The Ciência & Engenharia - Science & Engineering Journal
ISSN: 0103-944X
Volume 11 Issue 1, 2023
pp: 1892-1901

Review of Counter-Based Digester ACK's Effectiveness in MANET Packet Loss Prevention

Afsha Nishat [1], Dr. Mohd Abdul Bari [2], Dr. Guddi Singh [3]
[1] Research Scholar, Kaling University, Raipur.
afsha7390@gmail.com
[2] Associate Professor, HOD Computer Science Department ISL College of Engineering, Hyd, Telangana, India. Abdulbarimohammed11@gmail.com,
[3] Associate Professor, Computer Science Department, Kalinga University, Raipur. ,
singh@kalingauniversity.ac.in

Abstract: a wireless peer-to-peer network with a mobile component adaptability and self-formation characteristics that lacks infrastructure. The network is ideal for use in emergency and disaster assistance applications that need reliable communication.. Finding the channel between communicative entities and sending information across it enables communication. There are several routing protocols in the literature that are developed to achieve reliable communication. Routing protocols are susceptible to packet losses because they consider network nodes to be receptive to communication. Due to malicious behavior or a shortage of resources, nodes trash packets. To address the problem, a number of intrusion detection systems have been suggested in the literature. In order to prevent packet losses in MANET, the newly created counter-based digested Acknowledgement (CDACK) was developed. This study's objective is to assess the CDACK protocol's performance in relation to current MANET intrusion detection systems. The findings demonstrate that, in terms of avoiding packet dropping nodes from the routing path, the CDACK protocol is a good fit for MANET..

Keywords: resource, MANET, intrusion detection, Packet drop

1 Introduction

A mobile ad hoc network, or MANET, is a wireless network that is dispersed, peer to peer, and distributed. The network's design objective is to provide constant and universal access to the internet. The network's properties include adaptability, autonomy, and self-formation. Because of these features, the MANET is used in applications that are important and sensitive, such as military operations and disaster relief. Because a single faulty message disrupts the MANET's design goal, these applications need dependable communication.

Communication in any networking context is achieved by locating the route and transmitting data along that way [7,8]. Various routing techniques created in the literature to determine the route then deliver the data along the predicted route in the form of packets between the communication nodes. The majority of MANET routing protocols choose a route on the premise that network nodes are amenable to routing operations This assumption is not accurate with regard to MANET; for two reasons, nodes do not enable routing activities.: malicious conduct and a lack of resources, and nodes discard packets [6]. Packet drops caused Intrusion is the term used to describe hostile network layer actions [8,9,21].

The literature has developed a variety of intrusion detection techniques for MANET to stop packet dropping nodes from interacting. Security systems known as intrusion detection systems (IDSs) try to stop system security violations by detecting unusual network activity. The IDS detects anomalous network activity by continually monitoring the network. Some preventative actions include notifying the problem and issuing direct commands, such as preventing the shady relationships. A technique for seeing and reacting to malicious behavior on networking and computer resources is the intrusion detection system (IDS). The second line of defense is often used to describe an intrusion detection system since it reacts after an intrusion has already taken place. Because MANET lacks concentration sites for monitoring and evaluating data gathering performance, intrusion detection is significantly more complex and fascinating than in infrastructure-based networks. One of the fallacies about the routing protocol is that in order to send and receive data, nodes in a MANET must work together. This impression allows the attacker to utilize compromised nodes to have a large impact on the network [2].

The three main categories of MANET IDS now in use are credit-based, reputation-based, and acknowledgement-based approaches [4–5]. The credit-based technique [15] uses credits as an incentive mechanism to identify network nodes that are doing inappropriately. Conversely, nodes with lesser credits are unable to communicate with nodes with higher credits. Credits are given to nodes by the central payment system in return for dependable packet operations. However, the idea is inappropriate for MANET because of the centralized payment system.

Another method for mitigating rogue packet drooping nodes from the communication line in MANET is to monitor the method [13,22]. The network requires that each node examine all of its neighbors for packet activity. In their reputation-based approach, Thachil et al. [16] suggested that nodes in a system of communication keep tabs on the status values of their neighbors through a process known as promiscuous routing. The number of lost packets is divided to get the reputation value. by the number of forwarded packets and comparing it to a preset threshold value. When the calculated reputation cost is less than the threshold value, the technique considers the node to be malevolent. Recognized harmful nodes are notified to all other nodes in the network. This method is heavily reliant on the monitoring module and node process [10]. End-to-end acknowledgement between communication entities is a different technique for avoiding malicious packet drooping [11]. In response to packet reception, destination or intermediary nodes send ACK packets to the originating node. By sending two-ACK acknowledgments for each packet, it identifies malicious nodes [9]]. Upon receiving packets from the node that initiated the communication, It is necessary for each node along the route to send an ACK packet to the nodes that are two hops away. down the route. A neighbor node is considered to be malicious if a two-ACK packet sent from it does not arrive at the source node within a predetermined amount of time.

The article [6] included a recommendation the acronym "IDS" stands for "intrusion Detection System." known as EAACK, which had a variety of innovative defenses against attacker assaults. The system is equipped with functionalities like the regulation of strong strikes and the automated activation of the priority to essential nodes. In addition to this, he added that the Watchdog has a total of six vulnerabilities, three of which are being handled by the system at the present time, and the remaining three may be handled at a point in the not-too-distant future.

The MANET is an environment in which an acknowledgement-based solution works exceptionally well. environments since it does not need a central coordinating system and does not necessitate the installation of extra hardware. Furthermore, the strategy outperforms the reputation-based approach in terms of the amount of memory used and the compute cost.

In the works that were stated above, several aspects were taken into consideration to eliminate the nodes from the network that dropped packets; nevertheless, these aspects not determine whether node that dropped a packet was dishonest or trustworthy. A MANET is an example of an unstructured network that is comprised of several mobile nodes. When moving data from its origin to its destination through a network, it is inevitable that certain nodes, known as loyal nodes, would throw away data packets due to a lack of available resources. If an IDS If harmful packet drooping nodes are identified, then all packet drooping nodes are identified as malicious. because they drop packets maliciously or because they report dropping packets. This condition inhibits reputable nodes from participating in communication, which has a detrimental influence on system performance. When a reputable node receives more packets than it can handle in terms of buffer and energy, it dumps them. If the number of packets arriving in the input queue exceeds the node's buffer capacity, the packets are dropped. Due to insufficient energy and transmission power, subsequent nodes also discard packets [12,23]. In this case, the node is not drooping packets on purpose or maliciously.

Recently, CDACK [1] has been developed, with the purpose of improving the ACK-based technique by avoiding packets from dropping from the communication line due to inadequate resources or malicious activity. The residual state of intermediary nodes in terms of energy and buffer prevents packet drops owing to inadequate resources. By utilizing digested acknowledgement, it is possible to eliminate packet drops that are induced by hostile nodes.

The purpose is this research, is demonstrate a significance in taking into account reputable packet drooping nodes while constructing MANET intrusion detection systems. As a result, the study examines how well existing intrusion detection systems function when there are reported nodes in the network that are dropping packets. The performance of the network was analyzed with the help of the simulator. This article presents a complete performance analysis of the existing intrusion detection system, focusing on how different network behaviors affect packet delivery and communication throughput. Despite the fact that academics have put in a significant amount of effort to calculate the performance analysis of IDS using a large number of performance metrics, the results are still not satisfactory. In the study that has been proposed, the performance of the IDS will be evaluated in relation to the presence of nodes that have been reported to drop packets. This is a fresh perspective on the work overall. that we are doing.

2 CDACK

Despite the fact that the ACK-based method is the one most suited for MANET, it is unable to detect packets. failures caused by inadequate resources. Secure knowledge method [3] prevents packet losses owing to limited resources. However, although the secure knowledge technique may detect Because it has insufficient resources, it is unable for the purpose of preventing nodes that are dropping packets from leaving the communication route.. Recent research by CDACK [1] has been developed, with the purpose of improving the ACK-based technique by avoiding packets from dropping from the communication line due to inadequate resources or malicious activity. The residual state of intermediary nodes in terms of energy and buffer prevents packet drops owing to inadequate resources. Packet drops caused by utilizing digested acknowledgement, it is possible to avoid malicious nodes. The CDACK is an advancement on the ACK-based technique that was previously used., and its contributions include the following:

1. Identifying nodes with suitable residual buffer and energy status.
2. Communication entity session key agreement
3. Using to communicate between different communication entities, counter-based digested ACK is used.

The following is a detailed summary of CDACK's contribution:

1. Identifying nodes with suitable residual buffer and energy status.

A lack of resources, such as energy and buffer space, is one of the key factors that contributes to the loss of packets by MANET nodes. On a communication connection where the nodes do not have sufficient resources, they are unable to manage the load and so lose packets. As a result, the objective of CDACK is used to choose communication nodes based on their level of sufficiency. buffer and energy resource capacities. As a consequence of this, the following work was done to estimate the buffer and energy residual condition of the node:
In order to determine the typical length of the queue at the node buffer, the RED [19,24] gateway makes use of equation (1).

$$Av.Queue = (\alpha) * \text{Instant Queue} + (1-\alpha)Av.OldQueue \dots\dots\dots\dots\dots\dots.(1)$$

Where is the waiting constant and its value ranges from 0 to 1. If a node's calculated Since the node's average queue size is lower than the capacity at which it can process requests, is evaluated in communication the node's buffer handling capacity is calculated as 75% of the buffer size. Equation (2) determines the amount of power that Each node must in order to be able to in order to process packets.
Equation (2) calculates the packet control capabilities of a node in relation to its residual energy.

$$Packet\ handling\ Enery = \ E - E(packet)/(E_r + E_r + E_r) \dots\dots(2)$$

Where E is residual energy, E(packet) is the amount of energy that the node expends as a result of the packet processing, while Er, Ep, and Et are the amounts of energy that are necessary to first receive the packet, then to process it, and finally to send it,respectively. If a node's calculated packet handling energy exceeds its handling capabilities, the node is evaluated for communication. The node that meets the threshold criteria of equations (1) and (2) is chosen for the routing operation.

2. Communication entity session key agreement

As a consequence of the property referred to as the "Chaotic Maps Based Diffie Hellman problem [14,15]," it is possible for the source and the destination to come to an agreement over

an authenticated key. Ordered Maps a technique for implementing the key arrangement of communicative elements, is based on Chebyshev-Polynomials (Chaos theory) [17], and it is concerned with the behavior of dynamical systems. The following is a definition of the Chebyshev-Polynomial:
cos(n) might expressed $\cos(\theta)$polynomial, as seen in equation 3.

$$\cos(n\theta) = T_n * \cos(\theta) \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (3)$$

$$\cos\big((n+1)*\theta\big) = 2*\cos(n\theta)*\cos(\theta) - \cos\big((n-1)*\theta\big)$$

$$T_{n+1}\cos(\theta) = 2*T_n\cos(\theta)*\cos(\theta) - T_{n-1}\cos(\theta)$$

$$T_{n+1}(x) = 2*x*T_n(x) - T_{n-1}(x) \qquad \ldots\ldots\ (4)$$

According to Polynomial in 'X' degree is represented by Equation 4, which represents the Chebyshev polynomial in $T_n(x)$. 'n.' To accomplish authentication [18,25], the semigroup property of Chebyshev polynomials may be used, as shown in equation 5.

$$T_n(x) = 2*x*T_{n-1}(x) - T_{n-2}(x) \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (\,5), n \geq 2$$

Authentication between source and destination is accomplished using equation 6, which is a semigroup property [1].

$$T_n(x) = 2\,x*T_{n-1}(x) - T_{n-2}(x)*(\text{mod } N) \qquad \ldots\ldots\ldots\ldots(6), \quad n \geq 2$$

It is exceedingly difficult to estimate the value of 'n' in equation (6) when N is a very large prime number and X is in the range (- ∞, +∞). This aspect of the equation is referred to as the chaotic maps based discrete logarithmic issue. When N is a very large prime number and X is in the range (- ∞, +∞).it occurs. The characteristic referred to as "Chaotic Maps Based" Diffie Hellman Problem" asserts that it is impossible to calculate the value of $T_{nm}(X)$' in a given equation (7) with the provided values of $T_n(x)$, X, N and $T_m(X)$.

$$T_m(T_n(X)) \;=\; T_n(T_m(X)) = T_{mn}(X)*(\text{mod } N) \ldots\ldots\ldots\ldots\ldots(7), n \geq 2$$

Using counter-based digested ACK to communicate between communication entities

Counter-based ACK prevents the detection and prevention of nodes that maliciously drop packets. It transmits the ACK for packet receipt after a predetermined amount of time has passed, as opposed to communicating the ACK to be sent back to the source for each data packet or two data packets that have been received by the destination.

3 Performance Analysis

This study's objective is to explore how well the CDACK method works and assess how well it stacks up against other intrusion detection systems (IDS), including techniques such as SKA and ACK, which were created to protect MANET nodes from losing packets. this work, investigated a MANET that has malevolent packet drooping nodes, reputable nodes that drop packets, and reputable packet dropping nodes. The nodes can be found in a variety of locations around the radio communication zone. Through the use of many intermediate nodes, the data packets are transferred from the source node to the destination node. A technique for detecting intrusions has been built into the network so that packet-dropping nodes will not be able to access the communication path. IDS, on the other hand, are not able to identify rogue or renowned packet drooping nodes. During the process of intrusion detection and prevention, reputed nodes are penalized due to the limited resources available, and they are required to demonstrate the usefulness of separating hostile packet dropping nodes from reputable packet dropping nodes. If this is not avoided, the performance of the network in terms of packet delivery would suffer. As a result, we simulate the performance of the existing MANET (IDS) while well-known nodes that drop packets are present.

We utilize the NS-2.34 simulator. so that we may evaluate performance. The simulation scenario investigates a network of peers in order setting with several hops and 150 mobile nodes that are represented in a 1500 by 1500 square unit radio communication region. Each node possesses a buffer that can store data packets and energy that can be used to send data packets received from other nodes. The study employs modern intrusion detection techniques such as the ACK, SKA, and CDACK. protocols, in situations where it is believed that packet dropping nodes are present. Table 1 presents the simulation's settings and controls. The percentage of delivered packets, the throughput, and the percentage of lost packets are all. the performance assessment measures. Figures 1, 2, and 3 show the simulation findings.

Table-1: Simulation Parameters

Network-Parameters	Values
Area of Network	1200m x 1 000m
Nodes	150
Communication.	Two-Ray-Ground
Network layer	ACK & SKA
Link Layer	Logical Link
Mobility	Random
Simulation-Time	1000 s
Traffic	CBR
Queue	Drop-Tail
MAC	802.11
Energy	100j

The findings make it abundantly evident that the existence in the transmission of reported packet dropping nodes channel contributes to a decline in the performance of the network. This is because the legitimate node, which has limited resources, is forced to take on the role of the malicious node. It has been decided that the node will not be allowed to take part in the conversation. As a direct consequence of this, the network's performance in terms of delivery of packets is negatively affected.

The performance of the IDS is depicted in Figure 1 in terms of the percentage of packets sent by the IDS vs the various data speeds that are present when both respectable and malevolent packet dropping nodes are present. Within the context of our simulation, the data rate is increased by expanding the number of source-destination combinations. Each data rate sees its performance put to the test. According to the findings, the CDACK is superior to both the ACK and the secure knowledge algorithms in terms of performance.

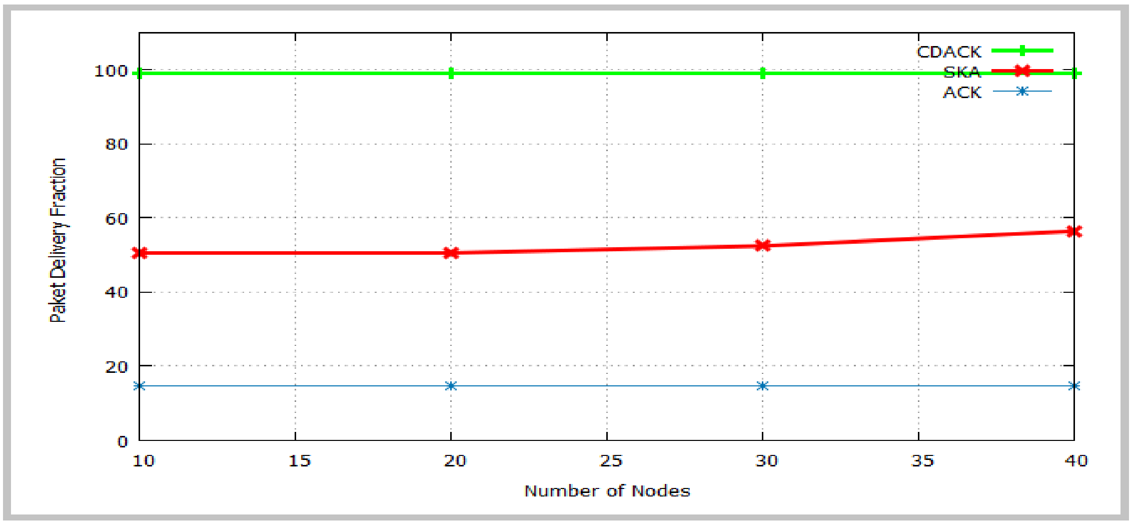

Figure 1: Performance of MANET's IDS degrades in the presence of limited and sabotage through the dropping of packets nodes in the PDF

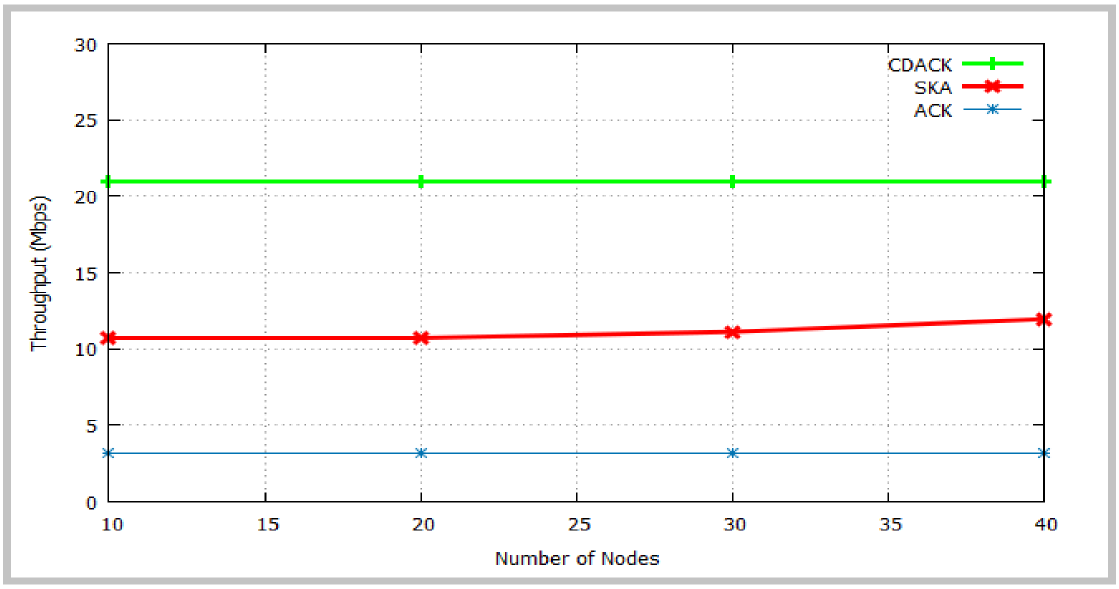

Figure 2: Degradation of MANET's Throughput Performance of IDS in the presence of limited and sabotage through the dropping of packets nodes

Figure 2 depicts the IDS's performance in terms of throughput in comparison to to various data rates while there are both trustworthy the nodes that drop packets and malicious the nodes that drop packets present. Within the context of our simulation, By increasing the number of source-destination pairings, the data rate is boosted.. Each data rate sees its performance put to the test. According to the findings, the CDACK is superior to both the ACK and the secure knowledge algorithms in terms of performance. The performance of the packet loss is shown in Figure 3. in the same way. The results clearly show that CDACK improves packet delivery and minimizes packet loss, and that it is ideally suited for MANET environments.

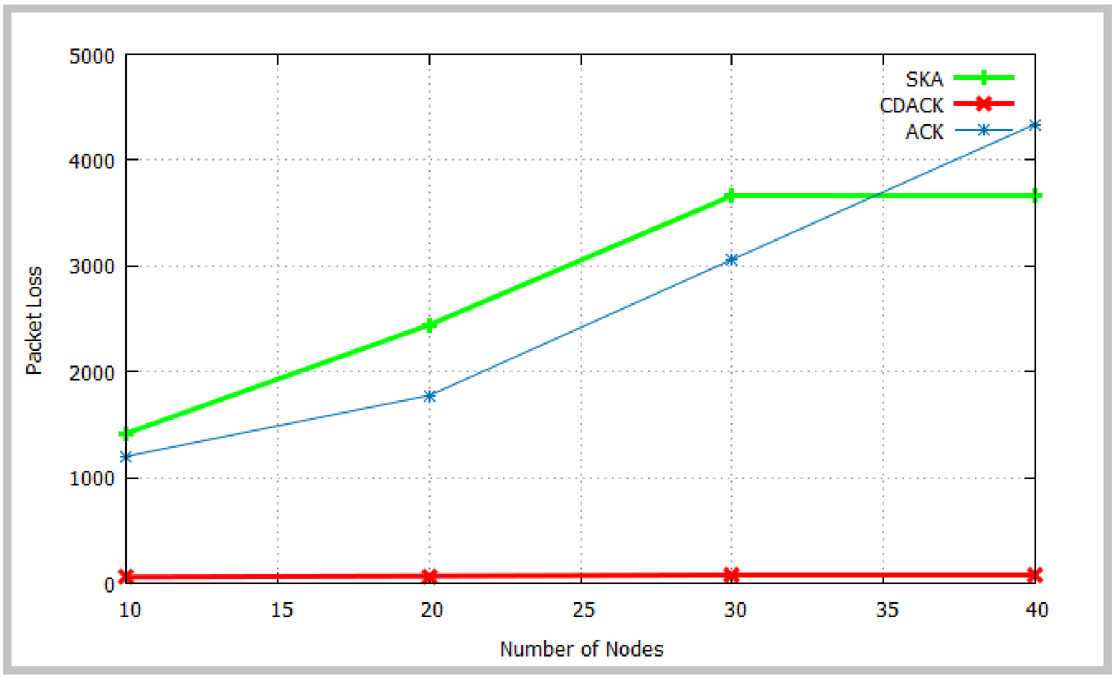

Figure 3-: Degradation of MANET's packet loss performance and IDS in the presence of limited and sabotage through the dropping of packets

4 Conclusion

Ad hoc networks that operate on the fly are a type of via peer-to- wireless network that lacks infrastructure but has adaptability and the ability to construct itself on its own. The network is ideally suited for use in applications that require dependable communication, such as those that are used in disaster relief and emergency situations. Because these protocols are based on the assumption that nodes in a network facilitate communication, they can experience packet loss as a result of this presumption. Sometimes packets are discarded by nodes because of malicious behavior or because there are not enough resources to process them. The CADCK protocol's primary objective is to eradicate packet dropping nodes, which can occur as a result of both in malevolent behavior and insufficient resources. In this study, the performance of the CDACK protocol is analyzed, and it is compared to other existing intrusion detection systems that are designed for MANET. The findings make it abundantly evident that CDACK enhances packet delivery, reduces the amount of packets that are lost, and is ideally suited for use in MANET systems.

References

[1] Hussain, Mohammed Ali, and Balaganesh Duraisamy. "Preventing Malicious Packet Drops in MANETs by Counter Based Authenticated Acknowledgement Preventing Malicious Packet Drops in MANETs by Counter Based Authenticated Acknowledgement."May 2020 Ingénierie des systèmes d information 25(2):173-181

[2] Mohammad, A.A.K., Mahmood, A.M., Vemuru, S. (2019). Intentional and unintentional misbehaving node detection and prevention in the mobile ad hoc network. International Journal of Hybrid Intelligence, 1(2-3): 239- 267. https://doi.org/10.1504/IJHI.2019.103580

[3] Siddiqua, A., Sridevi, K., Mohammed, A.A.K. (2015). Preventing black hole attacks in MANETs using secure knowledge algorithm. 2015 International Conference on Signal Processing and Communication Engineering Systems,

[4] Meitei, Moirangthem Goldie, and Biswaraj Sen. "A study on few approaches to counter security breaches in MANETs." Advances in Communication, Cloud, and Big Data. Springer, Singapore, 2019. 105-116.

[5] Kumbhkar, M., Shukla, P., Singh, Y., Sangia, R. A., & Dhabliya, D. (2023). Dimensional Reduction Method based on Big Data Techniques for Large Scale Data. 2023 IEEE International Conference on Integrated Circuits and Communication Systems (ICICACS), 1–7. IEEE.

[6] Marathe, Nilesh, and Subhash K. Shinde. "ITCA, an IDS and trust solution collaborated with ACK based approach to mitigate network layer attack on MANET routing." Wireless Personal Communications 107.1 (2019): 393-416.

[7] Schweitzer, Nadav, et al. "Detecting bottlenecks on-the-fly in olsr based manets." 2014 IEEE 28th Convention of Electrical & Electronics Engineers in Israel (IEEEI). IEEE, 2014.

[8] De Rango, Floriano, et al. "A new distributed application and network layer protocol for voip in mobile ad hoc networks." IEEE Transactions on Mobile Computing 13.10 (2014): 2185-2198.

[9] Kim, Dongkyun, et al. "Power-aware routing based on the energy drain rate for mobile ad hoc networks." Proceedings. Eleventh International Conference on Computer Communications and Networks. IEEE, 2002.

[10] Shakshuki, Elhadi M., Nan Kang, and Tarek R. Sheltami. "EAACK—a secure intrusion-detection system for MANETs." IEEE transactions on industrial electronics 60.3 (2012): 1089-1098.

[11] Pareek, M., Gupta, S., Lanke, G. R., & Dhabliya, D. (2023). Anamoly Detection in Very Large Scale System using Big Data. SK Gupta, GR Lanke, M Pareek, M Mittal, D Dhabliya, T Venkatesh,.." Anamoly Detection in Very Large Scale System Using Big Data. 2022 International Conference on Knowledge Engineering and Communication Systems (ICKES).

[12] Nadeem, Adnan, and Michael P. Howarth. "A survey of MANET intrusion detection & prevention approaches for network layer attacks." IEEE communications surveys & tutorials 15.4 (2013): 2027-2045.

[13] Liu, Kejun, et al. "An acknowledgment-based approach for the detection of routing misbehavior in MANETs." IEEE transactions on mobile computing 6.5 (2007): 536-550.

[14] Banerjee, Sukla. "Detection/removal of cooperative black and gray hole attack in mobile ad-hoc networks." proceedings of the world congress on engineering and computer science. 2008.

[15] Abbas, Sohail, Madjid Merabti, and David Llewellyn-Jones. "A survey of reputation based schemes for MANET." The 11th Annual Conference on the Convergence of Telecommunications, Networking & Broadcasting (PGNet 2010), Liverpool, UK. 2010.

[16] Kshirsagar, P. R., Reddy, D. H., Dhingra, M., Dhabliya, D., & Gupta, A. (2023). A Scalable Platform to Collect, Store, Visualize and Analyze Big Data in Real-Time. 2023 3rd International Conference on Innovative Practices in Technology and Management (ICIPTM), 1–6. IEEE.

[17] Mohammad, Arshad Ahmad Khan, Ali Mirza, and Srikanth Vemuru. "Cluster based mutual authenticated key agreement based on chaotic maps for mobile ad hoc networks." *Indian Journal of Science and Technology* 9 (2016): 26.

[18] Mohammad, Arshad Ahmad Khan, Ali Mirza Mahmood, and Srikanth Vemuru. "Providing Security Towards the MANETs Based on Chaotic Maps and Its Performance." Microelectronics, Electromagnetics and Telecommunications. Springer, Singapore, 2019. 145-152.

[19] Thachil, F., Shet, K.C. (2012). A trust-based approach for AODV protocol to mitigate black hole attack in MANET. 2012 International Conference on Computing Sciences, Phagwara, India. https://doi.org/10.1109/ICCS.2012.7

[20] Mason, John C., and David C. Handscomb. Chebyshev polynomials. CRC Press, 2002.

[21] Zhu, Hongfeng. "Flexible and Password-Authenticated Key Agreement Scheme Based on Chaotic Maps for Multiple Servers to Server Architecture." Wireless Personal Communications 82, no. 3 (2015): 1697-1718.

[22] Floyd, Sally, and Van Jacobson. "Random early detection gateways for congestion avoidance." *IEEE/ACM Transactions on networking* 1, no. 4 (1993): 397-413.

[23] Dhingra, M., Dhabliya, D., Dubey, M. K., Gupta, A., & Reddy, D. H. (2022). A Review on Comparison of Machine Learning Algorithms for Text Classification. 2022 5th International Conference on Contemporary Computing and Informatics (IC3I), 1818–1823. IEEE.

[24] A. A. K. Mohammad, A. K. Lodhi, A. Bari, M. A. Hussain,” *Efficient mobile sink location placement by residual status in WSN to enhance the network lifetime”,* (2021) 4779 – 4790, Journal of Engineering Science and Technology (JESTEC), Volume 16, Issue 6, December 2021, SCI ;Pages 4779 - 4790

[25] Dr. M.A.Bari, ”*EffectiveIDS To Mitigate The Packet Dropping Nodes From Manet* “, JACE, Vol -6,Issue -6,June 2019

[26] M.A.Bari,Sunjay Kalkal, Shahanawaj Ahamad, "Averting Grey Hole Attacks Using Secure Data Protocol in Mobile Ad-Hoc Networks" , International Journal of Advanced Research in Computer Science and Software Engineering ",Vol -7,Issue-6 ,June 2017(ISSN:2277-128X)

[27] M.A.Bari, Sunjay Kalkal, Shahanawaj Ahamad," Sheltered Energy Aware Routing Against Black Hole Attack”, IJRSM, VOL .4, Issue 3-March 2017, ISSN: 2349- 5197 Pages 22-27.(UGC APPROVED JOURNAL) ;

[28] Ijteba Sultana, Mohd Abdul Bari and Sanjay,” *Impact of Intermediate Bottleneck Nodes on the QoS Provision in Wireless Infrastructure less Networks*”, Journal of Physics: Conference Series, Conf. Ser. 1998 012029 , CONSILIO Aug 2021

[29] M.A.Bari, Sunjay Kalkal, Shahanawaj Ahamad," *A Comparative Study and Performance Analysis of Routing Algorithms*”, in 3rd International Conference ICCIDM, Springer - 978-981-10-3874-7_3 Dec (2016)