Wireless Personal Communications (2021) 119:21–35
https://doi.org/10.1007/s11277-021-08092-0

Optimised with Secure Approach in Detecting and Isolation of Malicious Nodes in MANET

R. Thiagarajan[1] · R. Ganesan[2] · V. Anbarasu[2] · M. Baskar[2] · K. Arthi[2] · J. Ramkumar[2]

Accepted: 10 January 2021 / Published online: 24 January 2021
© Springer Science+Business Media, LLC, part of Springer Nature 2021

Abstract
To keep the process of routing and data transmission operations, it is needed for a proper layer of security to keep it safe from malicious attacks. So in this paper, we proposed a framework that helps in detecting the malicious nodes at each of the destinations. After the detection process, it is isolated and discarded in while path establishment through various techniques. The development of an algorithm that supports Multipath Reliable Routing helps in determining paths for a set of disjoint nodes. Based on the index of reliability the paths are reordered. Now the process of information in form of data are been dispersed from source to destination. The main primary path is set to transfer the information. The final destination in case of mismatch of information transferred from a source when received at destination then feedback is given in negative manner stating that there is a mismatch of data along with the information related to the transmission and its path. Hence due to this, the destination will be able to recover since the information is checked each time for reliability. The final results show that the proposed approach results and have a greater impact when compared to the existing methods. Further, it reduces delay in packet transmission and overhead parameter increases the delivery of packets.

RETRACTED ARTICLE

✉ M. Baskar
baashkarcse@gmail.com

R. Thiagarajan
rthiyagarajanpt@gmail.com

R. Ganesan
rganesan1978@gmail.com

V. Anbarasu
anbarasukv@gmail.com

K. Arthi
arthimanivasakam@gmail.com

J. Ramkumar
ram.kumar537@gmail.com

[1] Department of Computer Science and Engineering, Prathyusha Engineering College, Chennai, Tamil Nadu, India

[2] Department of Computer Science and Engineering, School of Computing, College of Engineering and Technology, SRM Institute of Science and Technology, Kattankulathur, Chengalpattu, Chennai, Tamil Nadu 603 203, India

Keywords Disjoint path · Malicious nodes · Detection · Multipath

1 Introduction

A portable specially appointed organization (MANET) is a temporary foundation less multi-jump remote organization wherein the hubs can move haphazardly. With multihop bundle sending, the restricted remote transmission scope of every hub has been stretched out by such organizations. Subsequently, they become viable for situations wherein preconveyed foundations uphold isn't accessible. Along with random data say example source point or portable exchanging focuses that are available in an impromptu organization. Versatile hubs that are present within a range of other available nodes able to convey within that range whereas other sets of nodes present far off can transfer information through switches. Successive variations in a group of node organization geography are brought about through hub versatility in a specially appointed organization. The examination activities focusing on the secure process of MANET seems to be still evolving in different dimensions, though the steering parts of MANETs are beforehand surely known. Notwithstanding the issues of customary organizations, MANETs face various new security issues [1]. The malevolent hubs can promptly work without legitimate security, like switches, and keep the organization from conveying the parcels appropriately. For instance, the malignant hubs can pronounce mistaken steering refreshes. In this way mostly it is spread in the organization or drop all the bundles going within that range. In this way safekeeping issues in specially appointed organizations explicitly the assurance of their organization layer tasks from malignant assaults is critical [2].

Various kinds of mischief out of various purposes have been made by the getting out of hand hubs in an impromptu organization. The sorts of rowdiness on the information identified with the work are as per the following:

1.1 Data Dropping

This is the refusal of administration (DoS) assault. In this assault, the childish or malevolent transitional hubs decrease to advance information bundles for different hubs in the organization. In this paper, two unfavorable conditions are reviewed. They speak to the sorts of information dropping misconduct shaped by individuals and collaborating getting rowdy hubs separately.

1.2 Modification of Data

In process of data diffusion, the vindictive hubs adjust, got information bundles. A noxious hub is expected to frame the information adjusting bad conduct autonomously along the information transmission way.

On disseminated PC frameworks, there are various notable assaults. These incorporate Refusal of Service: An organization's administration isn't accessible because of over-burden or glitch. Data burglary: Information is perused by an unapproved occasion. Interruption: Access to some limited assistance is picked up by an unapproved individual. Altering: Data is changed by an unapproved individual. As an answer to these sorts of assaults, an organization layer security arrangement has been given in impromptu organizations. Here researchers focus on building up a secure structure that is proposed. A Multipath Reliable

RETRACTED ARTICLE

Routing (MRR) calculation, which decides a lot of hub disjoint dependable ways. The ways are organized in the sliding request of their unwavering quality list. Information bundles are scattered and communicated at the same time through the disjoint numerous ways. The information bundle is sent through the fundamental reliable way. At the target, if there is a puzzle between the transmission information and the data groups got, negative information is sent back to the source which contains the nuances of the impacted ways. The source at present discards the impacted ways from the once-over of a center point disjoint ways. Since the data packs are dissipated along different ways using an incredible dispersing count, the goal can recover the data viably [3, 4]. This security structure incorporates 1. Acknowledgment of malignant center points by the goal center. 2. Restriction of malicious center points by discarding the way. 3. Shirking data allocates using dissipating techniques. The ways are arranged in the slipping solicitation of their resolute quality document. Data packs are dissipated and conveyed at the same time through the disjoint various ways. The information group is sent through the fundamental strong way. At the goal, if there is confound between the transmission information and the data packs got, a negative analysis is sent back to the source which contains the nuances of the affected ways. The source as of now discards the affected ways from the once-over of center point disjoint ways. Since the data packs are dispersed along various ways using a practical dissipating count, the goal can recover the data adequately.

2 Literature Survey

An interruption discovery in remote organizations has been proposed [5, 6]. The interruption location network has been centered principally on wired organizations. A relationship between the probability of identifying an interruption and the measure of hubs that must partake during the time spent recognizing interruptions is examined further. Exercises in organizations are watched with contrasted and known assaults through different techniques. Then again, new unidentified dangers can't be distinguished in this methodology. This is the primary impediment of this methodology. Given AODV over IPv6, usage of a safe directing convention has been proposed [7] and a steering convention free Intrusion Detection and Response framework for specially appointed organizations fortifies this further. Nonetheless, the directing assaults just mainly chatted in the procedures introduced in this paper. In MANETs, a generous disposition is normal from all the hubs present in the organization. But these kindhearted hubs, there may exist vindictive hubs. Consequently, directing is a genuine shortcoming if a portion of the hubs is working vindictively. Creator in papers [8] and [9] proposed an answer to recognize malignant hubs in MANETs. Also, some security conventions [10] allude to public keys that give an assortment of security administrations. These administrations are over the top expensive by utilizing cryptographic natives, for example, hash-based message verification code, advanced marks, and hash chains. For MANETs with formal thinking and reenactment tests for assessment, in [11] proposed a flat-out appropriated interruption recognition framework that incorporates four models. Anyway, this too speaks just the directing assaults, not the others. The discovery stage has been engaged and offered another instrument used to recognize narrow-minded hubs in MANET.

After this [12], clarified issue of secure steering convention and it is inferred that current secure directing conventions like SEAD, ARAN, SAODV can just ensure against outer assaults. Along these lines, this is as yet a difficult assignment for inner assaults. In [13]

RETRACTED ARTICLE

introduced two methodologies known as guard dog and pathrater. Guard dog recognizes malignant hubs and pathrater encourages directing conventions to evade these novel ways. Be that as it may, the recommended approach was not reasonable if there should arise an occurrence of a crash. Creator [4] proposed another technique, where they alluded to two messages known as additional solicitation (FREQ) message and further answer (FREP) message to check the legitimacy of the hub. This was not an ideal arrangement because the arrangement accepts that the malevolent hubs don't exist in gatherings. Additionally in [8] have broadened this methodology [13], by proposing an answer for hubs impact. In [14], a danger model has classified hub type as (I) fizzled; (ii) gravely fizzled; (iii) childish hub and (iv) vindictive hub. In light of this arrangement, bombed hubs and egotistical hubs don't play out all activities, while narrow-minded hub additionally preserves energy for its future use, and gravely bombed hub performs flawed and mistaken tasks. Thus, the exhibition of the whole organization corrupts steadily.

Bundle Conservation Monitoring Algorithm is the most recent identification instrument. The issue of bundle sending assaults just has tended through the component which does not focus on upcoming dangers. A protected information communication convention, the safe single-way (SSP) convention is introduced in [4]. A course revelation convention is put forth by researchers in [15]. This Secure Link State Routing Protocol [16, 17] provides secure geography disclosure which multiplies favorable to the organization activity. Mischievous activities can't be identified in this technique, while unwavering quality is accomplished. To animate collaboration among portable hubs with singular securities, a credit-based Secure Incentive Protocol evolves in [3]. The skill of SIP has been perceived through careful reproduction considers. The issue of parcel sending assaults has been tended to in this, not different dangers. To see steering misconduct and to reduce their negative impact, the 2ACK plan that fills in as an extra strategy for directing plans has been suggested [18]. Sending two-bounce affirmation parcels the opposing way of the steering way is the significant idea of the 2ACK plan. Regardless of whether if mischief, alternate affirmation parcels are transferred. These outcomes in trivial overhead. To relieve unfavorable impacts that are trouble-making, a Multipath Routing Single way transmission plot has been put forth which is further enhanced in [19]. With a continuous criticism system it blends multipath steering and single way information transmission. In any case, the data bundles are refused from accomplishing the objective by a course disappointment or connection disappointment. Moreover, the objective may not be skilled to identify the rowdiness, if a childish hub doesn't advance the data parcel or changes the substance of the data bundle. A Mobile Intrusion Detection System for multilevel transmission is made in [13, 20]. This identifies hubs' bad conduct and anomalies during transmission of packets, to be precise, moderate level of stations reducing or postponing packets. Further to the above review we likewise observe that in [21, 22] analysts have presented a particular hub known as gatekeeper hub. This plan depends on a trust computation measure in which if the hub has a trust level lower than a pre-characterized limit, at that point, it is recognized as malevolent. Also, this specific hub won't be considered for course choice. In [23, 24], they presented another protected force mindful subterranean insect province calculation for recognition of bargained and pernicious hubs in MANETs.

RETRACTED ARTICLE

3 Methodology

This plan keeps a record of all hubs present in the organization. Energy utilization is limited by changing the transmission scope of every hub and keeps on sorting out the pernicious hub dependent on trust level and complete information rate. The conduct of hubs is arranged into three sorts: (I) customary hubs; (ii) dubious hubs and (iii) vindictive hubs. Because of this arrangement, it is accepted that at first, all hubs are normal and polite. A hub is dubious by considering two cases, for example, (I) on the off chance that it is moving out of transmission range after course disclosure system and (ii) if correspondence breakage happens during information transmission and grouping number of rebroadcasting RREQ isn't equivalent to a similar RREQ which as of now exists in the steering table. In this circumstance, we break down the idea of recognized dubious hubs by contributing their certainty esteem (lies somewhere in the range of 0 and 1) and hub limit. On the off chance that the expository outcomes don't give great outcomes to certainty worth and hub limit then a dubious hub will be set apart as a vindictive hub. The limit of a hub relies upon the level of parcels sent by that hub.

3.1 Analysis of Data Misbehavior

Various sorts of bad conduct for various purposes have been made by the making trouble hubs in a specially appointed organization. The kinds of bad conduct on the information identified with the work are examined here. Information Dropping—This is the refusal of administration (DoS) assault. In this assault, the egotistical or noxious moderate hubs decrease to advance information parcels for different hubs in the organization. In this paper, two antagonistic conditions are assessed. They speak to the sorts of information dropping mischief framed by individual and coordinating acting mischievously hubs separately. Information Modifying—During their transmission, the malignant hubs change the got information parcels. One vindictive hub is expected to frame the information changing rowdiness autonomously alongside the information transmission way. While the plans in [8, 25] can effectively recognize such bad conduct, can't distinguish such sort of mischief.

3.1.1 Case 1: How to Deal if a Node is Moving Out of Transmission Range

At the point when course disclosure methodology is started, at that point source hub thinks about the current courses for an objective. Attributable to the dynamic nature, all hubs are moving. It is accepted that every hub can communicate or get information inside a most extreme sweep R, however, the two activities can't happen all the while. Additionally, energy power is introduced to every hub. Let us characterize a hub that has N normal number of neighbors. At that point, N demonstrates network availability. Also, hubs of an organization are consistently appropriated as 2D Poisson point measure with thickness l. In this way, the likelihood of discovering I hubs in territory A, where I is a progression of number. This zone shows the situation of hubs inside the reach R, that is, the position of B regarding A. Estimation of r depends on the greatest and least estimations of r ′.

3.1.2 Case 2: Identification of Malicious Nodes

It has been expected that all the hubs are reliable and dynamic. These hubs are known as ordinary hubs. Such normal hubs can be imagined as dubious depending on two cases: (I) if the

RETRACTED ARTICLE

hub is moving out of reach and besides (ii) if the execution of the hub is diminishing steadily. Case (I) issue can be effectively amended and defeated. Presently, further work manages the optional case (ii). We use the flooding idea for the change of grouping numbers in RREQ. At the point when a moderate hub gets RREQ parcels having the most recent data, that point steering table is adjusted and RREQ bundles are communicated to its neighbors. Also, the hub disposes of copy parcels. If the succession number is unique, at that point it is considered as an irregular movement. Likewise, we break down the idea of distinguished dubious hubs by ascertaining their certainty esteem (lies somewhere in the range of 0 and 1) and hub limit.

Algorithm for detecting malicious nodes

Input: Total number of nodes, with its corresponding range value and suspect value, malicious node number

Output: Normal node number, malicious node number

Parameters: n – Number of nodes, PI- Packet Information, RI- Reliability Index, ACK- Acknowledgement, PD- Packet delivery ratio, k- path, R_n- Reliable path of n disjoint nodes, PT- Path table

For (k=1; k<n; k++) //creating paths for the given node

Calculate the distance and nodes are placed

Key generated and packet transferred with source and destination ID

Security Association ($SA_{s, d}$) - Packet information

Each node

If ($R_k > R_h$):

Put k in list – define k as malicious node //Identification of malicious node

Else if:

Destination packets verified with source information

Source id, timeout value t mapped

Identify and list normal nodes and infected noes

End

RETRACTED ARTICLE

4 Implementation

4.1 Setting Up the Path

Our steering convention MRR utilizes a Multiway Set containing hub disjoint ways, chosen utilizing the AOMDV convention. A MPS of hub disjoint ways is worked by utilizing progressively ascertaining the hub disjoint, most brief in the scope of bounces, ways, utilizing the network availability measurements gave the guide of the course disclosure. The number of ways RMR needs to work depends on the convention's setup goal, which might be the convention chosen boundary. Inspite of advanced availability records gotten, RMR tries for choosing novel ways generally both initiation and responsively, following the conjuring of a course revelation. Alternately, to maintain a strategic distance from rehashed summons at what time no more ways might be found, way revelations craving to decorate the MPS should be rate-limited. Inevitably, we know that setting the way choice on a source from where data initiated exhibits that realities are directed and usefulness which is clear to blend in along loose steering conventions.

Regarding dependability, RI mirrors the distinction of the path. This can be applied to pick the dynamic ways inside the following transmission and how they will be stacked. Predictable with the presentation of the course regarding bundle dispatching proportion, R1 is estimated at the objective as

$$RI_k = P * V$$

where the above term stands for reliability index and packet delivery ratio for the path chosen which is denoted by k.

4.2 Process of Detecting Malicious Nodes

Our plan handles bad conduct overutilization of two novel kinds of rheostat parcels, named PI and NACK. A parcel, that is needed in stagger on bad conduct, is dispatched gracefully into excursion spot through a source of information transfer. A NACK parcel, moderate horrible outcomes, are dispatched from get-away spot to the initiation point when speculated misconduct close by information transmission course is recognized. A PI bundle comprises of realities of the relating transmission: (a) records period records along with data time costs, realities parcel size, and anticipated records amount; (b) information transmission heading records, alongside the way length and hubs along the course. A PI parcel likewise can convey a haphazardly produced key to verify the realities bundles of the comparing transmission clump. A NACK bundle joins a ready node that helps in identifying and data of bearing, for example, extents of ways and hubs ways.

Inside the proposed structure, the flexibly gets the main trustworthy course Rl from the MPS sooner than conveying data parcels. Out of the n disjoint solid ways (Rn) from the MPS, realities parcels are scattered and sent through m dependable ways (Rm). To help the objective showcase the general exhibition of scattered courses Rm utilized for insights transmission, a PI bundle is sent through Rl legitimate after the information parcels have been shipped off Rm. The PI bundle incorporates the data of this transmission (Figs. 1, 2).

RETRACTED ARTICLE

Source ID (Waiting for Confirmation)	Time out Value	R1 (Route 1) R2 (Route 2)	Data Information

Fig. 1 Waiting list table

Fig. 2 Confirmed list of malicious node

Source ID (Confirmed)	R1 (Route 1) R2 (Route 2)	Data Information

4.3 Removal of Detecting Malicious Nodes

After accepting a NACK bundle, the source disposes of the relating ways from its MPS and way store. On the off chance that it has information that is supposed to be transmitted, the flexibly tests MPS for the accompanying k trustworthy hub split ways (Rk) and propels scattered realities bundles and PI, holding novel techniques for communication. IT flexibly starts a course demand system that either of none hub disjoint ways to be inside the MPS. The objective wipes out the relating things from the work area while it gets RREQ from the initiation point which gives info for a table while it gets bundles encompassing innovative realities. If new transmission realities are gotten after the past data of the gracefully has been appeared, the get-away spot refreshes the relating thing from the PT. The objective disposes of the relating objects that are PT when it gets another RREQ from a source.

5 Results and Discussion

The general presentation of the proposed strategy is assessed in this section. We examine the proposed technique for malignant hub recognition in MANETs and assess it with the predominant directing convention AODV in MANET the utilization of reproductions. We have mimicked our belongings with the utilization of ns2.3. The possibility that we have embraced for reproduction is all hubs are moving progressively. Likewise, the course and speed of hubs are mulled over. Portability situation is produced by the method of utilizing an irregular way factor model with 600 hubs in a position of 800 m × 800 m for 50 s reenactment time. The recreation boundaries are referred to under. We expect each hub activities freely with the indistinguishable regular speed. All hubs have a similar transmission scope of 260 m. In this portability form, a hub haphazardly chooses an excursion spot from the physical landscape. It developments inside the way of the get-away spot in a movement consistently picked amid the insignificant speediness with utmost movement. Subsequently, it arrives at an objective, hub remains here for a delay period then afterward developments again. Our recreation makes that, base speed is five m/s and the highest rapidity is 10 m/s. Reproduced guests are normal Bit value. We range no. of acting up hubs to be 5, 10, 15, and 20 (Table 1).

RETRACTED ARTICLE

Table 1 Simulation parameters and settings

No. of nodes	600 nodes
Area size	800 × 800
MAC	IEEE 802.11
Initial energy	100
Speed	5/10/15/20 m/s
Transmission threshold power	0.27991
Packet size	512
Range of transmission	260 m
Radio range	260 m
CS range	550 m
Simulation time	50 s
Traffic source	CBR
Misbehaving nodes	Randomly allotted
Tx power	0.18
Rx power	0.04

RETRACTED ARTICLE

5.1 Metrics performance

5.1.1 Control Overhead

This denotes the total amount of information transmitted to the total amount of data received (Figs. 3, 4).

5.1.2 Average End-to-End Delay

This is calculated by taking in the average of the total amount of information transferred in packets from source to destination (Fig. 5).

5.1.3 Average Packet Delivery Ratio

This exhibits the percentage of packets received at destination successfully to the number of packets transmitted in total (Fig. 6).

We set transmission assortment 250 m by changing transmission energy Pt_ and CS range 550 m individually. We adjust the transmission energy of the hub in the threshold. cc for a case if the scope of the hub surpasses. We lease parcel size for 512 bytes, and power benefited

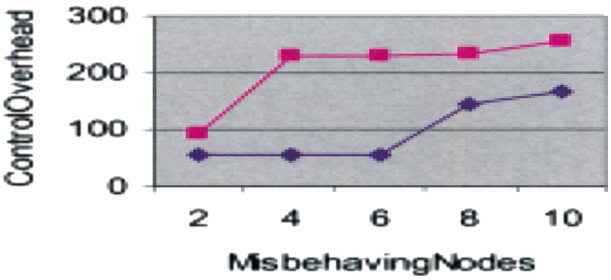


Fig. 3 Overhead of misbehaving nodes

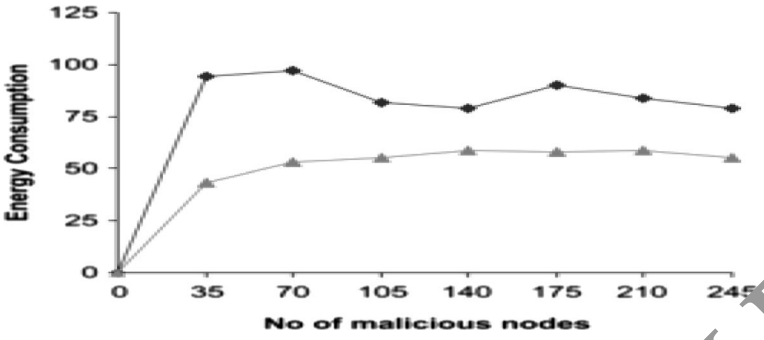
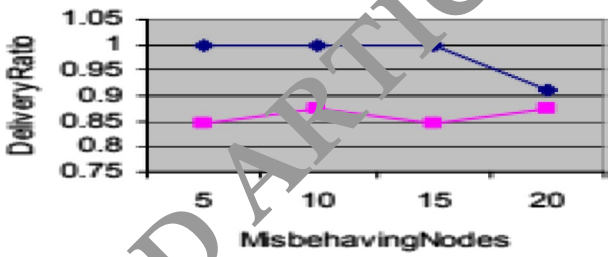


Fig. 4 Energy consumption of nodes

Fig. 5 Ratio of delivery of misbehaving nodes



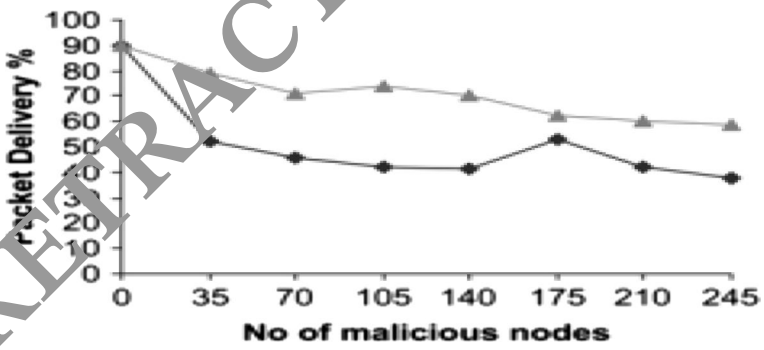


Fig. 6 Packet delivery ratio

RETRACTED ARTICLE

from in sending and accepting a bundle is zero.0173 and zero.05, separately. The recreation runs for 500 s. In the whole situation, noxious hub advances parcels and doesn't prevail due to overhead and hyperlink breakage. also, noxious hub publicizes counterfeit messages and imagines that these are reasonable hubs and passes on unimportant data roughly legitimate and productive hubs. This bogus impression debases network execution. We put our endeavor on pernicious hubs moves (Fig. 7).

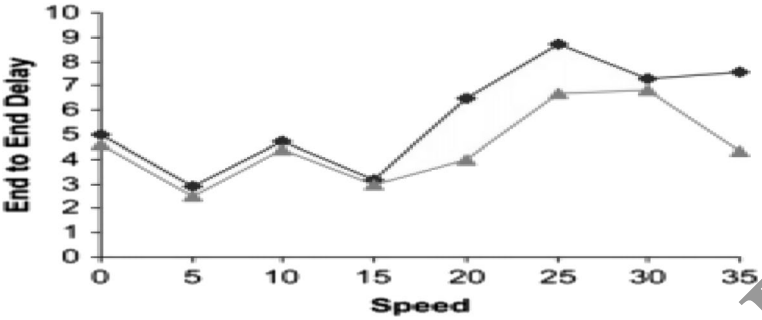


Fig. 7 End to end delay

6 Conclusion

Researchers focus here to bring up a novel contraption that fuses: Malicious node detects process center points through methods for goal center point separation of noxious center points by methods for disposing of the way, and evasion data packages by using dissipating procedures. Our solid and comfortable Framework contains a dependable Multipath Routing count that settles on choice an assortment center split consistent methodologies. Ways which planned diving solicitation with an enduring superb record. Test records packages are dispersed and sent the entirety of the even as through the trustworthy disjoint techniques. The records bundle containing the transmission insights is dispatched utilizing a significantly reliable way. On the goal if there is a mix among the transmission data and the data groups were given, an awful complaint is transferred back to the point which started initiation that incorporates the nuances of the incited strategies. The flexibly presently remove incited ways with a once-over of center point disjoint methodologies. Since the information packs are dispersed close by several techniques utilizing an amazing dissipating computation, the goal can get well the information solidly, thereby utilizing completing constancy. Our reenactment impacts recommend that, while differentiated and present arrangement, our gadget diminishes overhead and deferral, simultaneously extending the package transport extent.

Funding Not applicable.

Availability of Data and Material Not applicable.

Compliance with Ethical Standards

Conflict of interest We authors not having any conflict of interest among ourselves to submit and publish our articles in Wireless Personal Communications journal.

Code Availability Not Applicable.

RETRACTED ARTICLE

References

1. Farooq, A., Dhanant, S., & Saswati, S. (2003). Signature based intrusion detection for wireless ad-hoc networks: A comparative study of various routing protocols. In *Vehicular Technology Conference, 2003. VTC 2003-Fall. 2003 IEEE 58th*.
2. Anand, P., Jim, P., Anupam, J., Michaela, I., & Tom, K. (2005). Secure routing and intrusion detection in ad hoc networks. In *Pervasive Computing and Communications, 2005. PerCom 2005. Third IEEE International Conference on March 2005*.
3. Madhavi, S., & Tai, H. K. (2008). An intrusion detection system in mobile adhoc networks. *International Journal of Security and its Applications, 2*(3), 2008.
4. Papadimitratos, P., & Haas, Z. J. (2002). Secure routing for mobile ad hoc networks. In *Proceedings of SCS CNDS, San Antonio, TX*, Jan. 27–31, 2002, pp. 193–204.
5. Li, Z. & Delgado-Frias, J. G. (2007). MARS: Misbehavior detection in ad hoc networks. In *Global Telecommunications Conference, 2007. GLOBECOM'07*. IEEE Publication Date: 26–30 Nov. 2007.
6. Yanchao, Z., Wenjing, L., Wei, L., & Yuguang, F. (2007). A secure incentive protocol for mobile ad hoc networks. *Wireless Networks (WINET), 13*(5), 2007.
7. Marti, S., Giuli, T. J., Lai, K., & Baker, M. (2000). *Mitigating routing misbehavior in mobile ad hoc networks*. MobiCom: Proc.
8. Chin-Yang, H. T. (2006). Distributed intrusion detection models for mobile ad hoc networks. University of California at Davis Davis, CA, USA, 2006.
9. Tarag, F., & Robert, A. (2006). A node misbehaviour detection mechanism for mobile ad-hoc networks. In *The 7th Annual PostGraduate Symposium on The Convergence of Telecommunications, Networking and Broadcasting*, 26–27 June 2006.
10. Lou, W., Liu, W., & Fang, Y. (2004). SPREAD: enhancing data confidentiality in mobile ad hoc networks. In *IEEE INFOCOM 2004*, pp. 2404–2413.
11. Patwardhan, A., Parker, J., Iorga, M., Joshi, A., Karygiannis, T., & Yesha, Y. (2008). Threshold based intrusion detection in adhoc networks and secure AODV. Elsevier Science Publishers B. V., Ad Hoc Networks Journal (ADHOCNET), June 2008.
12. Arulananth, T. S., Baskar, M., Udhaya, K. S. M., Thiagarajan, R., Arul Dalton, G., & Suresh, A. (2021). Evaluation of low power consumption network on chip routing architecture. *Journal of Microprocessors and Microsystems*. https://doi.org/10.1016/j.micpro.2020.103809.
13. Arulananth, T. S., Balaji, L., Baskar, M., et al. (2020). PCA based dimensional data reduction and segmentation for DICOM images. *Neural Processing Letter*. https://doi.org/10.1007/s11063-020-10391-9.
14. Baskar, M., Ramkumar, J., Rishk, R., & Raghav, K. (2020). A deep learning based approach for automatic detection of bike riders without helmet and number plate recognition. *International Journal of Advanced Science and Technology, 29*(4), 1844–1854.
15. Ernesto, J. C. (2006). Vulnerabilities of intrusion detection systems in mobile ad-hoc networks—The routing problem 2006.
16. Baskar, M., Renuka Devi, R., Ramkumar, J., et al. (2021). Region centric minutiae propagation measure orientation recovery detection with finger print analysis in health care systems. *Neural Processing Letter*. https://doi.org/10.1007/s11063-020-10407-4.
17. Ramkumar, J., Baskar, M., Viswak, M., & Ashish, M. D. (2020). Smart shopping with integrated secure system based on IoT. *International Journal of Advanced Science and Technology, 29*(5), 306–312.
18. Baskar, M., Gnanasekaran, T., & Saravanan, S. (2013). Adaptive IP traceback mechanism for detecting low rate DDoS attacks. 2013 IEEE International Conference ON Emerging Trends in Computing, Communication and Nanotechnology (ICECCN). *Tirunelveli, 2013,* 373–377. https://doi.org/10.1109/ICE-CCN.2013.6528526.
19. Baskar, M., Ramkumar, J., Karthikeyan, C., et al. (2021). Low rate DDoS mitigation using real-time multi threshold traffic monitoring system. *Journal of Ambient Intelligence and Humanized Computing*. https://doi.org/10.1007/s12652-020-02744-y.
20. Suchithra, M., Baskar, M., Ramkumar, J., Kalyanasundaram, P., & Amutha, B. (2020). Invariant packet feature with network conditions for efficient low rate attack detection in multimedia networks for improved QoS. *Journal of Ambient Intelligence and Humanized Computing*. https://doi.org/10.1007/s12652-020-02056-1.
21. Paul, K., & Westhoff, D. (2002). *Context aware detection of selfish nodes in dsr based ad-hoc networks*. GlobeCom: Proc.
22. Jothikumar, R., Kumar, T. R., Jayalakshmi, P., Baskar, M., Thiagarajan, R., & Mohan, I. (2020). Enhanced resemblance measures for integration in image-rich information networks. *JCR, 7*(16), 106–111. https://doi.org/10.31838/jcr.07.16.14.

RETRACTED ARTICLE

23. Balakrishnan, K., Deng, J., & Varshney, P. K. (2005). TWOACK: preventing selfish in mobile ad hoc networks. In *Proceedings of WCNC'05*, 2005.
24. Madhumitha, R., Ilango, K., Vimal, S., & Suresh, A. (2020). Analysis of obstructive sleep apnea disorder with accuracy prediction using SVM for smart environment. *ACM Transactions on Multimedia Computing, Communications, and Applications*. https://doi.org/10.1145/3382782.
25. Panagiotis, P., & Zygmunt, J. H. (2006). Secure data communication in mobile ad hoc networks. *IEEE Journal on Selected Areas in Communications, 24*(2), 2006.

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

RETRACTED ARTICLE

Dr. R. Thiagarajan is working as an Assistant Professor in Department of Computer Science and Engineering, Prathyusha Engineering College. He received his Ph.D. degree under the Faculty of Information and Communication Engineering in Anna University, Chennai, India, in 2020. He pursued his Bachelor degree from Anna University and Master's in Computer Science and Engineering from Dr.M.G.R University, Chennai. His research interests include Wireless Adhoc Networks, Network Security, Machine Learning and Deep Learning Techniques. He is a Life time Professional body member of CSI, ISTE.

Dr. K. Ganesan completed his Bachelor degree in Information Technology from VelTech Engineering College, Chennai (Affiliated to Madras University, Chennai) in 2002. He has completed his Master degree in Information Technology from Sathyabama University, Chennai in 2009. He has completed his Ph.D. degree in Faculty of Information and Communication Engineering from Anna University, Chennai in 2020. Currently he is working asAssistant Professor in Department of Computer Science and Engineering (School of Computing), SRMIST, Kattankulathur(Since August 2020). He has published more than forty technical papers and his main areas of interest include Machine Learning, HealthCare System, Mobile Computing and Pervasive Computing.

Dr. V. Anbarasu received his B.E from SVNIT, Surat, Gujarat in Computer Engineering and M.Tech in IT and PhD in CSE from Sathyabama University, Chennai in 2006 and 2014 respectively. Presently he is working as Associate Professor in the Department of Computer Science and Engineering, School of Computing, SRM Institute of Science and Technology. He is having 17 years of work experience in Engineering Colleges around India. He has Published 2 Patent and Grant 1 Patent. He has published 12 National & International Journals and 31 Conference publications, attended various workshops, seminars and delivered lectures in workshops during his career. Also acting as a Guest Faculty in BITS, Pilani and taken various offline/online courses like OOPs, Advanced Programming Techniques, Operating System, OOAD, Software Architecture, Computer Graphics, Cryptography etc for WILP with WIPRO. His area of interest includes Human Computer Interaction, IoT, Machine Learning, Algorithms, Cryptography and Security.

Dr. M. Baskar is a Researcher cum Faculty in Department of Computer Science and Engineering, School of Computing, Kattankulathur Campus, SRM Institute of Science and Technology. He received B.E. Computer Science and Engineering from Anna University, Chennai, M.Tech. Information Technology from Sathyabama University, Chennai and Ph.D.(Information and Communication Engineering) from Anna University, Chennai. His Area of research interest includes Computer Networks and Security, Parallel and Distributed Systems, Image Processing, Big Data, Machine Learning and IoT. He has published 39 Research Article in reputed International Journals and 13 Article in International Conferences. He has published 5 patents. He is acting as a reviewer in Cluster Computing, Journal of Web Engineering, Multimedia Tools and Applications, Neural Processing Letters and Concurrency and Computation: Practice and Experience. He is a Life time Professional body member of ACM,CSI, ISTE, IET, ISRD, IRED, IACSIT, IAENG, SDIWC and UACEE.

Dr. K. Karthi is affiliated to Department of Computer Science and Engineering, School of Computing, Kattankulathur Campus, SRM Institute of Science and Technology. She has received her Master's and Ph.D.(Information and Communication Engineering) from College of Engineering, Anna University, Chennai. Her current research interests are in Wireless Sensor Network and Security, Image Processing, Big Data, Machine Learning, Deep Learning and IoT. She has published 25 Research Article in reputed International Journals.

RETRACTED ARTICLE

Dr. J. Ramkumar is working as an Assistant Professor in Department of Computer Science and Engineering, School of Computing, Kattankulathur Campus, SRM Institute of Science and Technology. He received his Ph.D. degree under the Faculty of Information and Communication Engineering in NGNLab, Department of Computer Technology, Anna University, Chennai, India, in 2018. He pursued his Bachelor and Master's in Computer Science and Engineering from Anna University, Chennai. His research interests include Broadband Wireless Networks, Resource allocation in 5G networks, C-RAN and Network Security especially in Blockchain.

RETRACTED ARTICLE