ISSN 2347 - 3983
Volume 8. No. 9, September 2020
International Journal of Emerging Trends in Engineering Research
Available Online at http://www.warse.org/IJETER/static/pdf/file/ijeter159892020.pdf
https://doi.org/10.30534/ijeter/2020/159892020

Detection of Network Attacks in MANETs Based on Ack based Approach

M.S.R. Kiran Nag[1], S. Nagendram[2], K. Satish[3]
[1]Research Scholor, Department of Computer Science and Engineering, Andhra University, Vizag, AP, India
[2]Associate Professor, Department of Electronics and Communication Engineering, K L E F, Guntur, AP, India
[3] Post Doctor Fellow, Department of Management and Studies, Acharya Nagarjuna University, Guntur, AP, India
kirannag02@gmail.com[1], reena1286@gmail.com[2], drsatish2019@gmail.com[3]

ABSTRACT

MANET is an aggressive and flexible concept to explore randomly organized inter connections between different node locations are identified and modified based on their location of each node. For inter communications between different nodes, there are different types of attacks (i.e. wormhole attacks, grey hole and block hole attacks and etc.) are appeared to access data from other nodes via ambiguity/collision in routing and other specified attacks in wireless network communications. Different types of routing algorithms techniques and approaches like (AODV/DSR) were introduced to handle these types of attacks and increase the performance of network communication in provisions of data delivery ratio, power consumption at each node and identify different behavior of self-organized nodes. So that in this paper, we propose and introduce 2-Phase Acknowledgement Schema (2-PACKS) based on AODV routing scenario between nodes present in wireless network communication. This approach provides on-node strategy to explore re-directing routes from misbehavior nodes to other nodes present in wireless network communication. Simulation results of proposed approach give better and efficient data communication and attack detection results from misbehavior nodes in wireless networks. We also compare results with existing approaches present in wireless network communication in terms of detection of attacks.

Key words: MANETS, AODV protocol, DSR routing protocol, Intrusion detection systems.

1.INTRODUCTION

A mobile adhoc network is a type of multi-hop wireless network. Nodes in the network are mobile in general. The wireless hosts in such networks, converse with each other without the existing of fixed infrastructure and without a central control. Actually each machine in a MANET is randomly move in any direction, and will then alter its associations to other machines frequently. Each must forward traffic unrelated to its own use, and therefore be a router. While MANETs are self contained, they can also be tied to an IP-based global or local network[1]. A MANET does not necessarily need support from any existing network infrastructure like an Internet gateway or other fixed stations shown in figure 1.The physical structure of the network may animatedly change in an random manner so that nodes are free to move in any direction. Information is transmitted in a store-and forward packet switching manner using multi hop routing. Each node is set with a wireless sender and a receiver with an suitable antenna.We presume that it is not possible to have all nodes within each other's broadcasting range.When the nodes are close-by i.e., within broadcasting range, there are no routing issues to be addressed. At any point of time the connectivity between the nodes can disapper.

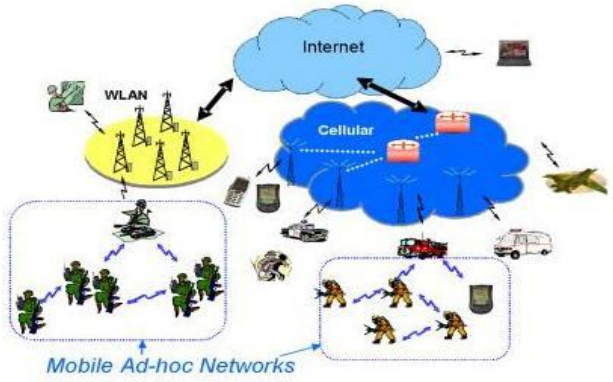

Figure 1: MANET with Data Transmission

MANTEs has numerous wireless application that can be used in a wide number of areas such as E-commerce,military,educationandentertainment.Nodes in MANETs are vulnerable, analyze data, traffic analysis, eaves dropping and attacking routing protocols[2],[3].

Attacks in MANET can also be classified as External attack is an attack conceded out by nodes that do not belong to the domain of the network and Internal Attack is an attack which are actually part of the network.

We deal with two kinds of course-plotting attacks particularly Black hole strike & Gray hole strike. A black hole is a malicious node that falsely repies for route requests without having an active route to the destination and exploits the routing protocol to publisize itself as having a shortest route to destination shown in Figure 2.

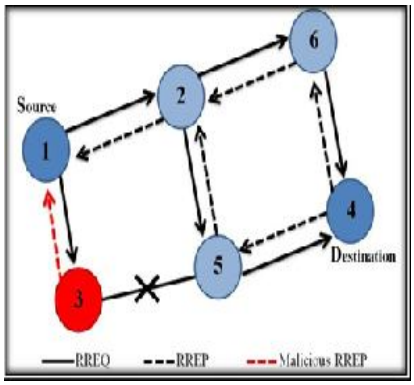

Figure 2: Black hole Attack

When the source select the path including the attacker node, the traffic starts passing through the adversary node and this node starts dropping the packets selectively or in a whole. Black hole region is the entry point to a large number of harmful attacks.

In gray hole attack there are two ways in which a node can drop packets. a) It can drop all UDP packets and b) It can drop 50% of the packets or can drop them with probabilistic distribution[4]. A gray hole attack affects one or two nodes in the network shown in Figure 3 but black hole attack affects entire network. There are two phases of gray hole attacks. It is a hub that can change from acting at present to acting like a dark opening that is really an assailant and it will go about as real hub. So it is hard to recognize the aggressor effectively since it acts as an ordinary hub as shown in Figure 3.

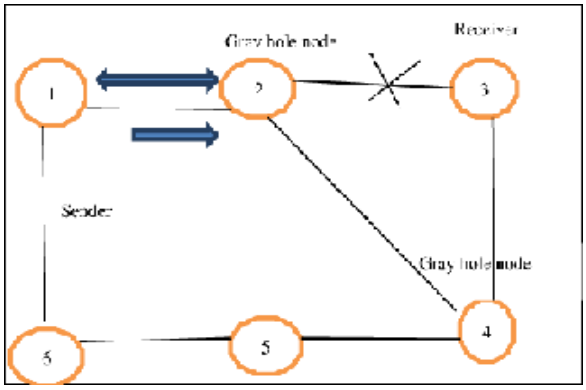

Figure 3: Gray hole Attack

When a gray hole attack takes place in the adhoc network, performance of adhoc network decreases[5],[6]. Gray hole attack decreases certain performance metrics of the network such as packet delivery ratio, end to end delay and packet loss ratio.

In order to decrease and mitigate node routing misbehavior, misbehaving nodes to be detected to avoided by well behaved nodes. So that in this paper, we propose 2-Phase Acnkowledgement Schema (2-PACKS) to decrease effects from misbehaving nodes in network communication[7]. Main basic idea behind proposed schema is, whenever node forwards packets of data successfully from source node to destination hop of next node will send back spetial acknowledgement which called 2-phase ACK to support and indicate that packet which is sented by source node is successfully received. In 2-PACK, transmitted packets takes place with only fraction of data packets sent from source to destination with selective acknowledgement to reduce additional routing scenario hierarchy and routing overhead caused by 2-phase acknowledgement.

Enduring of this document is organized as follows: Section 2 describes existing work for detection block hole attacks in manets. Section 3 explains about AODV routing protocol hierarchy for finding of blackhole and grey attacks attacks. Section 4 achieves 2 ACK schemaprocedure for detection of black hole attacks. Section 5 formalize simulated evaluation results with AODV and DSR in terms of packet delivery ratio and delay configurations and discussions. Section 6 concludes DSR in blackhole in mobile ad hoc networks.

2. RELATED WORK

This section describes about data transmission different authors opinion with detection of different types of attacks in wireless network communication.

In [4], Marti et al. recommended plans that comprises of essential areas, known as watch canine and pathrater, to find and diminish, individually, course-plotting unseemly activities in MANETs. Hubs execute in a wanton strategy wherein, the watch canine component catches the best approach to check whether the ensuing jump hub persistently conveys the bundle. on a similar time, it keeps on an ensure of at present despatched offers[8]-[10]. A subtleties bundle is taken out from the secure when the watch canine catches the similar bundle being introduced through the resulting bounce hub over the procedure. On the off chance that a subtleties bundle stays inside the ensure for a really long time, the watch canine component charges the accompanying jump close by nearby neighbor to cause issues. as needs be, the watch canine permits improper activities recognizable proof at the contribution stage notwithstanding the weblink stage. in light of guard heading in its extra room stockpiling reserve and in the end picks the course that wonderful quits causing issues hubs. on account of its need catching, be that as it may, the watch canine method may likewise don't be fruitful to hit upon unseemly activities or improve wrong security frameworks inside the utilization of indistinct mishaps, collector mishaps, and limited moving quality[11]-[13].

In [14], Awerbuch et al. recommended an On-demand secured Redirecting Strategy to adaptively indicator / indicator / probe faulty links at the course being used. much like the relaxed trace route technique, binary search for is started on faulty paths. Asymptotically, log(n) probes are needed to understand a faulty web website web link on a faulty n-hop route. This strategy most handy works with set mischievous activities and needs to cover the looking through subtleties as ordinary course-plotting control offers. when a web site web interface is recognized as broken, the web connect weight is stretched out all together that the achievement web interface choices will avoid this web site web connect.

In [9], [15] Conti et al. recommended an arrangement to pick tracks focused totally at the strength list of each sure nearby neighbor. each hub keeps a table of strength arachnids of its partners. such a strength inventory mirrors the past accomplishment/dissatisfaction like of parcel signals through this nearby neighbor. for instance, a hit end-to-quit sending will bring about a development of the strength list of the nearby neighbor related with the course. when picking tracks for research signals, hubs pick the ones dependent on the dear companions with higher dependability arachnids.

3. BLACK & GREY HOLE ATTACKS WITH ROUTING BEHAVIOUR

This section describes problems caused by routing scenario between different nodes based on misbehaving routing with following assumptions and notations. Based on bi-directional inter communication regarding properties of network layers. Usually selfishness are usually to individual nodes present in MANETS.

Following notations are used throughput the paper with different factors presented in implementation of misbehaving activities.

X*Y: Area of network

N: Number of nodes in network communication

R: Transmission range of network with omni and bi-directional heterogeneous network.

V_m: Speed of mobile node

h: average number of nodes with source to destination

l: one-node data transmission

d: distance between node to node in network.

P_m= misbehaving node with probability communication for different nodes

P_r = misbehaving route communication

R_{mis} = determine number of 2-pahse ACK schema packets

T_{obs} = observation of declaring node misbehavior

C_{pckets} = forwarded data packets.

Routing Behaviour Scenario

Routing hierarchy with node behaviours consider routing with dynamic source routing (DSR) to issulistrate add-on schema with different node communications. Selfish node does transmit data itself, it describes route recovery and maintenance of route defines DSR protocol hierarchy. Such types of misbehaving nodes enter into route recovery with discovery phase included with routes choosen to transmit data packets from source. Misbehaving nodes refuse data packets with capable of performing following tasks:

1. Packet data transmission with dropped data.
2. Masquerading for each node at receiver node with different node links.
3. Fabricate ACK packets
4. Misbehaving multi-hop next link selection at each node.

Probability of misbehaving route communication with misbehaving nodes is:

$$p_r = 1-(1-p_r)^{h-1}$$

Average number of node communication in data transmission

$$\xi = \frac{N}{X*Y}.\pi R^2$$

Where X*Y is the size of the networks and $\frac{N}{X*Y}$ describes node density.

Propobality of tranmisited circle with different radius r

$$F(r) = \left[\frac{\pi r^2}{\pi R^2}\right], \frac{r^{2\xi}}{R^{2\xi}}$$

Average transmitted data with progress excpected value

$$l = \int_0^R rf(r)dr = \frac{2\xi.R}{2\xi+1}$$

Expected number of hops canbe estimated as

$$h \approx \frac{d}{l} \approx \frac{\sqrt{X^2+Y^2}}{2l} \approx \frac{(2\xi+1).\sqrt{X^2+Y^2}}{4\xi R}$$

Dynamic source routing(DSR) and Ad Hoc On-Demand Vector Routing (AODV) procedure is a sensitive coordinating method for unrehearsed and convenient systems that oversee tracks just between center points which need to interface[16]. Occupying systems are gone facing with a broad assortment of strikes. Dull gap strike is one such strike and such a Denial of administration (DoS) in, a ruinous center point makes usage of the deficiencies of the road finding bundles of the guiding strategy to propel information itself having the snappiest course to the center whose parcels it needs to indentify[17]. This strike is away for changing the controlling method with the objective that movement goes through a specific center administered by the enemy. In the midst of the Path Discovery procedure, the source center passes on RREQ bundles to the moved centers to find clean bearing to the arranged territory. Dangerous centers react quickly to the beginning stage center point as these center points don't relate the coordinating work region. The benefit center point addresses that the road finding technique is done, dismisses other RREP information from various centers and picks the course through the destructive center point to course the information bundles. The perilous center does this by giving a high plan wide range to the response gathering. The enemy currently falls the got information instead of sending them as the methodology needs[18].

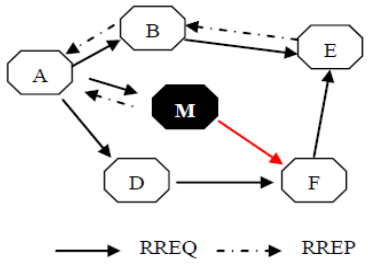

Figure 4: Black hole Attack problem in AODV

In the above Figure 4, build up an unsafe hub M. At the point when hub A sends a RREQ pack, to hub B, D and M get it. But Hub M, being an malicious hub, doesn't check packet request to deal with hub E.

Thus, it in a flash conveys back a RREP pack, proclaiming a way to deal with the area. Hub A gets the route reuest (RREP) from M forward of the route reuest (RREP) from B and D. Hub A speaks to that the straight through M is the fastest course and conveys any group to the area through it. At the point when the hub A conveys data to M, it takes up with different request like a Black hole.

4. 2-PACKS BASED BLACK & GREY HOLE DETECTION

The watch dog algorithm identification procedure [4] has a totally low expense. however, the watch dog approach is pretentious with several issues such as uncertain crashes, heir crashes, and constrained transmitting power. The overall image is that the occasion of a achievements package wedding party can most effective be completely determine at reciever node with next hop links, but this observe dog technique most practical timepieces the transferring from the emailer of the next-hop web website weblink[19].

Notify that, each node with respect to source to destination with subsequent node connection between nodes present in route hierarchy to connect different nodes. In the resulting bounce web site weblink, a performing up sender or a performing up beneficiary has a similar damaging effect on the in arrangement parcel: it will now not be introduced in consideration. The end result is this web site weblink can be perceptible.

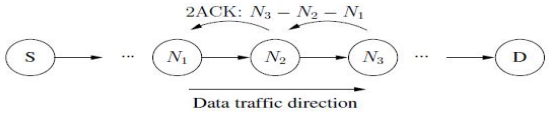

Figure 5: 2-pahse ACK schema Based schema for Black and Grey hole Attacks in MANETs.

The 2-pahse ACK schema plan is a community-layer policy to come across acting up hyperlinks and to minimize their repercussions. it can be taken out as an upload-directly to present redirecting methods for MANETs, including DSR. The 2-pahse ACK schema plan finds bad behavior via the use of a new kind of recommendation packet, known as 2-pahse ACK schema[20]. A 2-pahse ACK schema packet is allocated a set direction of two trips (three nodes), within the opposite direction of the information traf c direction shown in figure 5.

Based on above misbehaving route hierarchy data traffic with simulated nodes present in following Table 1.

Table 1: Probability of misbehaving route communications

Results for p_m = 0.1			
Network Area, X*Y	4R*4R	5R*5R	10R*10R
Number of Nodes, N	70	100	400
Analytical Results	0.18	0.25	0.49
Simulation Results	0.17	0.22	0.43
Results for p_m = 0.2			
Network Area, X*Y	4R*4R	5R*5R	10R*10R
Number of Nodes, N	70	100	400
Analytical Results	0.35	0.45	0.76
Simulation Results	0.31	0.39	0.65
Results for p_m = 0.3			
Network Area, X*Y	4R*4R	5R*5R	10R*10R
Number of Nodes, N	70	100	400
Analytical Results	0.50	0.62	0.90
Simulation Results	0.42	0.52	0.76

Based on above Figure 5, 2-PACKS procedure described as follows

If N1, N2, N3 are three consecutive nodes present in route communication, route is established from dynamic source to destination generated by route discovery phase with DSR and AODV routing protocols. When node N1 send data packets to node N2 and then node N2 forward packets to nodeN, it is not clear to receive consecutive acknowledgement if data transmitted successfully or not. In middle of data transmission wrong node communication appears because of misbehaving nodes[21]. Then 2-Phase Acknowledgement approach follows triplet route recovery procedure to transmit data from N1-> N2-> N3 and it desired from original route hierarchy based on 2PACKS sender acknowledgement based on observed node. Structure of misbehaving node communication as shown in Figure 6.

Option Type	Opt data len	Error Type 2ACK Report Misbehavior	Reserved	Salvage	error source address N_1 (Misbehaving report sender)	Destination S Report receiver	Type-specific information $N_2 - > N_3$ Misbeheving Link

Figure 6: Structure of misbehaving node communication.

When N3 receives data packet then N3 determines and needs to send 2PACKS to N1, in order to reduce additional overhead caused by routing then 2-PACKS defines data transmition acknowledges via 2PACK packets in data transmission with varying R_{ack} and

R_{mis} . 2-PACK schema summarized in pseudo code communication 2ACK packet sendet (N3) to node N1.

4.1 Compare Route overhead Scenarios

Based on above hierarchy 2-PACKS solves following scenarios

Ambiguos node collisions, may occur at node N1, when well specified node N2 behaves and forward data packets towards N3 with concurrent data transmission overhead with respect neighborhood nodes N1, proposed approach solves this ambiguous collision problem with 2-ACK packet data transmission.

Reciever node collisions, may occur N1 gets overhead being transmitted data packets forwarded by N2 then N3 fails to receive packets with neighborhood node selection. Proposed approach explicits 2ACK packets in data transmission.

Overhearing range, may occur when ever low transmission power to send data to N1 to N3. N2 is observing node then it may become misbehaving node based on false report from intermediate nodes. Proposed approach immune to reduce transmitted range issue. 2-PACKS provide privacy from source to destination with computed transmitted range based on random values $x \in \{0,1\}^p$ and then hash function at each node as follows:

$$h_0, h_1, h_2, ..., h_n$$

Based on hash functions available in recent data functions with 2-PACKS packet format shown in Figure 7.

N_2 Next Hop Receiver	N_1 Destination	ID sequence number	MAC Signature	h_i hash release

$$MAC = \left[N_2, N_1, ID \right]_{h_{i-1}}$$

Figure 7: Node format of 2-PACKS

The proposed approach distinguishes route link behavior and temporary route link behavior with the reception of 2ACK packets over certain period of time intervals between nodes with respect to observation period T_{obs}. Since temporary routing links fails with out usually last long activity with distinguishes route link failes from misbehaving routes in network communication[22].

4.2 Partial Data Forwarder

Misbehaving nodes forwarded packets partially based on packets cheat in route monetering system[23]. Then partial data forwarding at node N2 as follows:

$$1 - R_{ack}.R_{part} < R_{mis}$$

Re-arrange the failure route links with different node communications as follows:

$$R_{part} > \frac{1 - R_{mis}}{R_{ack}}$$

Based on patial data forwarding between different nodes then proposed approach gives false route link fails. 2ACK exploits re-arrange route link infront of misbehaving nodes[24].

5. SIMULATIONS AND DISCUSSIONS

In this part, we explain about simulation of proposed implementation using NS3. Based on bandwidth data rate of each node with TCP/IP protocol using 802.11 network versions with suitable node to node communication using the following simulation parameters exposed in table 2 with standard values of node-node communication in wireless network communication. The following parameters are described in detection of attacks in MANETS with data communication. We compare simulation results with AODV, DSR, Static ACK approach and 2-PACKS

A. Packet Distribution Ratio: The rate between the assortment of bundles began by the "application layer" CBR assets and the assortment of bundles got by the CBR course at a predetermined zone.
B. Throughput: Throughput is the how fast the data can pass over the transmission media.which means that the number of bits transmitted per second.
C. Node Mobility: Hub adaptability uncovers the adaptability measure of areas.
D. Packet Delivery Ratio: The Packet Delivery Ratio (PDR) decided for the AODV method when the center adaptability is moved on. The outcomes uncovers both the circumstances, with the diminish fissure assault and without the diminish hole assault. It is resolved that the group dissemination sum

impressively diminishes when there is a difficult center point in the structure. For instance, the group dispersion sum is 100% when there is no effect of Dark hole assault and when the center is moving at the loan fee 10 m/s. however, due to effect of the Dark fissure assault the group assignment sum diminishes to 82 %, considering the way that a segment of the bundles are decreased by the exhausting hole center.

We sanctify simulation results with comparison results of both AODV and DSR for discussion of above considerations with following parameters:

Table 2: Simulation Parameters.

Property	Value
Area of network	1500*1500
Noodes with presented area	60
Time of Simulation	30S
Range of Transmission	250 m
Speed of Mobility	0-20m/sec
Number of Blackhole nodes	10
Check point nodes	4 nodes(Fixed)

Communication Results W.R.T to Time: Time examination brings about manets with hubs correspondence concerning time for parcels droping in center of information conveyance by jump by bounce correspondence. Table 3 shows examination results as for time in information correspondence between hubs.

Table 3: Time efficiency with respect to nodes communication.

Number of Nodes	2-pahse ACK schema	AODV	DSR	Static ACK Approach
10	1.2	1.8	2.4	3.4
20	1.9	2.4	2.5	4.5
30	2.8	3.6	1.8	5.4
40	3.9	4.5	4.2	6.4
50	4.2	4.8	6.4	7.2
60	4.8	5.7	4.8	3.9

The time compass between the start of test framework till the finish of first center is portrayed as Balanced period, the time compass between the finish of first center point till the reenactment terminations is described as flimsy period.

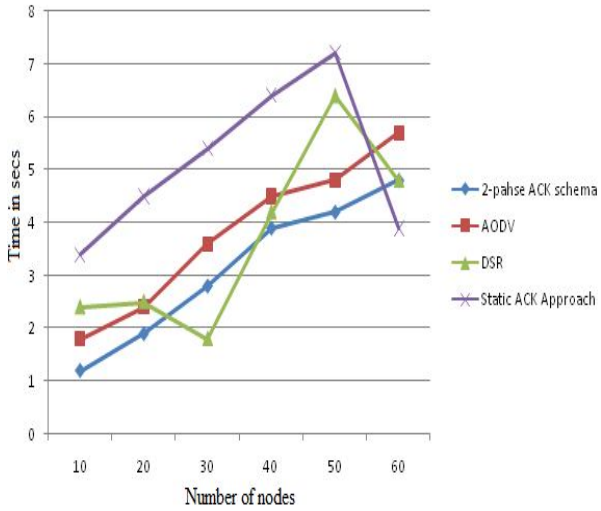

Figure 8: Time efficiency results in real time data communication for wireless sensor networks.

As shown in Figure 8 when ever number of nodes increased then the number of outcomes in real time applications of device to device communication with respect to time in our 2-pahse ACK schema gives efficient communication with out loss of data delivery in MANETs. Ans Figure 8 and Table 4 shows efficient throughput analysis of 2-phase acknowledgement approach with existing approaches

Table 4: Throughput analysis of different with data processing between nodes**.**

Number of Nodes	AODV	2-pahse ACK schema	DSR	Static ACK Approach
50	256	350	278	294
100	324	345	178	290
150	212	412	254	325
200	315	297	324	315
250	278	315	289	320
300	178	425	315	298

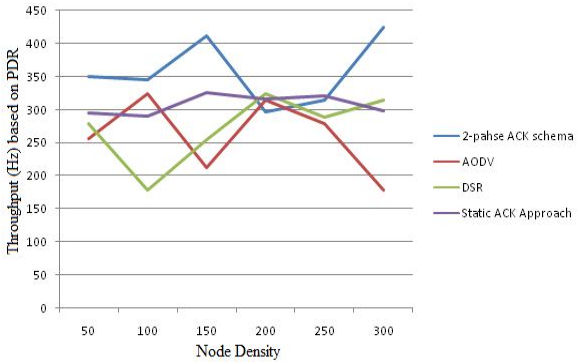

Figure 9: Throughput results in real time data Communication for wireless sensor networks

From conceptual investigation of Figure 8 and 9, we realize that in the entire running of the framework, the force admission of enhanced criteria is much lower than that of 2-pahse ACK schema schema at the same roundabout of test system Table 5.

Table 5: Packet Delivery Ratio with respect to nodes communication.

Number of Nodes	AODV	2-pahse ACK schema	DSR	Static ACK Approach
50	42	48	34	45
100	48	52	49	54
150	54	58	38	39
200	60	65	54	49
250	68	72	48	64
300	75	79	52	64

This balanced the power confirmation of the whole structures, tardy the life-season of shared affair drives which may kick the basin as of now and redesigned the efficiency of the system truly tapering the total power confirmation of the ground-breaking life-cycle.

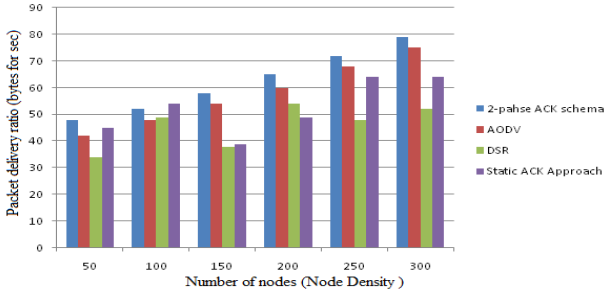

Figure 10: Packet delivery ratio with respect to nodes Communication for processing efficient data transmission in MANETs.

As shown in Figure 10 if the number of nodes increases then the system performance with respect to the number of outcomes in real time data transmission of host to host communication energy consumption in our 2-pahse ACK schema schema gives efficient communication without loss of data delivery in MANETs.

Comarison Results: In this section we have to compare AODV routing protocol with our proposed approach in terms of energy consumption and other proceedings in real time data communication. Our 2-pahse ACK schema gives efficient energy levels as shown in Table 4 and 5 with respect to existing technology of the processing data in device to device communication in wireless adhoc networks for proceedings in commercial data events in device properties and other considerable events in MANETs.

6.CONCLUSION

In this papers, we've got analyzed the performance destruction due to such sel sh (misbehaving) nodes in MANETs. We've got recommended and analyzed a way, known as 2-pahse ACK schema, to recognize and reduce the consequence of such course-plotting bad actions. we've got offered the 2-pahse ACK schema strategy in aspect and described one of a type aspects of the 2-pahse ACK schema strategy. important kinds of the 2-pahse ACK schema strategy had been acquired to examine its performance. Our simulation results show that the 2-pahse ACK schema strategy maintains as much as 91% package submission rate even if there are forty% performing up nodes in the MANETs that we have analyzed. In our achievements paintings, we can check out how to post the 2-pahse ACK schema strategy to other kinds of course-plotting methods and start systems. Further improvement of this approach is to extend to support energy optimization with attack detection in MANETs with efficient data communication.

REFERENCES

1. Gundeep Singh Bindra1, Ashish Kapoor 2, Ashish Narang 3, Arjun Agrawal, **" Detection and Removal of Co-operative Blackhole and Grayhole Attacks in MANETs"** *2012 International Conference on System Engineering and Technology* September 11-12, 2012, Bandung, Indonesia.

2. S.Nagendram, K.Ramchand H rao, and Bojja Polaiah, **"A Review on recent advances of routing protocols for MANET"** *Journal of Advanced*

Research in Dynamical and Control Systems, vol. 2, Issu no. 2, October 2017.Pages:114-122.

3. Sony K, N.D.Indira, S.**Nagendram "Modelling the systems for improvised performance in fso networks".** *JARDCS,*January 2017.

4. Sahu AK; Swain G. "**Data hiding using adaptive LSB and PVD technique resisting PDH and RS analysis".***International Journal Of Electronic Security and Digital Forensics 2019.* 10.1504/IJESDF.2019.102567

5. Oscar F. Gonzalez, Michael Howarth, and George Pavlou, "**Detection of Packet Forwarding Misbehavior in Mobile Ad-Hoc Networks. Center for Communications Systems Research, University of Surrey, Guildford, UK. Integrated Network Management, 2007.** *IM '07. 10th IFIP/IEEE International Symposium* on May 21, 2007.

6. Piyush Agrawal, R. K. Ghosh, Sajal K. Das, "**Cooperative Black and Gray Hole Attacks in Mobile Ad Hoc Networks".** *In Proceedings of the 2nd international conference on Ubiquitous information management and communication*, Pages 310-314, Suwon, Korea, 2008.

7. S.Nagendram, and Ramchand H Rao**, "Survey of different security and routing protocols hierarchy in wireless network communication,"** *IJEAT*, December2018.

8. A. Shevtekar, K. Anantharam, and N. Ansari, **"Low Rate TCP Denial-of-Service Attack Detection at Edge Routers,"** *IEEE Commun. Lett.*, vol. 9, no. 4, Apr. 2005, pp. 363–65.

9. Mohammad Al-Shurman and Seong-Moo Yoo, Seungjin Park, **"Black hole Attack in Mobile Ad Hoc Networks"** *Proceedings of the 42nd annual Southeast regional conference ACM-SE 42*, APRIL 2004, pp. 96-97.

10. Y-C Hu and A. Perrig, **"A Survey of Secure Wireless Ad Hoc Routing,"** *IEEE Sec. and Privacy*, May–June 2004.

11. K. Sanzgiri *et al.*, **"A Secure Routing Protocol for Ad Hoc Networks,"** *Proc. 2002 IEEE Int'l. Conf. Network Protocols*, Nov. 2002.

12. Sanjay Ramaswamy, Huirong Fu, Manohar Sreekantaradhya, John Dixon and Kendall Nygard. **"Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks".** *Department of Computer Science, IACC 258 North Dakota State Universities, Fargo,* ND 58105.

13. Harmanpreet Kaur, P. S. Mann **"Prevention of Black Hole Attack in MANETs Using Clustering Based DSR Protocol"** *IJCST* Vol. 5, Iss ue 4, Oct - Dec 2014 ISSN : 0976-8491 (Online) | ISSN : 2229-4333 (Print).

14. S., Sai Anil P., Pavan E.V.S., Amarendra V. (2019), **'Performance evaluation of wide area network using cisco packet tracer',** *International Journal of Advanced Trends in Computer Science and Engineering*, 8(6), PP.2915-2919.

15. Mr.Rahul Vasant Chavan 1, Prof.M S.Chaudhari **" Enhanced DSR protocol for Detection and Removal of Selective Black Hole Attack in MANET",** *International Research Journal of Engineering and Technology (IRJET)* e-ISSN: 2395 -0056 Volume: 02 Issue: 04 | July-2015 www.irjet.net p-ISSN: 2395-0072.

16. Rajesh, L.; Satyanarayana Penke, "**Vulnerability Analysis and Enhancement of Security of Communication Protocol in Industrial Control Systems**." *HELIX 2019*. 10.29042/2019-5122-5127.

17. B. Awerbuch, D. Holmer, C-N. Rotaru, and H. Rubens, ".**An on-demand secure routing protocol resilient to byzantine failures",.** in *ACM Workshop on Wireless Security (WiSe)*, September 2002.

18. Rao G.A., Syamala K., Kishore P.V.V., Sastry A.S.C.S. (2018) , **'Deep convolutional neural networks for sign language recognition',2018 Conference on Signal Processing And Communication Engineering Systems'**, *SPACES 2018*, 0 (),PP. 194- 197

19. M. Conti, E. Gregori, and G. Maselli, ."**Towards reliable forwarding for ad hoc networks".** in *Proc. of Personal Wireless Communications (PWC '03)*, September 2003.

20. Y. Hu, A. Perrig, and D. B. Johnson, .Ariadne: "**A secure on-demand routing protocol for ad hoc networks".** in *Proc. Of the Eighth ACM Annual International Conference on Mobile Computing and Networking (MobiCom'02)*, September 2002.

21. Sundaraiah P., Sri Kapardi K., Jaya Lakshmi C.H., Srinivas K., Uday Kumar M.V. (2017),**'Comparative study of leach and pegasis energy efficient protocols'**,*Journal of Advanced Research in Dynamical and Control Systems,*9(),PP.1949-1954.

22. Kishore, P. V. V.; Kumar, K. V. V.; Kumar, E. Kiran; Sastry, A. S. C. S.; Kiran, M. Teja; Kumar, D. Anil; Prasad, M. V. D. "**Indian Classical Dance Action Identification and Classification with Convolutional Neural Networks."** *Advances in Multimedia 2018.* 10.1155/2018/5141402.

23. P. Srikanth Reddy, P. Saleem Akram, M. Adarsh Sharma, P. Aditya Sai Ram, R. Pruthvi Raj**;" Study and Analysis of Routing Protocols"** dy et al., *International Journal of Emerging Trends in Engineering Research(IJETER),* 7(11), November 2019, Volume 7, No. 11 November 2019.

24. N V V N J Sri Lakshmi , P. Saleem Akram , V. Madhu Bhragavi , G. Harshika , A. Sravani." **Study and Analysis of Defense Techniques for Various Network Topologies"** *International Journal of Emerging Trends in Engineering Research(IJETER).* Volume 7, No. 11 November 2019.