TEST Engineering & Management

March - April 2020
ISSN: 0193-4120 Page No. 11287- 11293

Preventing Black Hole Attack and Safe Data Transfer in MANET Using Neural Network and RVM Classifier

[1]Jemima Silvia J, [2]L.R.Aravind Babu

[1]M.Phil Research Scholar, [2]Assistant Professor,
Division of Computer and Information Science,
Annamalai University, Annamalai Nagar-608002

Article Info
Volume 83
Page Number: 11287 - 11293
Publication Issue:
March-April 2020

Article History
Article Received: *24 July 2019*
Revised: *12 September 2019*
Accepted: *15 February 2020*
Publication: *15 April 2020*

Abstract

Mobile ad-hoc network is a developing area of interests, which utilized in a wide range of applications. A MANET is a self-sufficient group of mobile users that impart over data transmission of constrained with wireless connections. Since the nodes are versatile, the network topology may change quickly and unusually over time. The mobile nodes are self-configured network that were formed in anytime, anywhere without interfering centralized management or infrastructure. While transmitting the data the security attacks were formed because of open centralized management. Main cause of attack is black hole attack at most of the time. Black hole is one type of attack which makes the packets loss or dropping the packets and then sends the acknowledgement as the packet send, hence it is a serious malicious activity. As a user point view the packets forward to the target/node, but actually the packets are not sent properly. So to avoid this problem proposes the Path Identification of Black Hole Check (PIBHC) using neural network. Which classifies the attacker path node or by using the Relevance Vector Machine (RVM) to proceed further data transmission.

Keywords: *MANET, Data Transfer, Security, Neural network and RVM.*

I. Introduction

Wireless communication network could be obliged by a focal framework that controls communication between hubs in the network, or it could be a foundation less which is called Ad hoc Networks. Mobile Ad hoc Network (MANET) is a utilization of the Wireless Ad hoc Network (WANET) that interfaces versatile hubs to one another. In MANET, hubs don't depend upon a central hub to co-ordinate the communications or to pass the information between them; rather than that, they convey to pass the information between hubs that can't appear at one another unmistakably right now, may fill an expansion between the sender and the recipient hub when sender and collector are not in a relative incorporation. The adaptability of the hubs prompts an amazing changing in the network topology. MANET steering protocol are required to be adaptable to any one of a kind topology changes [MonitaWahengbam et al 2012].

MANET has no focal structure that controls the communication between hubs, so hubs depend upon themselves to pass on information to the destination hub. In this manner, a malicious attacker hub may adjust the association or drop the sent information. Denial of Service (DoS) assault is viewed as one of the most genuine dangers to MANET, in which a malicious attacker hub debilitates the battery of different hubs by referencing them to forward an enormous portion of information [Taranum, Fahmina et al 2020].

In black hole attack, every single hub acts like void hole known to man. in this moment here the void node expends all the information, here we expect which is if hubs are in their general vicinity in their area, they can give a jam towards itself and doesn't transmit to different hubs.At whatever point, source node needs to send group of data to the target node with the basic issue [Thebiga, M. in like manner, Pramila, S., 2020]. All through the route distinguishing system, the source node sends route mentioning bundles which is normally called the like a requesting packets (RREQ) to the center of the node to introduction new way to the anticipated goal. Malicious node reacts quickly to the source node in view of these hubs don't impart the directing route [D. Sabarish and C. Ranjani 2015]. The source node perceives that the route exposure process is done, dismisses other route reply messages from different hubs and picks the way through the malicious node to route the information data items [J. Ramkumar and R. Murugeswari, 2014].

Each node has the information about most recent network topology, any developments happened to the network is commonly spread to the network, and as prerequisites be hub restores their routing table. Regardless, this sort of convention makes two or three issues to the network comparatively as information transmission overhead, wastage of battery intensity of the hubs, area of trivial overabundance route, and so forth [S. T. P. Saurabh,et al 2011]. Subsequently of these challenges, Ad hoc On-Demand Distance Vector (AODV) directing convention is liked. The source hub bestows a mentioning to the goal hub, any hub getting this sales checks on the off chance that it has a crisp way to the goal hub. Precisely when black hole hub gets this mentioning it quickly sends a reaction to the goal hub with the expressing that it has the new remain of briefest way. Source hub recognizes that answer considering the route that there is no guidance to watch that the sales is from a common hub or from a dark opening hub. Source hub begins sending bundles to black hole node meaning to pass on these parcels to the goal hub, by then black hole node begins to drop these sent bundles.

II. Literature Review

K.Santhi et al, Mobile specially appointed network (MANET) is a self-orchestrating network of portable hubs confined at whatever point and wherever without the help of a fixed system or bound together organization. It has various potential applications in a disaster help exercises, military network, and business conditions. In view of dynamic, establishment less nature, the specially appointed networks are powerless against various assaults. AODV is a noteworthy on-demand detachment vector steering convention for versatile impromptu networks. It is logically weak against dark and diminish gap assault. In MANET, dark opening is an assault where a hub shows malevolent direct by ensuring false RREP (course answer) message to the source hub and correspondingly vindictive hub drops the entire getting bundle. To crush above issues, the Adaptive Neural Fuzzy Inference Systems (ANFIS) is proposed and perceive dark gap assault in MANETs. The proposed system will perceive the assault over the hub similarly as give the solute on to lessen the information adversity over the network.

Yasin, Adwan, and Mahmoud Abu Zant Mobile Ad hoc Network (MANET) is a kind of wireless networks that gives various applications in various areas. Security of MANET had gotten probably the most shooting subject in networks fields. MANET is defenseless against various sorts of assaults that sway its accommodation and network. The dark opening assault is viewed as one of the most unimaginable novel assaults that degenerate the show and unfazed nature of the network taking into account dropping each pushing toward pack by the vindictive hub. Dark gap hub expects to mislead each hub in the network that prerequisites to chat with another hub by imagining that it generally has the best way to the goal hub. AODV is a responsive directing convention that has no techniques to perceive and kill the dark opening hub in the network. Right now, updated AODV by sorting out another light weight technique that utilizes timekeepers and urging so as to perceive and separate single and satisfying dark opening assaults. During the dynamic topology changing the recommended system empowers the MANET hubs to perceive and pull back the dark opening hubs in the network. The execution of the proposed strategy is performed by utilizing NS-2.35 reenactment contraptions. The inevitable results of the recommended structure to the degree Throughput, End-to-End Delay, and Packet Delivery Ratio are incredibly near the close by AODV without dark gaps.

Chaudhary, A., V. N. Tiwari, and A. Kumar A Mobile Ad hoc NETwork (MANET) is a social event of versatile hubs that depend upon wireless network interfaces, without the utilization of fixed structure or joined affiliation. Right now, networks are truly powerless to various assaults. One of these assaults is the dark gap assault and it is considered as one of the most influenced kind on MANET. Thusly, the use of an Intrusion Detection System (IDS) has a basic vitality in the MANET security. Right now, new course of action has been proposed by utilizing an Adaptive Neuro Fuzzy Inference System (ANFIS) and Particle Swarm Optimization (PSO) for portable spur of the moment networks to perceive the dark gap assault of the present exercises. Assessments utilizing separated database from a duplicated network utilizing the Network Simulator NS2 show the ampleness of our framework, on the other hand with an improved IDS based ANFIS-GA.

Abdel-Azim, M., Salah, H.E.D. besides, Ibrahim, M., separate an improvement in the wireless communication has been climbed, near to the progression another kind of tremendous potential use of wireless network shows up, which is the Mobile Ad-Hoc Network (MANET). Dark opening assault contemplates one of the most affected kind on MANET. In this manner, the utilization of obstruction acknowledgment structure (IDS) has a tremendous criticalness in the MANET certification. Right now, progression of a delicate based obstruction revelation structure is proposed which automate the way toward passing on a woolen structure by utilizing an Adaptive Neuro-Fuzzy Inference System (ANFIS) for the instatement of the FIS and a brief timeframe later streamline this introduced framework by utilizing Genetic Algorithm (GA).

III. Problem Statement

Since the idea of the MANETs, that fast it for specific applications, for e.g., in comfort zone and business gathering, there is an essential for ensuring about the data moved between any communication nodes. Black hole attack mulls over a Denial of Service (DoS) attack and then also steering attack in MANET [M. Sengar, P. P. Singh, and S. Shiwani, 2013]. Here it is worked by the method for pull down the data packets in the network to it and drop the packets as well, many substance of the data packets, or even allows the data to alternative malicious node. AODV routing protocol here tries to locate the most compelled way between any two nodes that need to pass on in the network when the way is required. AODV protocol isn't given a calculating that helps in perceiving and forestalling the black hole attack.

IV. Proposed System

Mobile Ad-Hoc network is one of general ordinal off the network with part of issues identified with block and directing. We are outfitting one of the reactions for secure the transmission over the network. Security perspectives expect an enormous movement in every practical sense the whole of the application conditions given the vulnerabilities characteristic in wireless unrehearsed networking from the very truth that radio communication happens (for example in key applications) to steering, man-in the inside and clarify data implantation attacks. Security has become a fundamental worry so as to give ensured communication between versatile nodes in a compromising situation [S. Brar and M. Angurala,2016]. The proposed structure is going to plan an obstruction discovery framework to see the black hole attack on MANET We propose an IDS system where improvement is by utilizing two segments for instance package difficulty rate, data rate. We proposed an estimation which depends upon above segments. As of now we depict the network with N number of nodes and we set source node to S and target node D and after that we let current node is as source node. We go over the techniques until current node isn't proportionate to target node. Right now discover the overview of neighboring nodes of current node. We see the parameter s of each neighbor node for example bunch hardship, data rate. Here this paper utilizes a just genuine node to check out communication. For this need, here we depict the three phase at sender side.

a. Routing

It is the demonstration of moving data from a source to a destination in a network. During this procedure, at any rate one intermediate node inside the between network is experienced. The routing idea fundamentally includes, two exercises: right off the bat, deciding ideal routing paths and also, moving the data gatherings (called packets) through an internetwork [A. Chaudhary, 2014]. The later idea is called as parcel exchanging which is straight forward, and the path assurance could be perplexing. Routing protocols utilize a few measurements to compute the best path for routing the packets to its goal. The procedure of path assurance is that, routing calculations introduce and keep up routing tables, which contain the absolute route data for the parcel.

b. Detecting and Eliminating Black Holes (DEBH)

So as to beat the existing methodology or conceivably end moves close, we propose another technique called Detecting and Eliminating Black Holes (DEBH) to perceive each malicious node in any request and any circumstance in network. The DEBH utilizes an extra data control pack to see malicious nodes. We proposed this data control packets in [Padilla E, Aschenbruck N, 2007]. In our work, this data control pack was utilized once by the source node for checking the flourishing of picked way. The structure of the data control bunch is the equivalent with the ahead of time plan done; nevertheless, in DEBH the data group is utilized for checking way in all techniques and for all nodes. Likewise, every node keeps a Black Hole Check (BHC) table to choose trustable nodes. Lots of discovery approaches start security calculation from the RREP generator and all nodes between the source and the RREP generator are believed to be shielded [Poonam Yadav,2012]. In any case, because malicious nodes are pleasing, it is possible that the last malicious node make RREP to cover its cooperatives. The DEBH uses two extraordinary lines for checking the nodes in ways, which are; "Black hole" line and "RREP generator" line. "Black hole" line contains the ID of nodes which are suspected to be malicious and "RREP generator" line contains the ID of nodes which has delivered the freshest RREP in view of RREQs. The DEBH approach contains the going with four phases: 1) Fresh way Finding. 2) scrutinizing Path security. 3) BHC modernize.4) Removing malicious nodes.

c. Detection Using RVM

Relevance Vector Machine (RVM) is another sort of AI strategy which has the tantamount choice structure with SVM [Revathi B, Geetha D,2012]. By introducing the lacking Bayesian learning theory, it not just has the benefit of dodging the over-recognize which is the property of the SVM, yet likewise keeps up an essential decent ways from the deformities of the SVM that the inadequacy isn't solid, the gigantic extent of estimation comparatively as the part work must fulfill the Mercer's condition and that human observationally picked parameters. Therefore, separated and SVM, RVM is sparser, has shorter test time, and is continuously appropriate for the online classifieds. Here is an acknowledged network stream for instance Checked sample sets $X= \{x1, x2 ..., xn\}$ in which $Xi= (x., xij, xim)$ xij is the jth measurable attributes of the network stream The looking at convention grouping of the n network stream tests is $\{c1, c2, c3... cn\}$ the estimation of I c has a place with the set $C= \{ c1, c2,..ct,... ck\}$ .When the estimation of I c is equivalent to j c , it addresses that the two network stream conventions are the proportionate. The purpose of the traffic gathering is to set up the request model $f: x \rightarrow c$ and to condemn the convention class I c of the network streamIx.

V. EXPERIMENTAL RESULT

In this section, here we show the consequences of our technique and differentiate and the present techniques were provided. Our simulation was shown in five conditions. (1) Without malicious attack in the network (2): The network with the closeness of simply black hole node, (3): The network with the closeness black hole node and diminish hole nodes, (4): The network with the proximity of simply black hole node and the IDS. (5): The network with the proximity of black hole node and diminish hole nodes and the IDS.

Packet Delivery Ratio (PDR), which demonstrates the capacity to effectively convey packets to the goal.

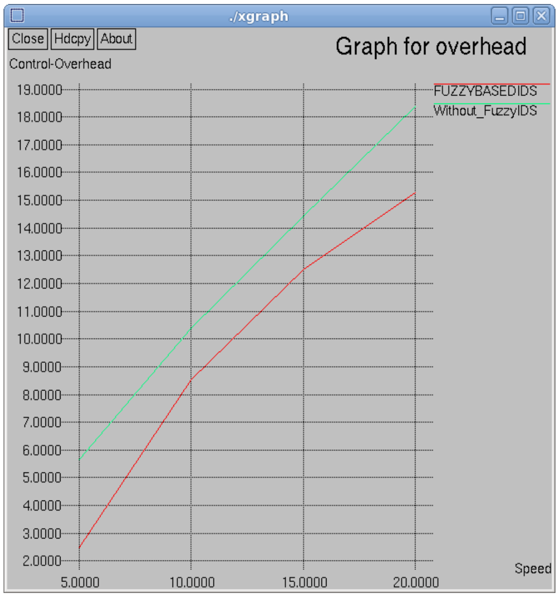

Figure 1: Over-Head

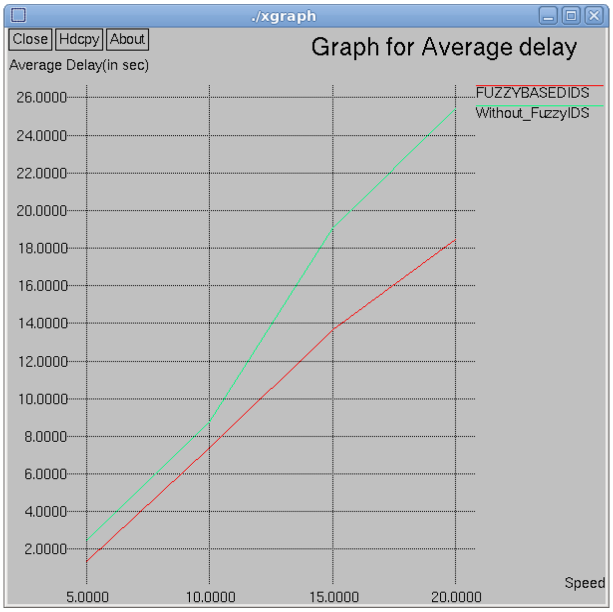

Figure 2: Average Delivery

Every situation recreated in two circumstances (without attack, with an attack) which is based on the IDS.

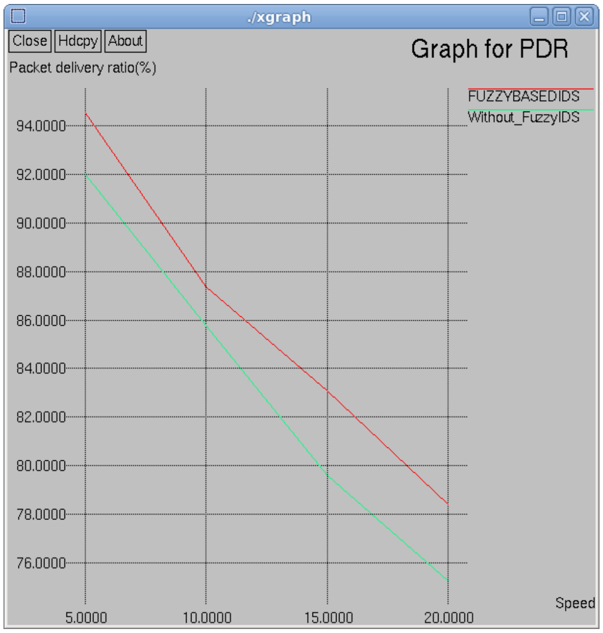

Figure 3: Packet Delivery Ratios

Figure 3 shows when versatility speed is shifting then Packet Delivery Ratio diminishes under ordinary condition and enduring an onslaught Packet Delivery Ratio likewise diminishes. Since when we speed up than more connections are broken in the network.

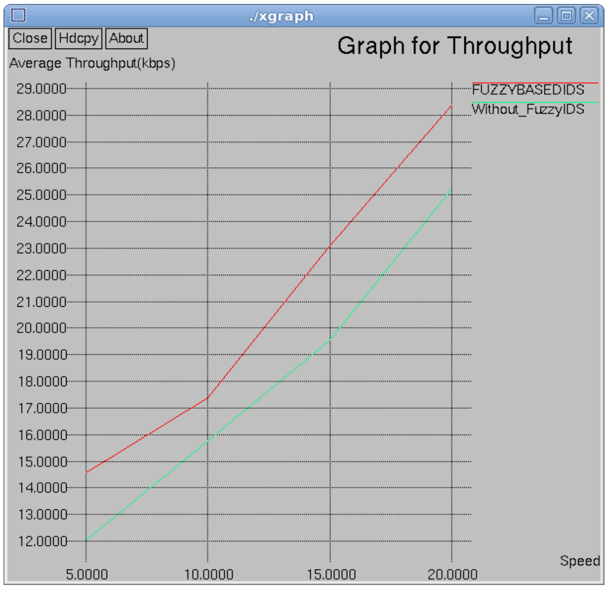

Figure 4: Throughput Computation

Be that as it may, with the utilization of the proposed IDS and the nearness of dark Hole attack node, just the PDR increments to a normal of 80% with just 4% decline from the normal rate if there should be an occurrence of no attacks.

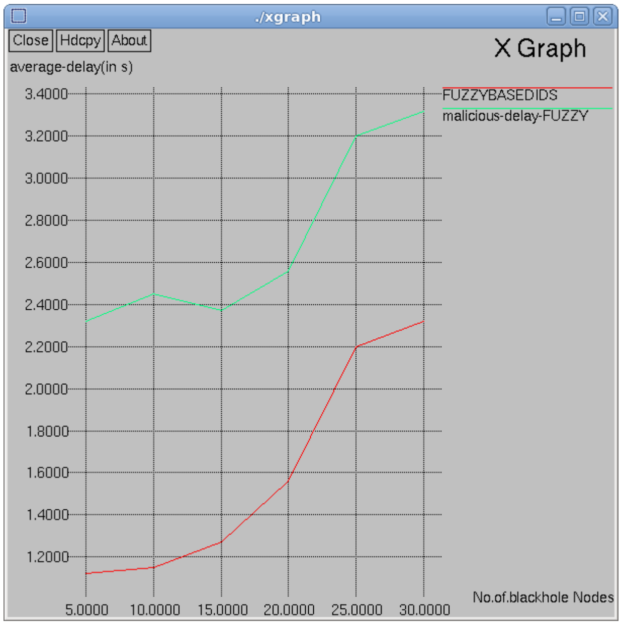

Figure 5: Graph for Average Delay

Network through put scopes to roughly 400 packets in the stateof malicious node by 9 and it around 300 data packets with malicious nodes of two.

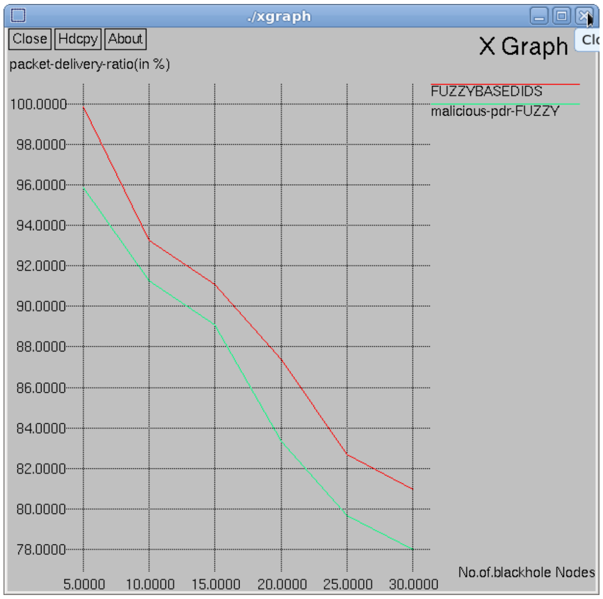

Figure 6: Graph for packet Delivery Ratios

Since malicious nodes are agreeable, they may utilize a few components indemand to sidestep security algorithms. Progressing data packets between one another or making RREP packet by the final node in the path.

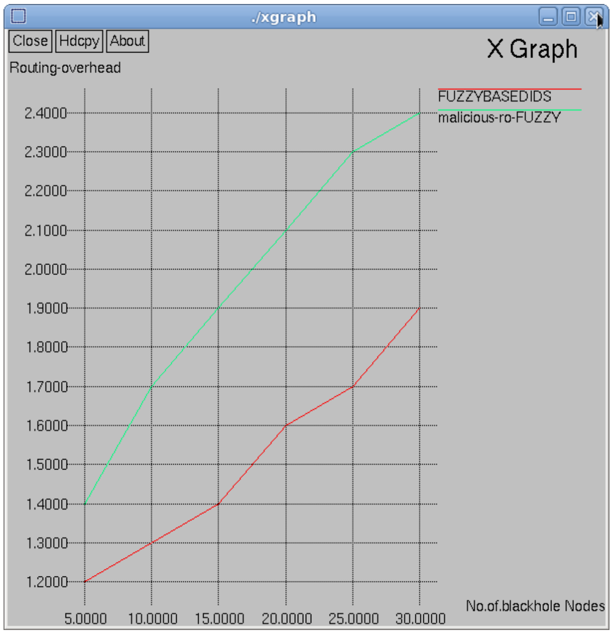

Figure 7: Graph for Routing Overhead

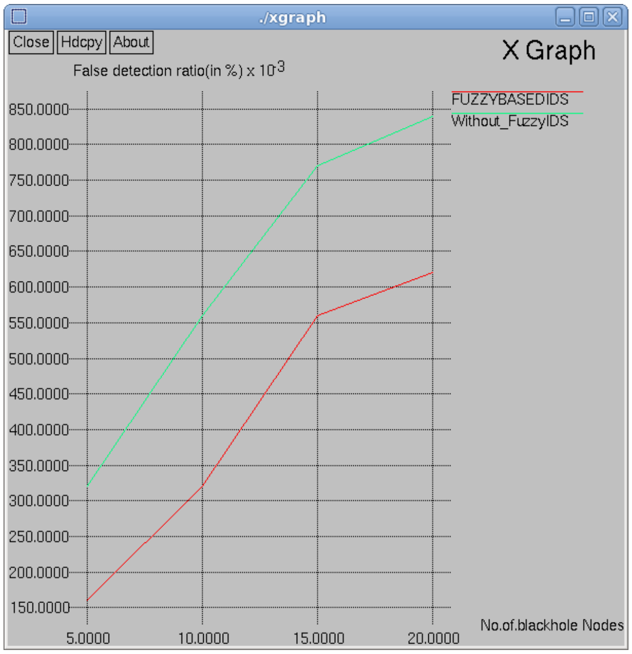

Figure 8: Graph for False Detection Ratio

VI. Conclusion

The black-hole attack is seen as one of the important and genuine attacks which were affected to the network like MANET. The recognition and control of any black hole nodes in the network are seen as a basic undertaking to forestall network breakdown. This exploration, we present a keen black hole discovery and disengagement method that should be deliberate in creating and building any black hole battling protocols or strategies. So to avoid this issue here this paper proposes the Path Identification of Black Hole Check (PIBHC) utilizing neural network. Additionally, orders the attacker path node or not by utilizing the Relevance Vector Machine (RVM) to proceed with further data transmission.

VII. References

[1] Padilla E, Aschenbruck N, Martini P, Jahnke M and Tolle J, “Detecting Black Hole Attack in Tactical MANETs using Topology Graph”, Proceeding of 32nd IEEE Conference on Local Computer Networks, 2007.

[2] S. T. P. Saurabh, \A PDRR based detection technique for blackhole attack in MANET," International Journal of Computer Science and Information Technologies, vol. 2, no. 4, pp. 1513{1516, 2011.

[3] MonitaWahengbam,” Intrusion Detection in MANET using Fuzzy Logic”, 978-1-4577-0748-3/12/$26.00 © 2012 IEEE.

[4] Poonam Yadav, Rakesh Kumar Gill and Naveen Kumar, “A Fuzzy Based Approach To Detect Black Hole Attack”, International Journal Of Soft Computing and Engineering, ISSN: 2231-2307, vol 2, no 3, July 2012.

[5] Revathi B, Geetha D, „A Survey of Cooperative Black and Gray hole Attack in MANET“, International Journal of Computer Science and Management Research, Vol 1, no 2, September 2012.

[6] M. Sengar, P. P. Singh, and S. Shiwani, \Detection of black hole attack in MANET using fbc technique," International Journal of Emerging Trends & Technology in Computer Science, vol. 2, no. 2, pp. 269{272, 2013

[7] J. Ramkumar and R. Murugeswari, \Fuzzy logic approach for detecting black hole attack in hybrid wireless mesh network," in 2014 IEEE International Conference on Innovations in Engineering and Technology (ICIET'14), vol. 3, pp. 877{882, 2014.

[8] A. Chaudhary, V. Tiwari, and A. Kumar, \Analysis of fuzzy logic based intrusion detection systems in mobile ad hoc networks," International Journal of Information Technology, vol. 6, no. 1, pp. 690{696, 2014.

[9] Chaudhary, A., V. N. Tiwari, and A. Kumar. "Analysis of fuzzy logic based intrusion detection systems in mobile ad hoc networks." *BVICA M's*

International Journal of Information Technology 6, no. 1 (2014): 690.

[10] D. Sabarish and C. Ranjani, \Enhanced DSR protocol for detection and exclusion of selective black hole attack in MANET," International Journal of Computer Applications, vol. 112, no. 14, 2015.

[11] K.Santhi et al, “Intrusion Detection System for Black Hole Detection and Prevention in MANET Using Adaptive Neural Fuzzy Inference Systems”, IJCSE, 2015

[12] S. Brar and M. Angurala, \Review on grey-hole attack detection and prevention," International Journal of Advance research , Ideas and Innovations in Technology, vol. 2, no. 5, pp. 1{4, 2016.

[13] Abdel-Azim, M., Salah, H.E.D. and Ibrahim, M., 2017. Black Hole attack Detection using fuzzy based IDS. *International Journal of Communication Networks and Information Security*, *9*(2), p.187.

[14] Yasin, Adwan, and Mahmoud Abu Zant. "Detecting and isolating black-hole attacks in MANET using timer based baited technique." *Wireless Communications and Mobile Computing* 2018 (2018).

[15] Taranum, Fahmina, and Khaleel Ur Rahman Khan. "Maneuvering Black-Hole Attack Using Different Traffic Generators in MANETs." In *Intelligent Systems, Technologies and Applications*, pp. 101-115. Springer, Singapore, 2020.

[16] Thebiga, M. and Pramila, S., 2020. A Survey on Assorted Subsisting Approaches to Recognize and Preclude Black Hole Attacks in Mobile Adhoc Networks. *International Journal of Interactive Mobile Technologies (iJIM)*, *14*(01), pp.96-108.