International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-9 Issue-4, February 2020

Black Hole Attack Detection in MANETs using Trust Based Technique

Mahuwa Goswami, Prashant Sharma, Ankita Bhargava

Abstract*—A Mobile Ad-hoc Network (MANET) is a lot of nodes that impart together agreeably utilizing the remote medium, and with no focal organization. Because of its inborn open nature and the absence of framework, security is a convoluted issue contrasted with different systems. That is, these systems are powerless against a wide scope of attacks at various system layers. At the system level, malignant nodes can play out a few attacks going from detached spying to dynamic meddling. Blackhole is a case of serious attack that has pulled in much consideration as of late. It includes the traffic redirection between end-nodes via Blackhole attack, and also controls the directing calculation to give figment to the nodes situated a long way from one another are neighbours. To handle this issue, we are proposing a novel location model to enable a node to check whether an assumed most limited way contains a Blackhole attack or not. Our methodology depends on the way that the Blackhole attack diminishes essentially the length of the ways going through it. To keep the black hole, worm opening, black hole that is community oriented also the flooding attacks, the measure by which Secure esteem is figured by the premise of the course which is asked, course answer and information parcels. After the count put the stock in values in the range 0 to 1. The event in which that secure esteem is seen more prominent as of 0.5 at that time marks the node is solid and allow on a system commonly piece. The System performance of proposed convention secured secure AODV steering convention (SAODV) is assessed. The result shows execution varies when matched with standard AODV convention.

Keyword : MANET , AODV , SAODV , Blackhole Attack , NS-2

I. INTRODUCTION

With the quick advancement of remote innovation, versatile specially appointed systems have turned out to be progressively utilized in numerous zones and in various structures. A specially appointed system is a lot of conveying substances or nodes having at least one remote interface. This sort of system is conveyed without previous framework and built up powerfully without concentrated organization. Impromptu systems are utilized in a few areas [2] [3] [4], for example, military applications, safeguard tasks, business and modern applications, and so forth. In spite of their numerous advantages, The absence of a focal expert and a predefined framework necessitate that all nodes are effectively engaged with system capacities, for example, steering, tending to, security, and so on.

Revised Manuscript Received on February 28, 2020.
***** Correspondence Author
Mahuwa Goswami*, research scholar , pacific university (PAHER), Udaipur ,Rajasthan, India. goswamimahuwa@yahoo.co.in
Dr. Prashant Sharma , HOD CSE , pacific university (PAHER), Udaipur ,Rajasthan, India. prashant.sharma@pacific-it.ac.in
Ankita Bhargava , Assistant Professor CSE, , pacific university (PAHER), Udaipur ,Rajasthan, India. ankita.bhargava@pacific-it.ac.in

One of the fundamental favourable circumstances of specially appointed systems lies in lessening expenses of usage, since such systems require no earlier framework for their activity [1].
specially appointed systems are exposed to a few difficulties. Notwithstanding its remote nature, MANET is helpless against attacks [5] [6] for some different reasons, for example, absence of framework, restricted physical insurance and assets requirements. Among the most serious attacks against these systems, we are intrigued by those disturbing the steering procedure, exactly the Blackhole attack. To do this attack, a malevolent node catches traffic in one area in the system, and advances it to another noxious node at a remote area. This should be possible utilizing a passage made by two malevolent nodes. The passage might be built up in various courses: out-of-band channel, exemplification, transmission at a high power, and so on. Along these lines, parcels going through the passage arrive first or with fewer bounces contrasted and different bundles transmitted through a genuine course. The point of our work is to build up a Blackhole attack recognition framework, which can be adjusted to portable impromptu systems that utilization receptive steering conventions. The proposed methodology depends on the directing data contained in the traded messages, and additionally on the steering tables of nodes. The location conspire depends on the way that the Blackhole attack easy routes fundamentally ways from a source to a goal, where the quantity of bounces is little contrasted with that of an ordinary way [7].
The rest of the paper is sorted out as pursues. Segment II gives an outline of related work. Area III introduces the Blackhole attack. Area IV depicts the proposed model. Segment VI demonstrates the recreation results. At long last, segment VII finishes up the paper.

II. RELATED WORKS

Anastasia Tsiota et al. creator further spotlight on the difficult situation where end clients can get to a set number of system levels, while we additionally enable various levels to possibly use distinctive range groups. Expecting that effective help gathering from a node having a place with a given system level requires a base got signal quality limit to be achieved, we determine careful articulations and execution limits on the inclusion likelihood of irregular multi-level HWNs with joint sticking and black opening attacks, which rely upon the capacity of system nodes to identify and evade relationship with malevolent nodes (i.e., jammers or black holes).
Definite numerical outcomes feature the value of the proposed investigation, giving significant experiences on framework plan and parameterization towards improved system strength [8].

D. John Aravindhar et al. The directing attacks are one among the potential attacks that makes harm MANET. This paper creators are giveing another strategy for chance mindful reaction system which is joined variant the Dijkstra's most limited way calculation and Destination Sequenced Distance Vector (DSDV) calculation. This can decrease black opening attacks. Dijkstra's calculation finds the briefest way from the single source to the goal when the edges have positive loads. The DSDV is an improved variant of the regular system by including the arrangement number and next bounce address in each directing table [9].

Gibson Chengetanai et al. In MANET Security is one of the issue related with the MANET organize in light of the fact that nodes leaving and joining subjectively whenever and this endanger on the security of the system as some malevolent nodes can promote as potential nodes accessible for steering information parcels to the goal node(s) and these noxious nodes in the end bring about disavowal of administration attacks. This examination has thought of an answer for decreasing community black opening attacks in remote systems. Reproductions utilizing Network Simulator rendition 2.35 (NS2.35) test system apparatus has been accomplished for the proposed Secure AODV directing convention and results have been introduced and looked at against other steering conventions. The reproduction results show that the proposed arrangement performs as far as bundle conveyance proportion and normal start to finish defer comparative with other directing conventions [10].

Shoukat Ali1 et al. Internet of Things (IoT) now continued out to IoET (web of Everything) to awning all accessories abide around, agnate to a physique sensor systems, VANET's, ablaze cast stations, corpuscle phone, PDA's, absolute autos, fridges and agog toasters that can back and allotment abstracts utilizing absolute arrangement advancements. The sensor nodes in WSN accept belted manual extend just as accountable administration speed, stockpiling banned and low array control. Notwithstanding a advanced ambit of utilizations utilizing WSN, its asset answerable attributes brought alternating a amount acute aegis attacks for archetype Particular Forwarding advance the a lot of chancy BlackHole Attacks. Aggressors can after abundant of a amplitude endeavor these vulnerabilities to arrangement the WSN align [11].

Taku Noguchi et al. A black opening attack is one of the outstanding security dangers for MANETs. A black opening is a security attack in which a malevolent node ingests all information parcels by sending phony directing data and drops them without sending them. So as to safeguard against a black hole attack, in this paper we propose another limit based black hole attack counteractive action strategy utilizing various R_REP_S. To examine the exhibition of the proposed technique, we contrasted it and existing strategies. Our reproduction results show that the proposed strategy outflanks existing strategies from the angles of parcel conveyance rate, throughput, and directing overhead [12].

Mengfei Peng et al. author present a response for a strange ring framework using a token model, that is, a ring wherein a enduring number of tokens is the primary strategies for correspondence between the gathering of masters. We ensure that, in such a ring, b+ 9 authorities can fix each flawed center similarly as locate the dark opening that is polluted by this single one-stop diminish contamination. We exhibit the rightness of the proposed course of action and separate its multifaceted design the extent that number of flexible authorities used and complete number of moves performed by these
administrators. We show that in the most exceedingly horrendous case, inside O(kn2) moves, b+9 pros take care of business to fix b broken center points and report the region of the dark gap that is tainted, at any optional point in time, by the one-stop dark disease. [13].

Ida Nurcahyani et al. The black hole attack is one of a few kinds of attacks that happens in MANET. A black opening attack is an attack that causes parcels around the attacking hub to vanish as of the system loses a few data what's more, can lessen its exhibitions. Picking the privilege directing convention is one of the endeavors to limit the effect of black opening attacks in MANET. This investigation was done to think about which is better among AODV and DSR steering convention during black opening attack in MANET. From the reenactment results, the AODV steering convention shows better qualities contrasted with DSR directing convention from a few QoS parameters, for example, throughput, delay, what's more, bundle misfortune; either before being hit by black opening attacks or in the wake of being hit by single black hole and community black hole attacks [14].

III. PROBLEM STATEMENT

- A black hole advance injects acquisition aerial that is accretion significantly.
- This acquisition aerial anon appulse on the arrangement achievement in agreement throughput, end to end adjournment and packet supply ratio.
- The attackers absorb the bulge energy, and abstracts packets information.
- Because of the black hole attacks packets are continuously adapted accordingly packet absent amount is added beggarly while arrangement throughput reduced.

IV. PROPOSED MODEL

The secure level esteem results depends on the parameters can be seen in the table 4.1. The check field displays approx two measurements achievement and disappointment which evaluates that whether the communication established was an efficient and directed transmission or a disappointment. R_REQ and R_REP are the course request and course answer differently which is transferred within the nodes in the system.

The overhead transmitted by the node in the directing way is directed by Information.

Table 4.1 Calculation of Secure Value Parameters

COMMUNICATION TYPE	R_REQ	R_REP	DATA_MAX _QUEUE _SIZE (1000)
R_D_SUCCESS	R_REQ_S	R_REP_S	DATA_S
R_D_FAILURE	R_REQ_F	R_REP_F	DATA_F

The parameter R_REQ_S is customized as the course request for the rate of achievement which is calculated in the respect of the number of surrounding nodes those who have effectively got from the starting node which has communicated it, REEQF customized as the course which does not ask for win rate which is normally based on the number of surrounding nodes which have not got the inquiry ask for, R_REP_S is customized as the rate of course answer achievement which is seen as likely answers gotten by the staring node which has sent. The RREQ and R_REP_F is customised as the rate of course answer disappointment which is figured with respect to the quantity of surrounding nodes which have not answered for the questions ask forgot. The Facts are characterized as the rate of information achievement which is computed with respect of effectively transmitted information and DATA_F is characterized as the rate of information disappointment ascertained in the light of information which are avoided to achieve desired results. It is seen that because of different limitations for every system there will be low information misfortune.

R_R_R = (R_REQ_S – R_REQ_F) / (R_REQ_S+R_REQ_F) …… ….. (1)

R_P_R = (R_REP_S – R_REP_F) / (R_REP_S + R_REP_F) ……. . (2)

R_D_R = (DATA_S – DATA_F) / (DATA_S +DATA_F) …..……. (3)

Where RRR, RPR and RDR are centre of the route esteems which are used to ascertain the Request rate of nodes, Reply rate of nodes and Data transmission rate of nodes. The evaluations of RRR, RPR and RDR are standardized to fall in range between - 1 to +1. If the qualities are varied off the standard range then it is stated as the disappointment rate of the node is increased and it also states that the node which is used o\for comparing may not be used for directing.

T_V = (R_R_R + R_P_R + R_D_R) /3 ..... (4)

Here, secure esteem (value) is the T_V and T (R_REQ), T (R_REP) and T (D_ATA) are the time factorial at which course request, course reaction and information are sent in a specific order by the node. Apart from the earlier stated standardized range, utilizing the mentioned equation the secure esteem (T_V) is stated for every node amid steering and is also checked for the the edge esteem (extend - 1 to +1).

Table 4.2.Threshold Comparison

SECURE VALUE	ACTION	NODE BEHAVIOR
0 - 0.499	Block	Unreliable node
0.499-0.799	Allow	Reliable nodes
0.799 – 1.0	Allow	Most Reliable

I. **Unreliable:** The node of the system which depended is determined as Unreliable node. These types of nodes have secure esteem at least.

II. **Reliable:** The nodes which having the secure level in between the Most Reliable and Unreliable range are put in this category. A node is Reliable to its corresponding when it has sent a some bundles through that node.

III. **Most Reliable:** The nodes which are having higher secure esteems are states as solid node.

This nodes can be considered as the best nodes for other transfer in between different source and the destination in the same system. TAODV verifies every node with its secure to reach at extreme and along with valuable and capable directing and many more to ensure the security level in MANET.

Flow chart for the proposed work

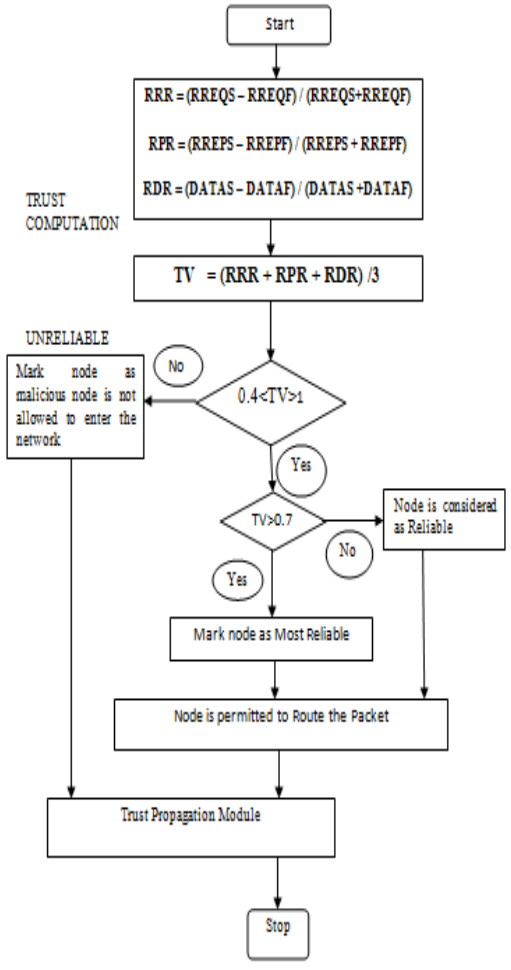


Figure: 4.1Flow Chart of Proposed Method

For the arrangement appeared in figure 4.2, the way to chose the path is S->E->F->D. For example, Node F has seven surrounding nodes and for this node we are figuring the secure esteem.

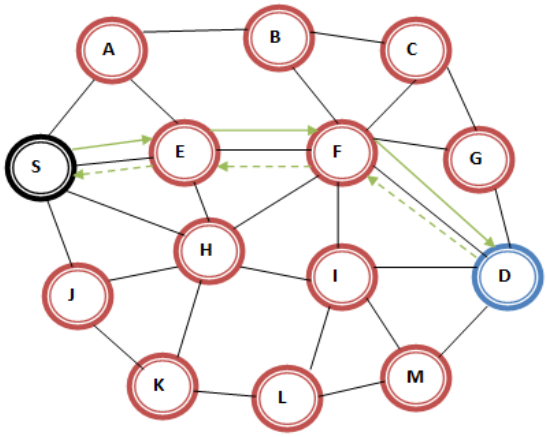


Figure 4.2 A Network sample for Implementing S_AODV

For node E the estimation table of the secure esteem is stated in table 2. This table contains the course demand, answer and information rate for the accomplishment and disappointment of the nodes.

Table 4.3 Secure value calculation for Node E

COMMUNICATION_TYPE	R_REQ	R_REP	DATA_MAX_QUEUE_SIZE_(1000)
R_D_SUCCESS	20	20	400
R_D_FAILURE	0	0	100

R_R_R = (20 - 0) / (20 +0) = 1
R_P_R = (20 - 0) / (20 +0) = 1
R_D-R = (400-100) / (400+100) = 0.6

The estimations of R_R_R, R_P_R and R_D_R are varying in the standardized range defined between - 1 to +1. In this way for the node F the secure esteem is assured.
Television = (1 +1 +0.6)/3= 0.86 (which is more than 0.799) in this way for directing, making this node as a best solid node, this secure estimation is determined for all the nodes in the steering way to screen nodes conduct. In some case that the rate of disappointment builds it will consequently influence the R_R_R, R_P_R and R_D_R esteems, in such way making them drop past the standardized principles with these lines will result in secure esteem not much as desired.

V. PERFORMANCE EVALUATION

In this part, the evaluation of the performance using network simulator NS-2of our model is done.

Table 5.1 summarizes the parameters of our simulations

Parameters	value
Simulation	ns 2.34
Routing protocol	AODV, Adversary Model
Scenario size	1000*1000 6 m^2
No. of nodes	20,40,60, 80, 100
Misbehaving nodes	0-40%
Simulation time	240s
Traffic type	CBR / UDP
No. of connections	20
Pause time	8s
Mobility	4-20 m /s

To examine the correctness of S_AODV with the adversary model, we utilized the NS-2 (ver. 2.35) simulator system. The simulation was performed for two examinations: (1) mobility of nodes was varied and (2) number of malicious nodes was varied. To evaluate the performance of the scheme proposed here, we used packet drop ratio (P_D_R), routing overhead (R_O), energy consumption (E_C). To show that S_AODV will result in better routing decisions; the performance of S_AODV is compared with B_AODV and AODV with the adversary model. Our simulations were carried out in a 1000 _ 1000 m2 area and employed IEEE 802.11 MAC. The benign nodes were randomly distributed throughout the network which employs the AODV, B_AODV and S_AODV protocols. Nodes which are randomly positioned perform various packet forwarding misbehaviours according to the adversary model. Table 5.1 states the simulation parameters.

5.1 Result Analysis Scenario: - Black hole Attacks

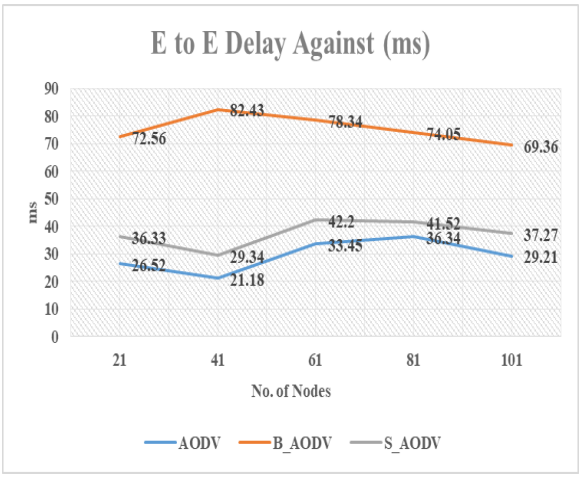
5.1.1 End to End Delay: As compared to Black Hole attack AODV (BAODV) the End to End delay of S_AODV is much better. The average time delay of data that to be sent to destination is the delay that is stated. Here the result have shown on 21, 41,61,81 and 101 number of nodes and used AODV, B_AODV and S_AODV for comparison, the outputs have resulted that S_AODV is much efficient than B_AODV.

E to E Delay = (Arrive time - Send time) / Total Number of Messages sent

EED = Total EED / No. of Packets Sent

Table 5.2 End to End Delay for AODV, B_AODV and S_AODV

E to E Delay Against (ms)			
No. of Nodes	AODV	BAODV	SAODV
21	26.52	72.56	11.23
41	21.18	82.43	14.31
61	33.45	78.34	13.52
81	36.34	74.05	12.23
101	29.21	69.36	11.44



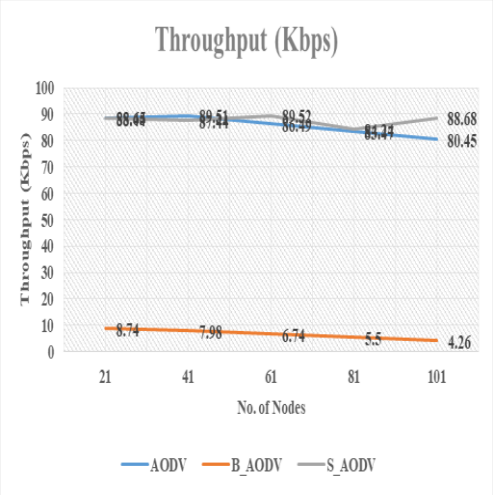
Graph 5.1 For Scenario of Black hole Attacks the End To End Delay

5.1.2 Throughputs: The results of S_AODV is seen more good than Black hole attack AODV (B_AODV). So we can conclude that in case of S_AODV the performances of our network rises at a great extent.

Throughput = (No. of Packets ∗ Packet Size) / Total Time

Table 5.3 Throughput for AODV, B_AODV and S_AODV

Throughput (Kbps)			
No. of Nodes	AODV	BAODV	SAODV
21	88.44	8.74	85.67
41	89.51	7.98	84.34
61	86.49	6.74	79.01
81	83.47	5.5	76.68
101	80.45	4.26	78.35



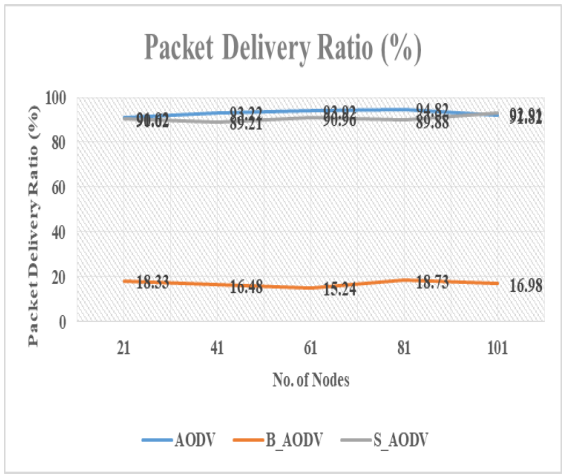
Graph 5.2 Throughputs for Scenario of Black hole Attacks

5.1.3 Packet Delivery Ratio: Packet Delivery Ratio: As compared to Black hole attack AODV, PDR of S_AODV is much better. It is calculated as ratio of number of packet received to the no of packet send. For analysis, the methods like AODV and B_AODV are compared with the result of our method with on different no of nodes. Finally we can state that the method proposed by us if much better than the other methods like B_AODV and we have also compared it with the method AODV.

PDR = No of Packet Received / No of Send Packets

Table 5.4 Packet Delivery Ratio against AODV, B_AODV and S_AODV

Packet Delivery Ratio (%)			
No. of Nodes	AODV	B_AODV	S_AODV
21	91.02	18.33	89.68
41	93.22	16.48	86.71
61	93.92	15.24	87.96
81	94.82	18.73	89.98
101	91.82	16.98	86.11



Graph 5.3 For Scenario of Black hole Attacks Packet Delivery Ratios

5.1.4 Energy (%)

As compared to Black hole attack AODV (B_AODV) and S_AODV, **Energy** of AODV is far better. Show table 5.5 and graph 5.4 Energy for AODV, B_AODV and S_AODV.

Table 5.5 Energy against AODV, B_AODV and S_AODV

No. of Nodes	AODV	B_AODV	S_AODV
21	98.45	62.85	94.53
41	96.85	58.76	91.85
61	97.43	54.83	93.64
81	92.85	42.85	86.27
101	89.67	39.73	83.75

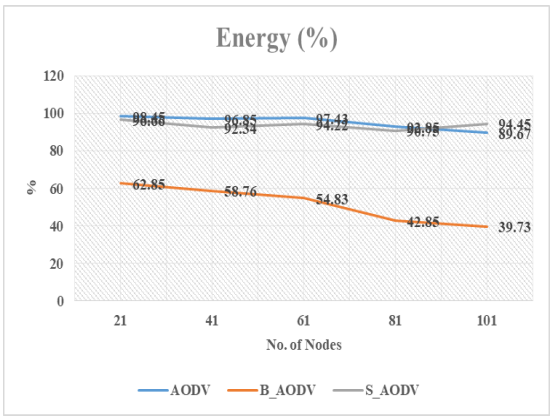


Figure 5.4 Energy against AODV, B_AODV and S_AODV

VI. CONCLUSION

The work proposed here depicts an intense component against Black hole Attack.

The proposed worm opening attack evasion instrument depends on various levelled bunch procedure. Every node in the system will have the capacity to identify vindictive node. All the correspondence between source node and the goal node will occur through group head regardless of the possibility that both source and the goal node are in same bunch or in other group. Every node does not have to always watch the execution of the neighbour node in this system.

In this review, an up degree is being actualized by S_AODV over AODV convention. Attacks imply more than one attack in the meantime propelled along with MANET. We have utilized, situation of attacks mimicked utilizing NS2, in situation comprised of dark opening attack, Blackhole attack and shared black hole attack all the while on the system. In the situation, arranged work S_AODV demonstrates execution advance of system measurements like bundle conveyance proportion, end to end postpone and throughput over AODV directing convention.

REFERENCES

1. Ashish Sharma , Dinesh Bhuriya , Upendra Singh , Sushma Singh, "Prevention of Black Hole Attack in AODV Routing Algorithm of MANET Using Trust Based Computing" , (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (4) , 2014, pp. 5201-5205
2. Nusrat Inamdar, Aliya Inamdar , "PPN: Prime Product Number Based Malicious Node Detection Scheme For MANETs" , (IJARSE) International Journal of Advance Research in Science and Engineering Vol. No. 4 , special Issue (01) august 2015 , pp. 163-170.
3. Neeraj Arya , Upendra Singh , Sushma Singh , "Detecting and Avoiding of Black hole Attack and Collaborative Blackhole attack on MANET using Trusted AODV Routing Algorithm" , IEEE International Conference on Computer, Communication and Control (IC4-2015) , 2015 , pp. IEEE International Conference on Computer, Communication and Control (IC4-2015) , 2015 , pp. 1-5.
4. Ashish Kumar Jain , Vrinda Tokekar , "Mitigating the Effects of Black hole Attacks on AODV Routing Protocol in Mobile Ad Hoc Networks" , 2015 International Conference on Pervasive Computing (ICPC) , 2015 , pp. 1-6.
5. Ashish Sharma, Dinesh Bhuriya, Upendra Singh, "Secure Data Transmission on MANET by Hybrid Cryptography Technique" , IEEE International Conference on Computer, Communication and Control (IC4-2015), 2015 , pp. 1-6.
6. S.V. Vasantha , Dr. A. Damodaram , "Bulwark AODV against Black hole and Gray hole attacks in MANET" , 2015 IEEE International Conference on Computational Intelligence and Computing Research , 2015, pp. 1-5.
7. Upendra Singh, Makrand Samvatsar, Ashish Sharma, Ashish Kumar Jain , "Detection and avoidance of unified attacks on MANET using trusted secure AODV routing protocol" , IEEE Colossal Data Analysis and Networking (CDAN), 2016 , pp. 1-6.
8. Anastasia Tsiota, Dionysis Xenakis, Nikos Passas, and Lazaros Merakos , "On Jamming and Black Hole Attacks in Heterogeneous Wireless Networks" , IEEE Transactions on Vehicular Technology , 29 August 2019 , pp. 1-14.
9. D. John Aravindhar , S. G. Gino Sophia , Padmaveni Krishnan , D. Praveen Kumar , "Minimization of Black hole Attacks in AdHoc Networks using Risk Aware Response Mechanism" , Third International Conference on Electronics Communication and Aerospace Technology [ICECA 2019] , pp. 1391-1394.
10. Gibson Chengetanai , "Minimising Black Hole Attacks to Enhance Security in Wireless Mobile Ad Hoc Networks" , IST-Africa 2018 Conference Proceedings Paul Cunningham and Miriam Cunningham (Eds) IIMC International Information Management Corporation, 2018 , pp. 1-7.
11. Shoukat Ali1, Dr. Muazzam A Khan, Jawad Ahmad, Asad W. Malik, and Anis ur Rehman, "Detection and Prevention of Black Hole Attacks in IOT & WSN" , Third International Conference on Fog and Mobile Edge Computing (FMEC) , 2018 , pp. 217-226.
12. Taku Noguchi , Mayuko Hayakawa , "Black Hole Attack Prevention Method Using Multiple R_REP_S in Mobile Ad Hoc Networks" , 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering , 2018, pp. 539-544.
13. Mengfei Peng , Wei Shi , Jean-Pierre Corriveau , "Repairing Faulty Nodes and Locating a Dynamically Spawned Black Hole Search Using Tokens" , IEEE Conference on Communications and Network Security (CNS) , 2018 , pp. 1-9.
14. Ida Nurcahyani, Helmi Hartadi , "Performance Analysis of Ad-Hoc On-Demand Distance Vector (AODV) and Dynamic Source Routing (DSR) Under Black Hole Attacks in Mobile Ad Hoc Network (MANET)" , International Symposium on Electronics and Smart Devices (ISESD) , 2018 , pp. 1-5.

AUTHORS PROFILE

Ms Mahuwa Goswami, doing M. Tech(CSE) From Pacific Institute of Technology(Udaipur) Rajasthan. I completed my BE(IT) in 2008 from Rajasthan University. I have 7 yrs teaching experience in RIET college in Diploma Section. My interest and research area is Networking and network Securites.

Dr. Prashant Sharma, I have 8 years of teaching experience. I am working as an Associate Professor in the Computer Science and Engineering department of Pacific University, Udaipur (Rajasthan). I completed my Ph.D. in September 2018. I did MTech (CSE) in 2012 and BE (IT) in 2007. My interest and research area is Nature-Inspired Algorithms and Machin Learning.

Ankita Bhargava, Assistant Professor in Pacific Institute of Technology and works as a resource person in various workshops of Data Science and Machine Learning in various colleges. I have 3 years of experience in teaching and 1 year of industry experience in CDAC R&D in Big Data Analytics department. Worked in various projects of Govt.of India.I have done specialization in the field of Data Science, Machine learning and Deep learning using Python.