and many more place where we don't have access to fixed networks or where fixed networks cannot be used.

MANETs is a network without any centralized administration. Which means we cannot deploy traditional security technologies which we use on our computers. We don't have centralized nodes to deploy a firewall to filter the network traffic. Due to its ad hoc nature where nodes can join and

leave as per the requirement. Mobile Ad Hoc Networks have many temporary nodes which means any node can become a point of attack. That's the reason Mobile Ad Hoc Networks are vulnerable to Black Hole and Gray Hole attacks.

In a black hole attack a malicious node pretends to have better access to the destination where the data is required to be sent by other nodes. This way it can collect the data from the network and destroys the data packets to cripple the network. Thus, creating a blackhole for the data packets sent by other participants of an ad hoc network and preventing the data from reaching the desired destination. Gray hole attack is a smarter version of black hole attack to fool the counter measures devised for black hole attacks. In this kind of attack instead of not sending and destroying all the data packets it sends some of the data packets to the desired destination and pretends to be working without malicious intent.

In Figure 1 M is the malicious node. A node only has access to three nodes directly. If A needs to send message to other nodes which are not in direct contact, it has to ask the nodes in direct contact to forward the message to them. To decide which node is closest to those nodes like C, G, E and F it will ask B, D and M to inform their distance from those nodes. As M is a malicious node it will inform A that it is closer to C, G, E and F node compared to B and D. The M node which is malicious does the same thing with other nodes too. This way every node which does not have access to other nodes directly will pass their message through M. As M node is a malicious node it will not forward any of the messages sent to it for forwarding. Thus, creating a virtual black hole where all the messages disappear forever. This makes the MANET unstable and most of the times practically unusable.

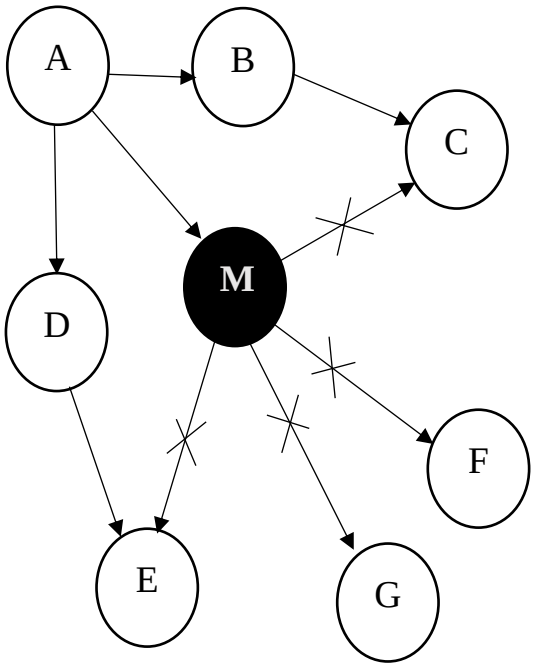


Figure 1: Black hole attack. Where M is malicious

The major challenges in developing a better counter measure are that there are no centralized servers to firewall and filter the traffic due to its ad hoc nature. Other challenges include lack of processing power in the mobile devices, lack of memory to work efficiently and most importantly the limited power supply. The participants of ad hoc network are devices that are powered by batteries and conservation of power is paramount in such devices. Due to these limitations, we cannot use power hungry heavy processing to counter the attacks on the ad hoc network.

2 Ad-hoc On-demand Distance Vector (AODV)

Ad-hoc On-demand Distance Vector is a loop-free routing protocol for ad-hoc networks. It is a reactive protocol because the routes are created only when they are needed. It is designed to be self-starting in an environment of mobile nodes. The advantages of the AODV protocol are minimal control and processing overhead, multi hop routing capability with dynamic topology maintenance.

Support for unicast, multicast and broadcast communications are provided by AODV. It can also support many nodes in the network. If the path link is lost AODV can repair the route locally. In this protocol nodes can join or leave arbitrarily to form ad hoc network. When the source node does not have a valid path to the destination, the discovery process in this protocol is performed., The following four messages are exchanged during the routing process:

(i) Route Request(RREQ):

A node, Initiates RREQ multicast message to start the route discovery process. Neighboring nodes keep track of where the message originated and move it on to their neighbors before it reaches the destination node.

(ii) Route Reply(RREP):

The destination node responds with an RREP, which returns to the source through the path taken by the RREQ. As the RREP returns to the source, forward routes are formed in the intermediate nodes. If an intermediate node knows the path to the destination, it may send an RREP in response to a received RREQ, allowing nodes to enter an established route. Once the RREP arrives at the source and the route is established, communication between the source and the destination will begin.

(iii) Route error (RERR):

When messages cannot be sent due to interruption, a RERR message is sent through a node detecting the link interruption. The message is re-cast by other nodes. The RERR message shows the unattainable destination. Message receiving nodes inactivates the route.

(iv)Route reply acknowledgment (RREP-ACK)

The Route Reply Acknowledgment (RREP-ACK) message is sent in response to a RREP message. This is typically done when there is danger of unidirectional links preventing the completion of a Route Discovery cycle

In AODV, a node requests a route to a destination by broadcasting an RREQ message to all its neighbors. When a node receives an RREQ message but does not have a route to the requested destination, it in turn broadcasts the RREQ message. AODV at source node selects the best route from received RREPs based on the high sequence number and lower hop count. Most of the misbehaving nodes in route discovery phase exploit this by sending RREP with high sequence number pretending to have a fresh route to the destination.

3 Alleviating the Effects of Black Hole Through Identification and Protection (ABIP)

In this research paper M. Kowsigan, J.Rajesh kumar, B. Baranidharan, N. Prasath, S. Nalini and K. Venkatachalam propose a system based on uses of mean and standard deviation as multiple statistical features in their research paper called A Novel Intrusion Detection System to Alleviate the Black Hole Attacks to Improve the Security and Performance of the MANET.

They had maintained three points as reference in the proposed system. There is a steady growth in these reference features which is organic at the time of nonoccurrence of attack and during an attack these features increase rapidly signaling the network that an attack is in progress.

In ABIP[1] model, it is assumed that the physical characteristics of all the nodes are common. In this model only the sender and receiver nodes are treated as trusted nodes. All other nodes are assumed to be malicious. During a black hole attack wrong routing information is sent by the black hole node with minimum hop count and maximum receiver succession number in the respondent packet. The functionality of the protection phase includes the detailed study of the security parameters used in the MANET environment such as confidentiality, integrity, authentication and denial of service.

The proposed Intrusion detection system ABIP[1] has been structured with below features:
(a) Non-static threshold value for receiver succession number by taking more than one respondent packets.
(b) No additional node is required for communication coverage which is not located dynamically in the network.
(c) The nodes don’t have to be in the overhearing mode.
(d) Mean and standard deviation has been used for the identification of the black hole attack in the environment.

In the Non-static threshold computation phase the non-static threshold value for the receiver succession number is calculated by the sender node. In the identification phase, the sender node

sends the MISTREAT packet to detect the malevolent node and then AWARE packet containing malevolent ID and MISTREATED succession number is published in the network. In the protection phase, the malevolent node is not allowed to participate in the route creation process and its response is avoided when it is identified by other nodes in the network. During transmission of data, the MISTREAT packet attack can occur. There is a possibility for the attackers to use these type of data packets. But this MISTREAT packet attack is very complex to identify as well as to handle. The MISTREAT packet attack will minimize the throughput, undergoes congestion and denial of service also. It produces interruption, change and redundancy of data packets.

In a MANET a request will be eliminated from the network if the receiver node receives false route request. In the proposed approach a false route information is sent back to all the nodes which send the false route request to the receiver node. In ABIP[1], the calculation of mean for the receiver succession number is computed. After that standard deviation for the receiver succession number is calculated. The ultimate threshold value is given by the standard deviation value in which it is computed by the receiver succession number of R response packets received from various nodes. The proposed system checks whether the average value is less than the threshold value and it also checks whether the threshold value is less than the receiver succession number which is present in the routing table. Every time the receiver publishes the new route request the computation of new threshold value is done. If the occurrence of the attacker is at next hop of the sender node and the threshold value is less than the receiver succession number in the routing table and the hop count is equal to one then the sender node detects the occurrence of malevolent node in the network and create awareness to the other nodes in the network and eliminates the mistreated receiver succession number from the routing table. The mistreated succession number which includes the MISTREAT message is transferred to the next hop by the sender node. The process of the transferring the messages continues until the detection of the malevolent node.

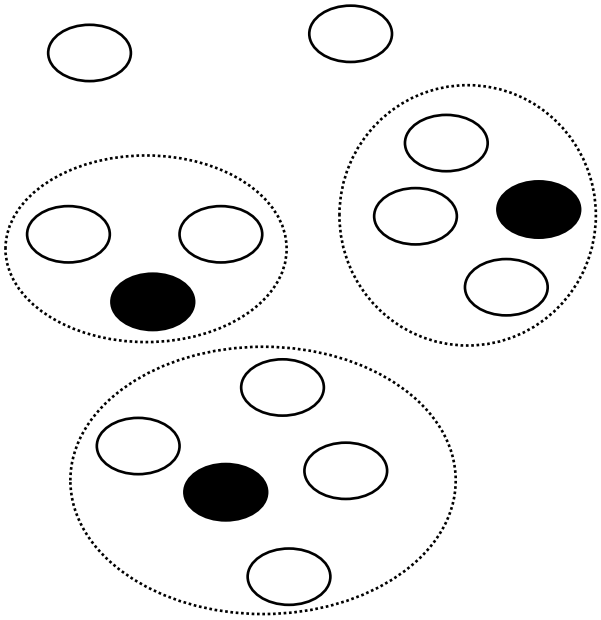
The protection phase is enabled after completion of the identification phase. An AWARE packet is sent to all the nodes and the malevolent node is black listed. The malevolent nodes entry is made in the table blacklist and its entry is removed from the routing table. This process is done before computing the request or response packet. After a node is identified and black listed all the nodes in the network ignore the request or response packet which is sent by the malevolent node.

Compared to other protection protocols, researchers found that ABIP protocol had significantly improved the packet delivery rates in single and double black hole attacks. Throughput output was very high in comparison to other security protocols even in multiple black hole attacks. Routing over head was almost negligible and detection rate out performed all other security protocols. Only drawback of ABIP protocol is the it is only meant for black hole attacks.

4Black Hole Attack Detection Using K-Nearest Neighbor Algorithm and Reputation Calculation in Mobile Ad Hoc Networks

In this research paper Gholamreza Farahanipropose a system to detect black hole attacks using KNN clustering with fuzzy inference [2].

Attacks in this system are detected by the data it receives from the nodes. In this system nodes follow the sent packets for this purpose. Then, neighborhoods of the nodes are calculated using the KNN clustering. A cluster is formed based on the nodes in a range. Then nodes calculate the level of trust around them and exchange information with the neighbors based on these values. Based on these threshold values a head is nominated among the nodes in each cluster. From the candidate nodes the node with the most reliable neighbors at the desired energy level is selected as the cluster head using the fuzzy inference. A network is formed and clusters are calculated and the cluster heads and nodes will trust each other. Malicious nodes will be identified after a closed routing in the network is started. The fuzzy logic used in this security system is based on the rule that it should increase the accuracy in detecting attacks without increasing the complexity of the system.
The main advantage of the proposed method over other methods is that in addition to the determination of trust of nodes to each other with the calculation of reputation, its clustering is also carried out with the KNN algorithm. As per the researcher this method is able to better separate the untrusted nodes. Using beta distribution, Josang mental logic and fuzzy inference helps to calculate the reputation better. The inference engine in this method contains a database of different rules and methods for inferring rules that process fuzzy values. The rule database is a series of IF-THEN rules that relate fuzzy input variables to the fuzzy output variables by language variables. Each of the rules is described by a fuzzy set and implicit fuzzy operators OR, AND, and so on.



● Cluster head node
O Nodes

Figure 2: Use of KNN for clustering

In Figure 2, you can see how k-nearest neighbor or KNN clustering is used to form clusters of neighbors and assigning a cluster head works. The cluster head is represented by the black node. The wight nodes closest to the black node and the black node is formed into a cluster. All the nodes inside the dotes circle are a cluster and the white nodes too far are not part of any cluster.
The proposed method has outperformed all the other methods. It has low packet loss rate, throughput is better, packet delivery ratio is also better and network delay was also lower than other methods. Though performs better than all other methods but the improvements are just marginal.

5 Future research

Though black hole attacks are devastating to a MANETs and both methods are able to mitigate black hole attacks efficiently. Black hole attacks are just one type of attack faced by MANETs. Research into other types of security measures used by MANETs with lower memory and processing usage for other types of attacks has to be conducted. Moreover, MANET and Internet of Things (IoT) have almost same kind of memory and processing limitations. Blockchain based security measures are being researched on IoT platforms and are called Blockchain Internet of Things (BIoT). Further research into BIoT is necessary.

6 Conclusion

The method named ABIP or Alleviating the effects of Black Hole Through Identification and Protection has spectacularly out perform all other methods in identifying and eliminating the black hole attacks. When compared ABIP[1] and KNN clustering with fuzzy inference[2], both methods provide enough security from black hole attacks.

Both methods are able to defend against black hole attacks but will not be able to defend against gray hole attacks. Which means these methods on their own cannot provide enough security for defending an ad hoc network. Both these methods can only be used as part of a larger security package.

KNN clustering with fuzzy inference[2] has only marginally outperformed other existing methods and is heavier on resources compared to the ABIP[1] method. As stated earlier, resources are a constraint on an ad hoc network. ABIP[1] has not only out performed other existing security packages but it barely uses the system resources. Therefore, ABIP[1] is a better choice to be included in a larger security package because other security modules in the security package will have no overheads caused by ABIP.

References

[1]M. Kowsigan, J. Rajeshkumar, B.Baranidharan, N. Prasath, S. Nalini, K. Venkatachalam. A Novel Intrusion Detection System to Alleviate the BlackHole Attacks to Improve the Security and Performanceof the MANET, April 2021.

[2] Gholamreza Farahani, Black Hole Attack Detection Using K-Nearest Neighbor Algorithmand Reputation Calculation in Mobile Ad Hoc Networks, Aug 2021.

[3] Singh, T., Singh, J., & Sharma, S.Energy efficient secured routing protocol for MANETs. Wireless Networks, 2018

[4]Dorri, A.An EDRI-based approach for detecting and eliminating cooperative black hole nodesin MANET. Wireless Networks, Aug 2019.

[5] Katal, A., Wazid, M., Goudar, R. H., & Singh, D. P. A cluster based detection and prevention mechanism against novel datagram chunk dropping attack in MANET multimedia transmission. In Proceedings of IEEE conference on information and communication technologies (pp. 479–484), 2018.

[6] Kowsigan, M., et al. Heart disease prediction by analysing various parameters using Fuzzy logic. Pakistan Journal of Biotechnology, 14(2), 157–161, Sep 2017.

[7] P. Tamilselvi and C. Ganesh Babu, "An efficient approach to circumvent black hole nodes in manets," Cluster Computing, vol. 22, no. S5, pp. 11401–11409, Aug 2017.

[8]Jhaveri, R. H., Patel, S. J., &Jinwala, D. C. DoS attacks in mobile ad hoc networks: A survey. In IEEE 2nd international conference on advanced computing and communication technologies, Sep 2018.

[9] C. Panos, C. Ntantogian, S. Malliaros, and C. Xenakis, "Analyzing, quantifying, and detecting the blackhole attack in infrastructure-less networks," Computer Networks, vol. 113, pp. 94–110, Sep 2017.

[10] Laxmi, V., Lal, C., Gaur, M. S., & Mehta, D.JellyFish attack: Analysis, detection and countermeasurein TCP-based MANET. Journal of Information Security and Applications, 22, 99–112, Sep 2019.

[11] V. K. Kollati and S. Somasundaram, "IBFWA: integrated Bloom Filter in Watchdog Algorithm for hybrid black hole attack detection in MANET," Information Security Journal: A Global Perspective, vol. 26, no. 1, pp. 49–60, Aug 2017.

[12] S. Gurung and S. Chauhan, "A dynamic threshold based approach for mitigating black-hole attack in MANET," Wireless Networks, vol. 24, no. 8, pp. 2957–2971, Sep 2018.

[13] Y. M. Khamayseh, S. A. Aljawarneh, and A. E. Asaad, "Ensuring survivability against Black Hole Attacks in MANETS for preserving energy efficiency," Sustainable Computing: Informatics and Systems, vol. 18, pp. 90–100, Aug 2018.

[14] Shi, F., Liu, W., Jin, D., & Song, J. A cluster-based countermeasure against blackhole attacks in MANETs. Telecommunication Systems, 57(2), 119–136, Aug 2019.

[15] A. Hammamouche, M. Omar, N. Djebari, and A. Tari, "Light weight reputation-based approach against simple and cooperative black-hole attacks for MANET," Journal of Information Security and Applications, vol. 43, pp. 12–20, Sep 2018.

[16] A. H. Hamamoto, L. F. Carvalho, L. D. H. Sampaio, T. Abrão, and M. L. Proença, "Network anomaly detection system using genetic algorithm and fuzzy logic," Expert Systems with Applications, vol. 92, pp. 390–402, Aug 2018.
[17]Kowsigan, M., &Balasubramanie, P. An efficient performance evaluation model for the resource clusters in cloud environment using continuous time Markov chain and Poisson process. Cluster Computing,22(5), 12411–12419, Sep 2019.
[18] Gurung. S., Saluja. K. K. Mitigating impact of black hole attack in MANET. In Proceedings ofthe 5th international conference on recent trends in information, telecommunication and computing, Apr2019.
[19]Faghihniya, M. J., Hosseini, S. M., & Tahmasebi, M.Security upgrade against RREQ floodingattack by using balance index on vehicular adhoc network. Wireless Networks, Apr 2018.
[20] R. Czabanski, M. Jezewski and J. Leski, Introduction to Fuzzy Systems," Deory and Applications of Ordered Fuzzy Numbers, pp. 23–43, Springer Open, Switzerland, Mar 2017.
[21] M. Goswami, P. Sharma, and A. Bhargava, "Black hole attack detection in MANETs using trustbased technique," International Journal of Innovative Technology and Exploring Engineering, vol. 9, no. 4, pp. 1446–1451, Aug 2020.
[22] H. Moudni, M. Er-rouidi, H. Mouncif, and B. E. Hadadi, "Black hole attack detection using fuzzy based intrusion detection systems in MANET," Procedia Computer Science,vol. 151, pp. 1176–1181, Apr 2019.
[23] G. Arulkumaran and R. K. Gnanamurthy, "Fuzzy trust approach for detecting black hole attack in mobile adhoc network," Mobile Networks and Applications, vol. 24, no. 2, pp. 386–393, Sep 2019.
[24] A. U. Khan, G. Abbas, Z. H. Abbas, M. Waqas, andA. K. Hassan, "Spectrum utilization efficiency in the cognitive radio enabled 5G-based IoT," Journal of Network and Computer Applications, vol. 164, no. 102686, pp. 1–16, Aug 2020
[25] Johnson, D. B., Maltz, D. A., & Hu, Y. -C. The dynamic source routing protocol for mobile adhoc network (DSR). IETF Internet Draft, Sep 2018.
[26] Verma, K., Hasbullah, H., & Kumar, A. Prevention of DoS attacks in VANET. Wireless Personal Communications, 73, 95–126,Sep 2018.
[27] Gurung, S., & Siddhartha, S. A review of black-hole attack mitigation techniques and its drawbacks in mobile ad-hoc network. In Proceedings of the 2nd IEEE international conference on Wi SP NET(pp. 2409–2415), Aug 2019.
[28] Chang, J. M., Tsou, P. C., Woungang, I., Chao, H. C., & Lai, C. F. Defending against collaborative attacks by malicious nodes in MANETs: A cooperative bait detection approach. IEEE System Journal, 9(1), 65–75, Apr 2019.