Review on Packet drop prevention in MANET by counter based digester ACK

Dr. Mohammed Ali Hussain[1,2], Dr. Balaganesh Duraisamy[3]

[1]*Post-Doctoral Fellow, Lincoln University College, Malaysia.*
[2]*Professor, Dept. of Electronics and Computer Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Andhra Pradesh.*
[3]*Professor & Dean, Faculty of Computer Science & Multimedia, Lincoln University College, Malaysia.*

[1,2] alihussain.phd@gmail.com, [3]balaganesh@lincoln.edu.my

Abstract
Mobile ad hoc network is an infrastructure less, constrained resource, and peer to peer wireless network with adaptation and, self-forming capabilities. The network is well suited for deploying in disaster relief and emergency applications, and demands reliable communication. Communication is enable by finding the path between communicating entities and forwarding the information through it. In literature number of routing protocols designed to achieve the reliable communication. Routing protocols vulnerable towards the packet drops due to their consideration such as nodes in a network are supportive for communication. Nodes drop the packets due to either malicious behaviour or insufficient resources. In literature several intrusion detection mechanisms have been designed to address the problem. Recently counter based digested Acknowledgement (CDACK) is designed to prevent the packet drops in MANET. The paper aim is to investigate the performance of the CDACK protocol and compare it with existing intrusion detection mechanisms designed for MANET. Results indicate that the CDACK protocol is well suited for MANET to prevent packet dropping nodes from communication path.

Keywords: *MANETs, Packet drop, malicious, resource, intrusion detection.*

I. INTRODUCTION

Mobile ad hoc network (MANET) is a wireless infrastructure-free, distributed, peer to peer, and distributed network. The design aim of the network is to assist internet access anywhere all the time. The characteristics of the network are adaptation, autonomous and self-forming. These characteristics lead the MANET to deploy in critical and sensitive applications such as disaster relief and military. These applications demands reliable communication, as single unreliable message disturb the design objective of the MANET.

Communication in any networking environment is accomplished by the finding the path and sending information through the found path [7,8]. In literature, various routing mechanisms designed to find the path between communication nodes and then forward the information in the computed path in terms of packets. Majority of routing protocols designed in MANET select the route by belief that nodes in the network are supportive for routing activities. This assumption is not valid in MANET, the nodes do not support for routing activities due to two reasons such as malicious behavior and insufficient resources, and then nodes drop the packets [6]. The packet drop due to malicious activity in network layer are considered as intrusion [8,9].

In literature, many intrusion detection mechanisms have been designed in MANET to prevent the packet dropping nodes from communication. Intrusion detection systems (IDSs) are the security systems that finds unusual activities in a network and tries to prevent such activities which violate the system security [24]. Detection of unusual activities is achieved by continuously monitoring the network by the IDS. Some of the measures of prevention are like alerting the issue and taking direct orders such as blocking the suspected connections. Intrusion Detection System is a procedure of recognizing and answering to malicious activity focused on networking and computing resources. An intrusion detection mechanism is also known as the second line of defense as it comes when an intrusion has already occurred. Intrusion detection in MANET is much composite and challenging than in infrastructure based networks, as MANET lacks the concentration points while monitoring and auditing the performance of the data collection. One of the myths of routing protocol [20] is that nodes in MANET assumes that all nodes coordinate with each other for sending and receiving data. Due to this belief, the attacker gets an opportunity to gain a noteworthy influence on the network with compromised nodes [2]. The existing IDS of MANETs are majorly divided into three types such as credit based approach, reputation based approach [4] and

Acknowledgement-based approach [5]. Credit-based approach [15] is detect the misbehaving nodes in the network by incentive mechanism in terms of credits. Node with higher credits allow to participate in communication and nodes with low credits does not. Central payment system provides the credits to nodes for their reliable packet operations. However, the approach is not suitable for MANET due to central payment system.

Reputation based approach is another way to mitigate malicious packet drooping nodes from communication path in MANET by monitoring process [13]. Each node in the network need to screen the all its neighbor nodes regarding packet operations. Thachil et al.,[16] designed a reputation based Approach, where every node in a communication path keep track of status value of neighbor nodes by promiscuous monitoring. Reputation value calculated by the ratio of number of packets dropped to forwarded, and it compared with predefined threshold value. The approach consider node as malicious when it detects the computed reputation value is lesser than the threshold value. Identified malicious nodes are further informed the all the nodes existing in the network. This approach majorly depends up on the monitoring module and process of the node [10].

Another approach of malicious packet drooping prevention is the end to end acknowledgement between communication entities [11]. Intermediate or destination nodes transmit the ACK packets to originator node regarding the reception of packet. Two-ACK [9], it identifies the malicious nodes by acknowledging every packet. Upon reception of packets form originator node, every node along the route is needed transmit back an ACK packets to the nodes that is two hop away from it down the route. If two-ACK packet did not reach to the source node in a particular time duration then neighbor node reported as malicious node.

The work [6] proposed IDS named EAACK with some sort of novel methods for the prevention of the attacks from the attacker. The features enclosed in the system like controlling powerful attacks and the automatic generation of activating the priority to the key nodes. He also claimed that the Watchdog has a sum of six known weaknesses, out of which three are already handled with the help of the system and the other three may be handled in the future.

Acknowledgement based approach is well suited for MANET environment, as there is no prerequisite of central payment system and need not to fix additional hardware. Further the method is much capable than reputation-based approach, as it has fewer overhead in terms of memory, and computation.

In the above discussed works, different aspects were taken into consideration to stop the packet dropping nodes from network, but they do not recognize the packet dropping node is either malicious or reputed. MANET is an unstructured network with different mobile nodes. During the data communication from source to destination in the network environment, there is a coincidental that the faithful nodes drop the packets due to insufficient resources. If IDS are deciding the packet drooping nodes as malicious nodes then the all the packet drooping nodes become malicious either malicious packet dropping or reputed packet dropping. This situation prevents the reputed nodes to participate in communication, and further negatively impact on system performance. The reputed node drops the packets when it receive the packets more than its handling capability with respect to buffer and energy. If the packet arrival at input queue is more than its buffer capacity, then the packets get automatically drop from the node. Further node also drop the packets due to insufficient energy and transmission power [12]. Here, node is not intentionally and/or maliciously drooping the packets.

Recently CDACK [1] is proposed, and goal of the CDACK is to improve the ACK based mechanism by preventing packets drop from communication path by either insufficient resources or malicious activities. Packets drop due to insufficient resources are prevented by residual status of intermediate nodes regarding energy and buffer. Packet drops due to malicious nodes are prevented by digested acknowledgement.

The aim of the paper is to show the importance of considering reputed packet drooping nodes while developing intrusion detection systems of MANET [23]. Thus the paper investigate the performance of the existing IDS in the presence of the reputed packet dropping nodes in the network. Performance evaluation carried out by network simulator. Paper presents the systematic performance study of the current IDS in terms of packet delivery and communication throughput with respect to various network behavior. Although there is a lot of review work has been carried out by researchers to calculate the performance analysis of IDS with different performance metrics. Our work evaluate the performance of the IDS with respect to the existence of reputed packet dropping nodes. This evaluation process is the novel aspect of our work.

II. CDACK

ACK based approach is a best suitable for MANET, but it fails to detect the packet drop due to insufficient resources. To prevent packet drop due to insufficient resources are prevented by secure knowledge algorithm [3]. However, secure knowledge algorithm able to detect the packet dropping nodes due to insufficient resources but it cannot prevent it from communication path. Recently CDACK [1] is proposed, and goal of the CDACK is to improve the ACK based mechanism by preventing packets drop from communication path by either insufficient resources or malicious activities. Packets drop due to insufficient resources are prevented by residual status of intermediate nodes regarding energy and buffer. Packet drops due to malicious nodes are prevented by digested acknowledgement. The CDACK is an improvement of the ACK based mechanism with the following contributions:

1. Finding the nodes with sufficient residual status of buffer and energy.
2. Session key agreement between communication entities
3. Communicating counter based digested ACK between communication entities

The detail description of CDACK contribution is explained as follows:

A. Finding the nodes with sufficient residual status of buffer and energy

One of the major reasons of packet drop by nodes in MANET is due to insufficient resources such as lack of energy and buffer. The node present in a communication path with insufficient resource cannot handle the traffic and drops the packets. Thus the aim of CDACK is to select the nodes for communication with sufficient resources I terms of buffer and energy. Thus work computed the node's buffer and energy residual status as follows:

The average queue size at node buffer is computed by the RED [19] gateway by equation (1)

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

Where, α is waited constant and it value is varied between 0 to 1. If the computed average queue size of node is less than its handling capability then the node considered for communication. And the handling capability of the node regarding buffer is computed as $75\%\ of\ buffer\ size$.

The sufficient energy to process the packets by node is computed by equation (2)

Packet handling ability of node due to residual energy of the node is computed by the following Equation (2)

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

Where, E is residual energy, $E(packet)$ energy consumed by node due to packet process, and $\boldsymbol{Er}$, $\boldsymbol{Ep}$ and $\boldsymbol{Et}$ are energy required to receive ,process and transmit, the packet respectively. If the computed packet handling energy of node is greater than its handling capability then the node considered for communication. During the routing process [25], the nodes which satisfy the threshold condition of buffer and energy by equations (1) and (2) are only considered communication.

B. Session key agreement between communication entities

An Authenticated key settlement between source and destination is achieved by the property "Chaotic Maps Based Diffie Hellman problem [14,15]. Chaotic Maps, way to implement the key agreement between communicating entities is based on Chebyshev polynomials [17] (Chaos theory), A field of study in mathematics dealing with the behavior of dynamical systems that are highly sensitive to initial conditions. The dynamical system is a system in which a function describes the time dependence of a point in a geometrical space. Chebyshev polynomial is defined as follows:

$\cos(n\theta)$ could be written in the polynomial of $\cos(\theta)$ as in equation 3

$$\cos(n\theta) = T_n * \cos(\theta) \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots (3)$$
$$\cos((n+1)*\theta) = 2 * \cos(n\theta) * \cos(\theta) - \cos((n-1)*\theta)$$
$$T_{n+1}\cos(\theta) = 2 * T_n\cos(\theta) * \cos(\theta) - T_{n-1}\cos(\theta)$$
$$T_{n+1}(x) = 2 * x * T_n(x) - T_{n-1}(x) \qquad \dots\dots\ (4)$$

Equation 4 shows the Chebyshev polynomial in $T_n(x)$ is a polynomial in 'X' degree 'n.' To achieve authentication [18], one can use semigroup property of Chebyshev polynomials as below equation 5

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

Work [18] uses the Chebyshev polynomial's semigroup property [1] to provide authentication between communicating entities, which shown below in equation 6

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

Where N is a big prime number and $X \in (-\infty, +\infty)$, in equation (4.6) it is incredible to compute the value of $'n'$ with the given values of $T_n(x)$, X, N, and this property is known as the chaotic maps-based discrete logarithmic problem.

The property "Chaotic Maps Based Diffie Hellman Problem" states that in a given equation (7) it is incredible to compute the value of $'T_{nm}(X)'$ with the given values of $T_n(x)$, X, N and $T_m(X)$ and this property known as Chaotic Maps-Based Discrete Logarithm problem.

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

C. Communicating counter based digested ACK between communication entities

Detection and prevention of malicious packet dropping nodes are prevented by counter based ACK. Instead of transmitting the ACK to source for receiving the each data packet or two data packets by destination, It transmits the ACK for packet reception after particular time interval.

III. PERFORMANCE ANALYSIS

The aim of the work is to investigate the performance of the CDACK approach and compare it with the existing IDS, such as SKA and ACK mechanisms developed to prevent the packet dropping nodes form MANET. In this paper, we consider a MANET consisting of reputed nodes, malicious packet drooping nodes and reputed packet dropping nodes. The nodes are disseminated in radio communication area. The source node transmits the packets to destination in multi hop communication manner. The network is designed with intrusion detection system, which prevent the packet drooping nodes from communication path. However, IDS are not recognizing packet drooping nodes are malicious or reputed. Therefore reputed nodes [21] are punished because of constrained resources, and need to show the importance of recognizing the malicious and reputed packet dropping nodes during Intrusion detection and prevention. Otherwise it negatively impact on network performance in terms of packet delivery. Thus, through simulation we evaluates the performance current IDS of MANET in the presence of reputed packet dropping nodes.

We use the NS-2.34 simulator to evaluate the performance. The simulation environment considers a multi-hop, peer to peer network environment with 150 mobile nodes represented in a radio communication are of 1500x1500 square units. Each nodes consist of buffer to hold packets and energy to forward the packets of other nodes. The paper runs an existing intrusion detection systems such as SKA and ACK and CDACK protocols in the presence of reputed packet dropping nodes [22][28]. The simulation parameters are shown in Table 1. The performance evaluation metrics are packet delivery fraction, throughput and packet loss. Simulation results are depicted in Figures 1,2 and 3.

Table-1: Simulation Parameters

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

Results are clearly indicating that the presence of the reputed packet dropping nodes in communication path leads to the performance degradation in the network, as legitimate node becomes the malicious node due to its constrained resources. The node lose the chance to participate in the communication. Thus the performance of the network [26] get decreased with respect to packet delivery.

Figure 1shows the performance results of the IDS in terms of packet delivery fraction with respect to different data rates in the presence of reputed packet dropping and malicious packet dropping nodes [27]. In our simulation we increases the data rate by increasing the number of source and destination pairs, Performance is evaluated at each data rates. The result shows that the Performance CDACK is better than the performance of ACK and secure knowledge algorithm.

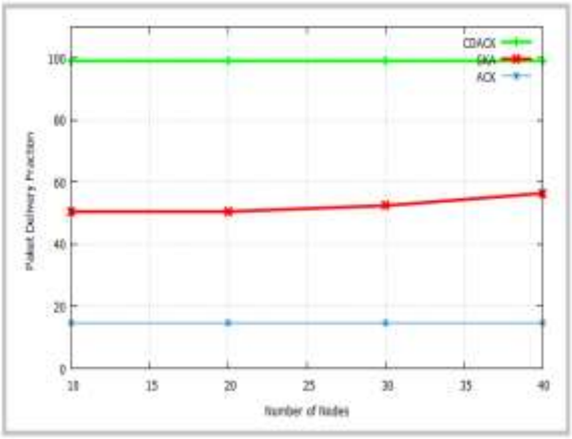

Figure 1-: PDF Performance of IDS degradation of MANET in the presence of constrained and Malicious packet dropping nodes

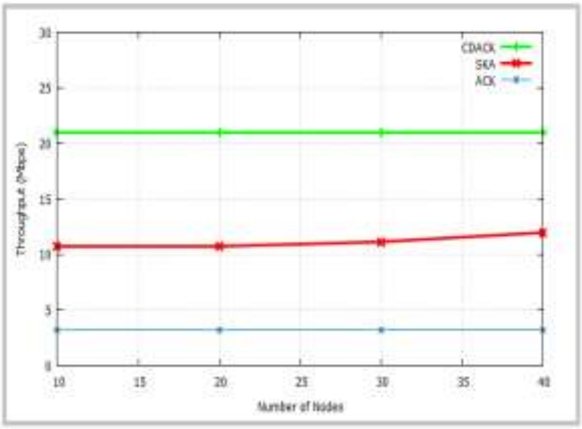

Figure 2-: Throughput Performance of IDS degradation of MANET in the presence of constrained and malicious packet dropping nodes

Figure 2 shows the performance results of the IDS in terms of throughput with respect to different data rates in the presence of reputed packet dropping and malicious packet dropping nodes. In our simulation we increase the data rate by increasing the number of source and destination pairs, Performance is evaluated at each data rates. The result shows that the Performance CDACK is better than the performance of ACK and secure knowledge algorithm. Similarly figure 3showsthe packet loss performance. Results are clearly indicating that the CDACK increases the packet delivery and reduces the packet loss, and well suited for MANET environment.

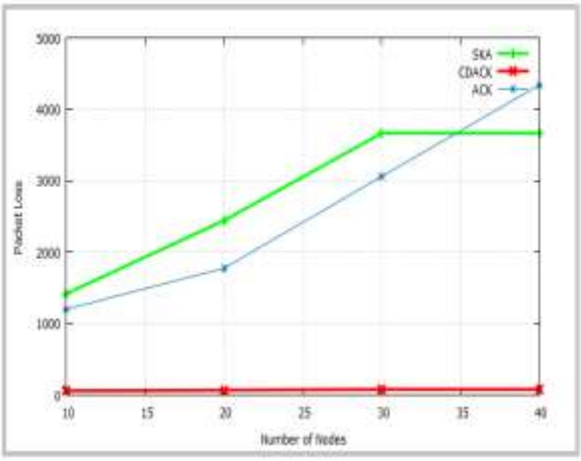

Figure 3-: Packet loss Performance of IDS degradation of MANET in the presence of constrained and malicious packet dropping nodes

IV. CONCLUSION

Mobile ad hoc network is an infrastructure less, constrained resource, and peer to peer wireless network with adaptation and, self-forming capabilities. The network is well suited for deploying in disaster relief and emergency applications, and demands reliable communication. Routing protocols vulnerable towards the packet drops due to its consideration such as nodes in a network are cooperative for communication. Nodes drop the packets due to either malicious behaviour or insufficient resources to handle it. CADCK protocol is designed to prevent packet dropping nodes due to constrained resources as well as malicious activities. The paper investigate the performance of the CDACK protocol and compare its performance with existing intrusion detection systems designed for MANET. Results are clearly indicating that the CDACK increases the packet delivery and reduces the packet loss, and well suited for MANET environment.

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] 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.

[6] 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.

[7] 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.

[8] 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.

[9] 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.

[10] 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.

[11] 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.

[12] 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.

[13] 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.

[14] 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.

[15] 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.

[16] 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

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

[18] 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.

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

[20] Sultanuddin S.J., Hussain M.A. (2019), "*Routing protocol for manet: Token based energy efficient qos aware routing using hybrid optimization algorithms*", International Journal of Recent Technology and Engineering, 7(6), PP.574-582.

[21] [21]Jayanthi E., Hussain M.A. (2019), "*Reliable white list management technique for warned nodes in MANET"'*, International Journal of Vehicle Information and Communication Systems, 4(4), PP.299-315.

[22] [22]Srinivasa Rao Y., Ali Hussain M. (2019), "*Adaptive quality of service medium access control protocol for IEEE 802.11 based mobile Ad hoc network*", International Journal of Innovative Technology and Exploring Engineering, 8(4), PP.430-433.

[23] Balamuralikrishna T., Hussain M.A. (2019), "*A framework for evaluating performance of MADA-AODV protocol by considering multi-dimensional parameters on MANET*", Smart Innovation, Systems and Technologies, 104(), PP.163-174.

[24] Suma P., Hussain M.A. (2018),"*Secure and effective random paths selection (SERPS) algorithm for security in MANETs"*,International Journal of Engineering and Technology(UAE),7 (2),PP. 134-138.

[25] Suresh Babu B., Hussain M.A., Geethanjali N. (2018), "*Adaptive and efficient routing model for MANET using TSCH network*",Journal of Advanced Research in Dynamical and Control Systems,10 (0),PP. 267-278.

[26] Srinivasa Rao Y., Hussain M.A. (2018), "*Dynamic MAC protocol to enhancing the quality of real time traffic in MANET using network load adaptation*", Journal of Advanced Research in Dynamical and Control Systems,10 (0),PP. 1612-1617.

[27] Suma P., Nagaraju O., Hussain M.A. (2017), "*Node disjoint random and optimal path selection (NDROPS) algorithm for security in MANETS*", International Journal of Electrical and Computer Engineering,7(3),PP.1197-1203.

[28] Kolagani P., Aditya K., Venkatesh N., Kiran K.V.D. (2017), "*Multi cross protocol with hybrid topography control for manets"*,Journal of Theoretical and Applied Information Technology,95(3),PP.457-467.

[29] Chavan G.T., Srikanth V. (2018), "*Zone based routing protocol with improved location estimation for MANET*", ARPN Journal of Engineering and Applied Sciences,13 (11),PP. 3650-3656.