Volume: 15 Issue: 03 Pages: 5959 - 5966 (2023) ISSN: 0975-0290

Detection of Malicious Nodes in UAV-IOT Environment

Anuradha Banerjee[1], Subhankar Ghosh[2]
[1] Kalyani Govt. Engg. College, Kalyani, NadiaWest Bengal, India anuradha79bn@gmail.com
[2]Department of Computer Science and Engineering,
Research Scholar, Kalyani Govt. Engg. College, subhankar_1980@rediffmail.com

---ABSTRACT---

These days UAV-IOT collaborative environment has become a hot topic for research because UAV adds significant potential to the IoT devices. However, there are multiple issues to address like resource allocation, trajectory optimization energy preservation, selfish and malicious node detection etc. In this article we propose a decision tree based selfish and malicious node detection technique based upon information like residual energy, energy depletion rate, present reputation and credibility of alternative routers. Based on this, next reputation is decided and the node is identified as non-malicious or malicious. During selection of route from clusterhead to a cluster member, malicious nodes are avoided as much as possible, to reduce unnecessary consumption of energy and time.

Keywords - Credit, Energy Efficiency, Malicious, Random Forest, Unmanned Aerial Vehicle

Date of Submission : September 17, 2023 Date of Acceptance : October 14, 2023

1. INTRODUCTION

IoT or internet of things is a composite environment consisting of smart devices that can be operated by multiple users residing in different geographical location in the world. This is extremely important in modern era where our day to day life activities are supported by such elements and we can not do without those. These devices are required during war, natural disaster etc. for surveillance, relief work, delivering food and medicine in remote and affected places. Also an increased number of temperature and fire sensors are being deployed in educational institutions, companies, hospitals, agriculture fields, zoo etc. to enhance security of students, teachers, employees, patients, crops, animals, and so on. Summarizing we can say that, IoT devices have become indispensable in our society and to successfully organize functioning of these devices, there should be unmanned aerial vehicle or UAVs to process the information such device deliver.

Communication between UAV and IoT devices is two way. Since the sensors have very low processing capacity, they submit their tasks to UAV for execution and subsequently results have to be delivered back from UAV to IoT devices. After executing a batch of some tasks, the UAV flies to another such set of nodes to execute another batch of tasks. This enables efficient resource sharing reducing the cost. But some devices tend to behave maliciously and try to snatch more cpu time by sending tasks to UAV through head of their own cluster before prescribed time stamp. These nodes are termed as disobedient for which legitimate task execution requests suffer and starve. This starvation can be reduced by properly identifying disobedient nodes and isolating them from the network after incidents of recurrent disobedience. The various types of attacking methods are denial of service (DoS), injecting enormous traffic (IET) and injecting-traffic-before-prescribed-timestamp (ITPT). The IoT devices are grouped into clusters and head of each cluster stores communication behavior of devices under it, in terms of residual energy, energy depletion rate, job arrival and departure rate, job queue size, reputation of sender of the current job, reputation of the router being investigated number and credibility of the alternative routers and their past behavior. Isolating malicious nodes from the network relieve the UAVs from executing their tasks and the routers from forwarding those. This is expected to result in reduction of energy consumption in UAV as well as IoT devices. Also legitimate IoT devices are anticipated to get access to UAV much faster leading to reduced latency in the system. Also the system is much more safe after identification of malicious nodes. Unique contributions of our present research work are as below:-

i) It differentiates between obedient and disobedient nodes.

ii) Identifies the attacking methods denial of service, injecting enormous traffic and injecting traffic at wrong timestamps. Injecting traffic at wrong timestamp is a new attacking mechanism which is specifically applicable for UAV-IoT environment.

iii) The issue of detection of malicious IoT devices is crucial for UAV-IoT environment but the issue is inadequately addressed in literature.

2. RELATED WORK

Among the articles that focus on recognizing malicious nodes, references [2], [3], [6-9], [10-12], [15-20], [22-47] are mention worthy. These can be divided into three clusters - articles that consider malicious nodes in sensor networks; articles that detect malicious nodes among IoT devices in UAV -IoT environment, articles that detect malicious activity among UAV devices. The literature on detection of selfish and malicious nodes in ad hoc and sensor networks is quite vast [22-47] and various techniques are applied in these including reputation based, credit-based, machine learning and so on. Reputation is a number that increase with cooperation of nodes and reduces non-cooperative behavior. Machine learning based techniques mostly use support vector machines to detect nodes as malicious or non-malicious. The problem is a two-class problem [25-28]. In some articles decision tree and logistics regression has also been used [30, 32, 33]. Credit based systems [35-37] allocate credits to each node based on their communication behavior. The methods use currency to pay the nodes to forward the packets and nodes gain more currency by cooperating with others and nodes with high credit demonstrate more reliable behavior where as those with low credit seem unreliable and avoided in communication.

In [7], of block chain based chained drown mechanism is proposed where malicious nodes are identified using federated learning in combination with RF and SVM classifiers. Here the environments consist of multiple drones which safely communicate with each other’s for the purpose of evaluation of performance of each other like watchdog. Articles [9] and [10] are also concerned with behavior of UAVs only whereas the issue of discussing communication behavior of malicious nodes is inadequately explored in literature. In the present article we try to fill this gap [47-62].

3. Proposed Method DTDM

3.1 Model architecture

The system consists of multiple UAVs with multiple IoT devices under the administration of each UAV. The set of all IoT devices in the system is clustered using hierarchical cluster algorithm (HCR) where clustering is based on Cartesian distance between the devices. The clusters may be single or single or multiple-hop. Multiple such clusters are enclosed within coverage area of one UAV. Each cluster head has one task queue where tasks submitted by cluster members, gather in an order defined by weightage. Weight is calculated depending upon certain factors. Hierarchical clustering is applied because it doesn't require number of cluster information and also it is easy to implement. The UAV travels from head of one cluster to another transferring information and executing task, based upon the data, they do not compute anything. Responsibility of processing it lies on the UAVs since they have some computing capability. Fig 1 demonstrates architecture of the proposed system. Fig 1 shows structure of one UAV-IoT system where four clusters are there CL1, CL2, CL3 and CL4 No. of hops CL1, CL2, CL3 and CL4 are 3 hop, 2 hop, 2 hop and 1 hop. So it is maximum 3-hop cluster arrangement. Information about various cluster members is stored in head of a cluster, as shown in table T (table 2). Similarly each UAV stores information of various clusters under the coverage area as per table T' (table 3). Associate attributes are stored in devices an id members and geographical location of each successor and predecessor along with average of waiting time of all messages forwarded so far by the successors.

Whenever a job request reaches the clusterhead CH, the entire path of the packet is also sent so that CH can properly update residual energy of nodes in its history. If a sender does not receive result of a job request it forwarded TH time ago (where TH is a threshold), it raises complaint to CH through come other path, against its immediate successor nj mentioning the path it is supposed to follow. Receiving this complaint, CH waits again for threshold time TH. If any other complaint is not received from nj or any mentioned successor of nj, mentioning the same job id, then behavior of ni is suspicious and it may have raised denial of service attack. However CH find out the attacker and applies decision tree to decide whether the attacker should be blacklisted or not.

$$TH = \max(\text{del-res}(i,2), \text{del-res}(i,3)..., \text{del-res}(i,np))$$

del-res(i,v) is the time lapsed between transmission of a job by the sender and receiving its result, s.t. $1 \le v \le np$

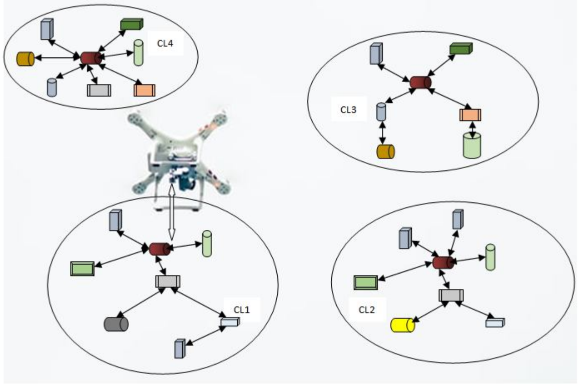


Fig 1: Clustered network of IoT devices

Table 1: Attributes of Table T

Name of The Attribute	Significance
dev-identifier	an identifier that uniquely defines an IoT device
head-status	head is indicated by 0 in this field and ordinary number by 1
location	geographic location in terms of X and Y coordinates
tmst 1	current timestamp
tmst2	timestamp of responding to service request
tsk - nm	summation of number of tasks generated by various IoT devices
wst - enrg	summation of the amount of energy required by devices to forward service request
wst - time	summation of the amount of time required by devices to forward service request

Table 2: Attributes of Table T′

Name of The Attribute	Significance
dev-con-id	Identifier of the connected devices
Loc	geographical position as the ordered pair of latitude and Longitude
tmst	current time
av_wait - time	average waiting time of all massages forwarded by the current IoT device
time-sub-srvice	timestamp of sending next service request

3.2 Identification of Malicious Nodes

Among various attacking methods we consider three in this context - denial of service attack, injecting enormous traffic and injecting traffic before prescribed timestamp. Each clusterhead maintains the following information about each of its members

i) n_i– unique identification number of device node i
ii) max – eng (i) – maximum battery power of n_i
iii) res – eng (i) – residual battery power of n_i
iv) eng – dep – rate (i) energy depletion rate of n_i
v) job – q – size (i) – size of the filled portion of job q of n_i
vi) rp (i) – current reputation of n_i
vii) β (i) – amount of energy required by n_i to receive a message
viii) f (i) – message transmission capability of n_i
ix) del (i) – maximum time delay to send the message n_i to CH
x) job – gen – rate (i) – rate of job generation by nodes
xi) next – pres – time (i) – next described time of job generation of node n_i
xii) status (i) – it has two values 0 or 1. 0 specifies non cooperative behavior anc specifies cooperative behavior

3.2.1. Denial of Service Attack

3.2.1.1. Evaluation of Relevant Parameters

a) Residual Energy

let, upto the current time t, ni has generated pi set of task and forwarded qi se of task. In order to receive each message, amount of energy required by ni is βi and for forwarding a message packet pli through chosen downlink neighbour nj, required energy is {K f(i)/dist^2 (i,j)} where K is a constant, f(i) is message transmission capability of ni; dist(i,j) is Cartesian distance between ni and nj s.t. nj ϵ D(i). D(i) is set of downlink neighbours of ni. Among these, nj has been chosen for forwarding pl(i). so, C(pl(i)) ϵ D(i) and j=c(pl(i)) where nc(pl(i)) is the downlink neighbour chosen by ni to forward pl(i)th packet Depending upon all these notations, residual cenergy αi(t) is formulated in (1).

$$\alpha_i(t) = E_i - F_1 - (i) - F_2(i) \quad (1)$$

Where,

$$F_1(i) = \sum\nolimits_{pl(i)\epsilon p_i} \frac{K+(i)}{dist^2(i,c(pl(i)))} \quad (2)$$

$$F_1(i) = \sum\nolimits_{pl(i)\epsilon q_i} \left(\beta_i + \frac{K+(i)}{dist^2\left(i,c\left(pl(i)\right)\right)}\right) \quad (3)$$

res-eng(i) = $\alpha_i(t)$

where t is the current time

b) Energy Depletion Rate

Energy depletion rate is calculated after every ζ amount of time interval. Let current residual energy of ni at time t is a α1(t) and the same ζ time back was αi (t-ζ). Therefore energy depletion rate for all job request packets transmitted between αi (t) and αi (t-ζ) is given by ϒi(t) in (4).

$$\Upsilon_i(t) = \left(\frac{\alpha_i(t-\zeta)-\alpha_i(t)}{\zeta}\right) \quad (4)$$

c) Job Queue Size

Current job queue size is predicted using ARMA model and job queue size at time t is predicted based on the same at time t-1, t-2, t-3… till time 0, as shown in (5),

$$FJ(t) = ARMA - pred(FJ_i(0), FJ_i(1), \ldots FJ_i(t-2), FJ_i(t-1)) \ (5)$$

ARMA – Pred is a function that predicts values using ARMA model

d) Current reputation

Ri (t) is also predicted using ARMA model based on the same at time t-1, t-2, t-3… till time 0, as shown in (6).

$$R_i(t) = \text{ARMA-pred}\ (R_i(0), R_i(1) \ldots R_i(t-2), R_i(t-1)) \quad (6)$$

3.2.1.2 Decision Tree For Possible Blacklisting of Suspicious Nodes

Decision tree is a powerful supervised learning algorithm which has been used in this article to take decision on possible blacklisting of a node. If a complaint is received by CH against a node nk, CH wait for second time interval after which is compute,

i) New reputation
ii) New job queue size
iii) New status

New reputation and new job queue size are computed using ARMA model as in (5 and 6). f(i) or message transmission capability and max-eng(i) or maximum battery power remain the same. New eng-dep-rate(i) is computed applying ARMA model. β(i) also remains the same. New values of job-gen-rate and next-pres-time are communicated using ARMA model. Based on all these attributes, new value of status is computed using decision tree. Available data is sliced as 80% and 20% where 80% is training data and 20% is testing data. Information gain is applied to select one among the attributes mentioned in history of nodes or cluster members, which is supposed to be placed at the root. Calculation of information gain is based upon the concept of entropy or "measure of uncertainty" as measured in (8).

$$IG = \text{Entropy (parent-node)} - \text{Entropy (children-node)} \quad (7)$$

$$\text{Where, Entropy} = -\sum_{i=1}^{N} pb_i \log_2 pb_i \quad (8)$$

"information gain" is specified as IG. Entropy (parent-node) is self-explanatory. Entropy (children-node)denote average of entropies of all the children. In (8), pbi specifies probability of random selection of an element is class i.

Among the attributes of decision tree, max-depth, min-samples-leap and min-sample-split are mention worthy. In our implementation, we set max depth to be equal to 12 where selection is allowed based on all the attributes in history. min-sample-leap and min-sample-split are set to 1 and 2, respectively because least number of samples is 1 and minimum is 2 samples are required before splitting. Similar to any other prediction algorithm it's efficiency can be expressed using accuracy, precision and recall. These are measured as the functions of true positive, false positive, true negative and false negative.

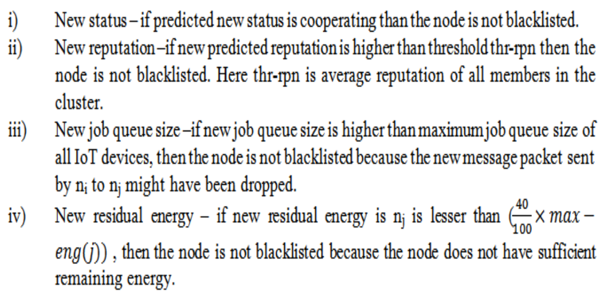
$$accuracy = \frac{true-positive+false-negeative}{(true-positive+true-negative+false-positive+false-negetive)} \quad (9)$$

$$precision = \frac{true-positive}{(true-positive+false-positive)} \quad (10)$$

$$recall = \frac{true-positive}{(true-positive+false\ negetive)} \quad (11)$$

3.2.1.3 Detection of Dos Attack

If the clusterhead CH receives complaint against a node nj , it checks the followings.



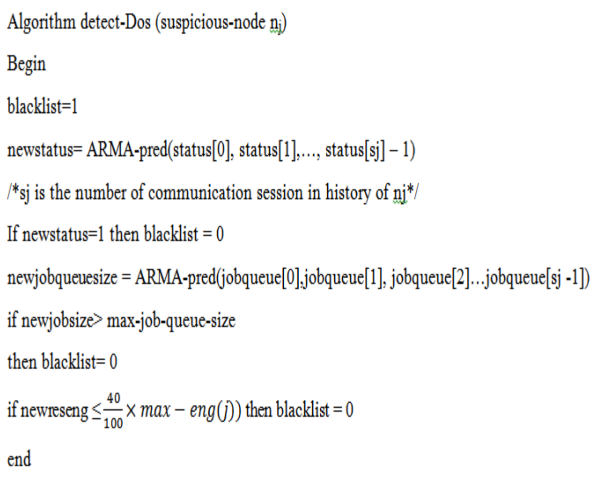
i) New status – if predicted new status is cooperating than the node is not blacklisted.

ii) New reputation –if new predicted reputation is higher than threshold thr-rpn then the node is not blacklisted. Here thr-rpn is average reputation of all members in the cluster.

iii) New job queue size –if new job queue size is higher than maximum job queue size of all IoT devices, then the node is not blacklisted because the new message packet sent by n_i to n_j might have been dropped.

iv) New residual energy – if new residual energy is n_j is lesser than $(\frac{40}{100} \times max - eng(j))$, then the node is not blacklisted because the node does not have sufficient remaining energy.

The corresponding algorithm appears below.



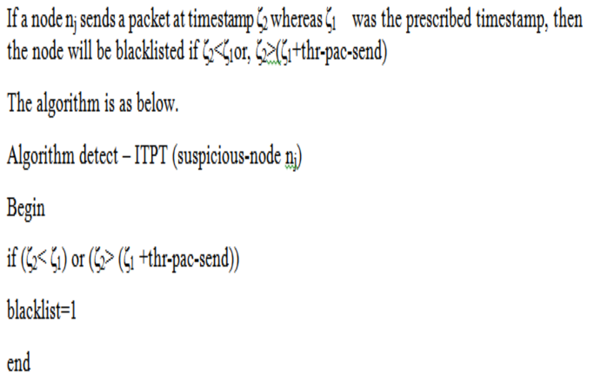
```
Algorithm detect-Dos (suspicious-node nj)
Begin
blacklist=1
newstatus= ARMA-pred(status[0], status[1],…, status[sj] – 1)
/*sj is the number of communication session in history of nj*/
If newstatus=1 then blacklist = 0
newjobqueuesize = ARMA-pred(jobqueue[0],jobqueue[1], jobqueue[2]…jobqueue[sj -1])
if newjobsize> max-job-queue-size
then blacklist= 0
if newreseng $\leq \frac{40}{100} \times max - eng(j))$ then blacklist = 0
end
```

3.2.2. Injecting Enormous Traffic Attack

If job-gen-rate (j) is higher than a predefined thresholds-rate, then the node is blacklisted without any further consideration. The corresponding algorithm appears below:-

```
Algorithm detect_IET (suspicious-node nj)
Begin
If job-gen-rate (j)>th-rate
Blacklist=1
End
```

3.2.3 Injecting Traffic before Prescribed Timestamp Attack (ITPT)



If a node n_j sends a packet at timestamp ζ_2 whereas ζ_1 was the prescribed timestamp, then the node will be blacklisted if $\zeta_2<\zeta_1$or, $\zeta_2>(\zeta_1$+thr-pac-send)

The algorithm is as below.

```
Algorithm detect – ITPT (suspicious-node nj)
Begin
if ($\zeta_2 < \zeta_1$) or ($\zeta_2 >$ ($\zeta_1$ +thr-pac-send))
blacklist=1
end
```

4. Simulation Environment Result and Discussion

4.1 Simulation Environment

Table 3 demonstrates the simulation environment. Each UAV covers a fixed geographical area in which clusters of IoT devices are there. Clustering has been performed based on Cartesian distance of the nodes: nodes which are in the close proximity with each other are placed in the same cluster where distance nodes are placed in different clusters. Number of simulation runs is 5. Number of UAVs increase in different simulations runs. The parameters like hovering altitude, computing power, transition power, channel gain etc. are supported by references [28, 35, 36, 38 and 39].

4.2 Simulation Metrics and Results

For better understanding of the proposed scheme, we compare DTDM embedded version of routing protocols EETS (Energy efficient Task Scheduling [50]) and TSIE (Task Scheduling for Indoor Environment [51]) with their ordinary versions. The performance metrics are UAV-energy-consumption, IoT_energy-consumption average-delay and connectors-in-detection. These are mathematically formulated below:

$$UAV-energy-consumption=\sum_{l=1}^{no-of-UAV} UAV-eng(l) \quad (12)$$

Where UAV-eng (l) is energy consumption in l-th UAV

$$IoT-energy-consumption=(\sum_{l=1}^{no-of-UAV} \sum_{k=1}^{\Psi(l)} IoT-eng[l,k]) \quad (13)$$

IoT-eng[l,k] is energy consumption of k- th IoT device under supervision of l-th UA

average-delay=(tot-amt-delay/tot-number-task))*100 (14)

Mathematical formulation of delay appears in (14). tot-amt-delay and tot-number-task denote summation of delay of all tasks and total number of tasks, respectively.

Correctness-in-detection

$$=\frac{|no\_of\_detected\_nodes-no\_of\_actual\_malicious\_nodes|\times 100}{no\_of\_actual\_malicious\_nodes} \quad (15)$$

no-of-actual-malicious-nodes specify actual number of malicious nodes in the network and no-of-detection-nodes denote number of malicious nodes that have been detected. In both EETS and TSIE schedules only the UAVs and IoT devices are scheduled only on FCFS or first-come-first-served basis which is not energy-efficient at all. Our proposed scheme-DTDM relieves the UAV from serving requests of malicious nodes and therefore a lot of energy is saved as shown in fig 2. A lot of energy is saved in IoT devices too (fig 3) because forwarding requests from malicious IoT devices no longer need to be carried out. Along with that the time that would have been required for serving those requests, is also saved. Therefore, average delay is much lesser in DTDM embedded scheduling algorithms in UAV-IoT environment, Hence, average delay for executing of tasks also reduce in DTDM embedded version of protocols (fig 4). This reduces packet contention and collision decreasing packet loss rate. Also percentage of correct detection of malicious nodes is very high in our environment because those are based on evidences (as shown in fig 5). Benefit of doubt is given to the suspicious node if its residual energy is less than or equal to 40% of initial or maximum battery power. 40% of initial battery power is termed as threshold and any node cannot remain operational if its battery power. In that case forwarding packets is impossible for a node and in this case the suspicious element is not blacklisted. Similarly if its queue is full then it is bound to drop packets and therefore the node is not marked as non-cooperating. Another criterion is the status. If behavior of the node was mostly cooperating as per records in history and its predicted value does not identify it to be non-cooperating then also the node is not blacklisted. All these evidences properly justify blacklisting or not blacklisting a node after being suspected of issuing Dos attacks. Similarly detection of IET and ITPT type of attacks are also performed based on proofs and hence they are mostly correct. This specifies the huge improvement caused by DTDM embedded versions of communication protocols compared to their ethnic versions.

5. Conclusion

Identifying the selfish and malicious nodes in UAV–IOT environment is extremely important because malicious devices do not cooperate and drastically reduce performance of the overall system. Here we have proposed a reputation based method that applies decision tree to classify a node as cooperating or non –cooperating. New status is predicted based on current behavior whereas previous status is denoted by reputation. Three types of attacks are considering –DOS or Denial of Service, Injecting Enormous Traffic or IET and Injecting Traffic before Prescribed Timestamp or ITPT. Considering all these attacking methods, malicious nodes are detected with huge amount of accuracy. In future we want to extend our work to other attacking methods that can be implemented in UAV –IOT environment.

Table 3: Simulation Parameters and Value

Name of Parameter	**Value**
Coverage Area	200×200 m^2
Number of devices	200, 400, 600, 800, 1000 in five different simulation runs
Number of UAV	2, 4, 6, 8, 10 in five different simulation runs
Hovering altitude of UAV	6m
Computing power of UAV	0.5 G CPU cycles per second
Transition power of IoT devices	100-200 m W
Wireless channel gain	-30 dB
Noise power	-50dbm
UAV speed	10 m/s
Transmission bandwidth	200 kHz
Clustering algorithm	Hierarchical clustering algorithm
Competitor protocols	Energy efficient Task Scheduling (EETS), Task Scheduling For Indoor Environment (TSIE)

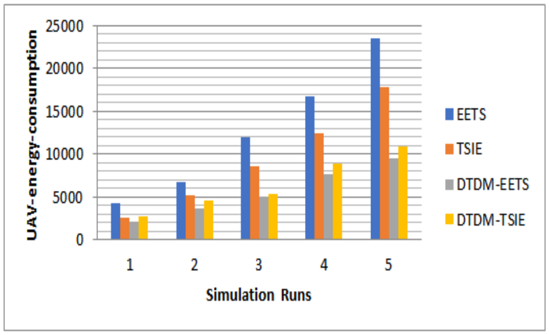


Fig 2: UAV-energy-consumption in various simulations run

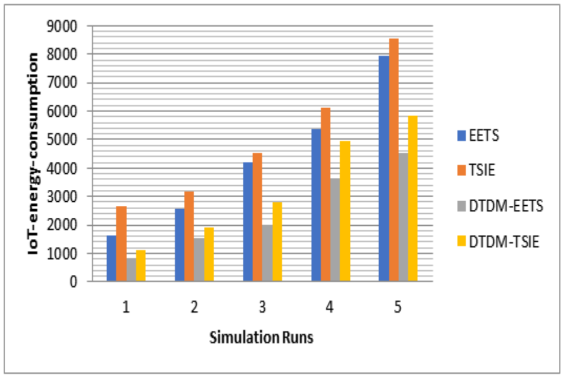


Fig 3: IoT-energy-consumption in various simulations run

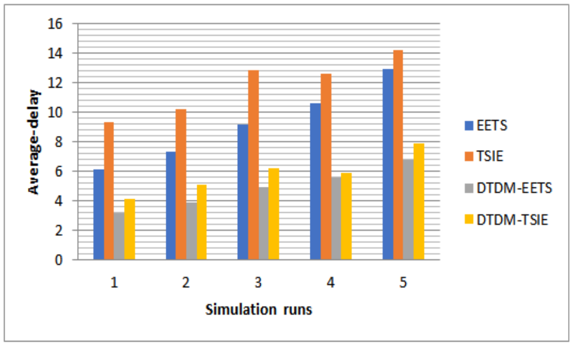


Fig 4: Average delay in various simulation runs

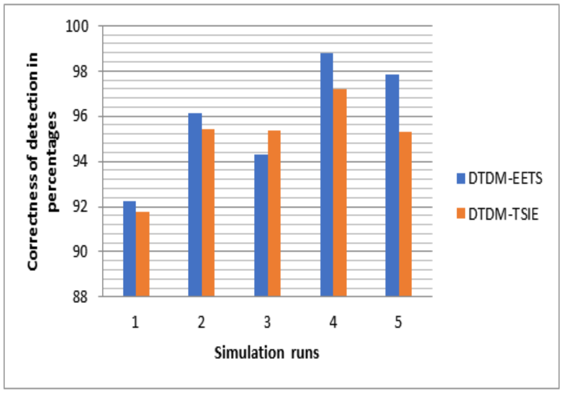


Fig 5: Correctness of detection in percentage in various simulation runs

REFERENCES

1. Perkins C E, Highly dynamic destination-sequenced distance vector routing for mobile computers, ACM Comput & Commun Rev, 14 (2) 234-244
2. Murthy S & Garcia-Luna-Aceves J J, An efficient routing protocol for wireless networks, in Mobile Networks and Applications (Kluwer Academic Publishers) 1996, 183-197.
3. Chen T W & Gerla M, Global State Routing: A new routing scheme for ad hoc wireless networks, in Proc IEEE Int Conf on Communications, 1998.
4. Chiang C C, Wu H K, Liu W & Gerla M, Routing in clustered multi-hop mobile networks with fading channel, in Proc of IEEE SICON, 1997
5. Johnson D B & Maltz D A, Dynamic source routing in ad hoc networks, Mobile Computing, 153-181.
6. Hu B & Gharavi H, DSR-based directional routing protocol for ad hoc networks, in Proc IEEE GlobeComm, 2008.
7. Chakeres I D et Al, AODV routing protocol implementation design, in Proc WWAN, March 2005.
8. Ueda T et Al, ACR: An adaptive communication aware routing through maximally zone-disjoint shortest paths in ad hoc wireless networks with directional antenna, J Wireless Commun & Mobile Comput, 2007.
9. Su W & Gerla M, IPv6 flow handoff in ad hoc wireless networks using mobility prediction, in Proc IEEE GlobeCommun, 1997, 271-275.
10. Toh C K, Associativity-based routing for ad hoc networks using mobility prediction, in IEEE Int Phoenix Conf on Computers and Communications (IPCCC'96)
11. Singh S, Woo M & Raghavendra C S, Power aware routing in mobile ad hoc networks, in Proc Mobicom 1998 (Dallas, Texas) October 1998.
12. Toh C K,Maximum battery life routing to support ubiquitous mobile computing in wireless ad hoc networks, IEEE Commun Mag, June 2001.
13. Tarique M, Tepe K E & Naserian M, Energy saving dynamic source routing for ad hoc wireless networks, in Proc WIOPT 2005.
14. Kaabneh K et al, An effective location-based power conservation scheme for mobile ad hoc networks, Amer J Appl Sci, 6 ( ) 1708-1713.
15. Nitnaware D & Verma A, Energy constraint node cache based routing protocol for ad hoc networks, Int J Wireless & Mobile Networks, 2 (2010).
16. M. Bandai et. al. Signal strength based energy efficient routing for ad hoc networks. In IEICE Transactions on Communications, volume E 91.B, pages 1006–1014, June 2010.
17. Mehdi Lotfi et. al. A new energy efficient routing algorithm based on a new cost function in wireless ad hoc networks. Journal of Computing, 2, June 2010.
18. P.K. Suri et. al. Qos enable power-aware routing protocol for manets. International Journal of Engineering, Science and Technology, 2:4880–4885, 2010.
19. S.K. Dhurandher et. al. Eeaodr: An energy-efficient ad hoc on-demand routing protocol for mobile ad hoc networks. International Journal of Communication Systems, 22(7), July 2009.
20. Z. J. Haas and M. R. Pearlman. The performance of query control schemes for the zone routing protocol. In In Proceedings of SIGCOMM, volume I, page 167177, Jan 1998.
21. Luo Junhai, Xue Liu, and Ye Danxia. Research on multicast routing protocols for mobile ad-hoc networks. In Elsevier,, 2007.
22. Kaabneh, Halasa K., and H A., Al-Bahadili. An effective location-based power conservation scheme for mobile ad hoc networks. American Journal of applied Sciences, B:1708–1713, 2008.

23. J. Widmer M. Mauve. A survey on position-based routing in mobile ad hoc networks. In IEEE Network Magazine, volume 15, pages 30–39, Nov 2001.
24. N. Meghanathan. Energy consumption analysis of the stable path and minimum hop path routing strategies for mobile ad hoc networks. In International Journal of Computer Science and Network Security, volume 7, pages 30–39, October 2007.
25. A. Misra and S. Banerjee. Mrpc: Maximizing network lifetime for reliable routing in wireless environments. In Proceedings of WCNC, 2002.
26. N. Nikaein and C. Bonnet. Alm adaptive location management model incorporating fuzzy logic for mobile ad hoc networks. In in Proceeding of Med Hoc Net, Italy, pages 1489–1499, 2002.
27. K.Srinivasa Rao, R.Sudhistna Kumar, P. Venkatesh, R.V.Sivaram Naidu, and A.Ramesh. Development of energy efficient and reliable congestion control protocol for multicasting in mobile adhoc networks compare with aodv based on receivers. In International Journal of Engineering Research and Applications (IJERA, volume 2, pages 631– 634, Mar-Apr 2012.
28. Anuradha Banerjee, Paramartha Dutta, Reputation-based Attack Resistant Cooperation Stimulation (RACS) for Mobile Ad Hoc Networks, International Journal of Artificial Intelligence and Applications, vol. 1 no. 3, 2010
29. Anuradha Banerjee, Paramartha Dutta, Fuzzy Controlled Route Discovery For Mobile Ad Hoc Networks, vol. 2 no. 6, International Journal of Engineering, Science and Technology, June 2010, pp. 2337-2346
30. Anuradha Banerjee, Paramartha Dutta, Fuzzy Controlled Adaptive and Intelligent Route (FAIR) Selection in Mobile Ad Hoc Networks, European Journal of Scientific Research (impact factor: 0.736), vol. 45 no. 3, September 2010
31. Anuradha Banerjee, Paramartha Dutta, Fuzzy Controlled Localized Route-Repair (FLRR) for On-demand Routing Protocols in Ad Hoc Networks, International Journal of Computer Applications, vol. 7 no. 6, pp. 1169-1444, September 2010
32. Anuradha Banerjee, Paramartha Dutta, Link Stability and Node Energy Conscious Local Route-Repair Scheme for Mobile Ad Hoc Networks, American Journal of Applied Sciences (Impact factor: 0.223) , vol. 7(8), pp. 1129-1138, 2010
33. Anuradha Banerjee, Paramartha Dutta, A Survey of Unicast Routing Protocols in Ad Hoc Networks, International Journal of Advances in Science and Technology, vol. 1 no. 3, 2010
34. Anuradha Banerjee, A Survey of Broadcast Routing Protocols in Mobile Ad Hoc Networks, International Journal of Advances in Science and Technology, vol. 1 no.2, 2010
35. Anuradha Banerjee, Paramartha Dutta, A Survey of Multicast Routing Protocols For Ad Hoc Networks, International Journal of Engineering, Science and Technology, vol. 2 no. 10, October 2010,pp.5594-5604
36. Anuradha Banerjee, Paramartha Dutta, An Efficient Method For Tracking Nodes (EMTN) In Mobile Ad Hoc Networks, International Journal of Computer Applications, vol. 11 no. 2, December 2010,pp.38-41
37. Anuradha Banerjee, Subhankar Ghosh, Paramartha Dutta, Fuzzy-controlled Energy Efficient Weight-based Two Hop Clustering For Multicast Communication in Mobile Ad Hoc Networks, Fuzzy and Neural Computing Conference, Vishakhapatnam, Dec. 19-21, 2011
38. Anuradha Banerjee, Paramartha Dutta, Fuzzy-controlled Multi-hop Adaptive Clustering (FMAC) For Mobile Ad Hoc Networks, Scientific Research and Essays vol.7 no. 2(impact factor: 0.445), 2012
39. Anuradha Banerjee, Paramartha Dutta, Fuzzy-controlled Load-balanced Broadcasting (FLB) In Clustered Mobile Ad Hoc Networks, International Journal of Computer Science Issues (IJCSI - impact factor: 0.242), vol. 9, no. 1, January 2012
40. Paramartha Dutta, Anuradha Banerjee, Fuzzy –controlled Power-aware Multicast Routing (FPMR) For Mobile Ad Hoc Networks, Procedia Technology (Elsevier), vol. 4, pp-38-49, 2012
41. Anuradha Banerjee, Fuzzy-controlled Intelligent Multicast Routing (FIMR) Protocol For Mobile Ad Hoc Networks, Advanced Science Letters (impact factor: 1.253) vol.19 no. 1, pp.42-47, 2013
42. Anuradha Banerjee, Subhankar Ghosh, Paramartha Dutta, Experience Based Energy efficient Reactive Routing Protocol (EXERP) for Mobile Ad-hoc Networks, Arabian Journal of Science and Engineering (Springer), vol. 39 no. 2, 2013
43. Anuradha Banerjee, Paramartha Dutta, Alternative Node Based Energy Depletion and Expected Residual Lifetime Balancing Method For Mobile Ad Hoc Networks, International Journal of Advanced Networking and Applications, vol. 5 no. 2, pp. 1886-1892, 2014
44. Anuradha Banerjee, Paramartha Dutta, Delay-efficient, Energy and Velocity-conscious Non-preemptive Scheduler for Mobile Ad Hoc Networks, International Journal of Advanced Networking and Applications, vol. 5 no. 4, pp. 2002-2010, 2014
45. Anuradha Banerjee, Cost Effective Route Discovery (CERD) For Mobile Ad Hoc Networks, International Journal of Advance Research in Science and Engineering, Vol. 04, Issue 01, march 2015
46. Anuradha Banerjee, FESA: Fuzzy-controlled Energy-efficient Selective Allocation and Reallocation of Tasks Among mobile Robots, International Journal of Advance Research in Science and Engineering, Vol. 04, Issue 01, march 2015
47. Anuradha Banerjee, Fuzzy-controlled Rebroadcasting Based on 2-hop Downlink Neighborhood Information (FR-2N) In Mobile Ad hoc Networks, International Journal of Applied Engineering Research (Scopus), vol. 10 no. 81, pp. 114-120 2015

48. Anuradha Banerjee, Paramartha Dutta, Cost-Effective routing Protocols Based on 2-hop Neighborhood Information (2NI) in Mobile Ad Hoc Networks, International Journal of Applied Networking and Applications, vol. 7 issue 3, pp. 2771-2778, 2015
49. Anuradha Banerjee, Paramartha Dutta Abu Sufian: "Fuzzy Controlled Scheduling on Real Time Data Packet (FSRP) in Mobile Ad-hoc Network", International Journal of Computer Science and Mobile Computing, Vol. 5, Issue. 5, pg- 507-5013, May-2016
50. A. Sufian, A. Banerjee, P. Dutta, "Survey of Various Real time and Non Real time Scheduling algorithms in Mobile Ad-hoc Networks" International Conference on Industry Interactive Innovations in Science, Engineering and Technology (I3SET-2K16), Proceedings published in Springer series of Lecture Notes in Networks and Systems (LNNS)
51. Abu Sufian, Anuradha Banerjee and Paramartha Dutta: "Fuzzy-controlled Scheduling of Route-Request Packets (FSRR) in Mobile Ad Hoc Networks", Indian Journal of Science and Technology, Vol 9(43), DOI: 10.17485/ijst/2016/v9i43/104384, November 2016
52. Anuradha Banerjee, Paramartha Dutta and Abu Sufian: "Fuzzy Route Switching for Energy Preservation (FEP) in Ad Hoc Networks", Indian Journal of Science and Technology, Vol 9(43), DOI: 10.17485/ijst/2016/v9i43/104383, November 2016.

53. Anuradha Banerjee, Paramartha Dutta and Abu Sufian: "EMR-PL: Energy-efficient multipath routing based on link life prediction in ad hoc networks", Journal of Information and optimization Science (Taylor and Francis), vol. 39, issue 1, 2018
54. Anuradha Banerjee, Shirshadipta Chowdhury, "Expected Residual lifetime based Ad Hoc On-demand Multipath Routing Protocol (ERL-AOMDV) In Mobile Ad Hoc Networks", accepted for publication in International Journal of Information Technology (Springer), 2018
55. Anuradha Banerjee, D.M. Akbar Hussain, SD-EAR: Energy Aware Routing in Software Defined Networks, Applied Sciences (SCI Indexed, Impact factor: 1.627), Vol 8(7), 2018
56. Anuradha Banerjee, Paramartha Dutta, Abu Sufian, Movement Guided Management of Topology (MGMT) With Balanced Load In Mobile Ad Hoc Networks, accepted for publication in International Journal of Information Technology (Springer), 2018
57. Anuradha Banerjee, Paramartha Dutta, Abu Sufian, Fuzzy Controlled Energy Efficient Single Hop Clustering Scheme (FESC) In Mobile Ad Hoc Networks, accepted for publication in International Journal of Information Technology (Springer), 2018
58. Anuradha Banerjee, D.M. Akbar Hussain, "Experience Based Efficient Scheduling Algorithm (EXES) For Serving Requests in Cloud Using SDN Controller", Accepted in Journal of Intelligent and Fuzzy Systems (SCI Indexed, Impact Factor: 1.412), IOS Press, Netherlands, 2018
59. Sufian, A., Banerjee, A. & Dutta, P. "Energy and Velocity Based Tree Multicast Routing in Mobile Ad-Hoc Networks"Wireless Pers Commun (Springer, Impact Factor : 1.612) (2019). https://doi.org/10.1007/s11277-019-06378-y
60. A. Banerjee, A. Sufian, Smart-Green-Mult (SGM): overhear from topological kingpins in software defined wireless sensor networks, Journal of Ambient Intelligence and Humanized Computing (SCI indexed, impact factor: 4.594), May 2020.
61. Muhammad Alyas, Shahid, Aisha Azeem, "Disseminating Traffic Information in Vehicular Networks ",International Journal of Advanced Networking and Applications (IJANA), ISSN: 0975-0290, EISSN: 0975-0282.
62. Mussarat Yasmin, Muhammad Sharif, Muhammad Alyas Shahid, "Content Based Image Retrieval Based on Color: A Survey ",International Journal of Advanced Networking and Applications (IJANA), ISSN: 0975-0290, EISSN: 0975-0282.