International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-9 Issue-5, March 2020

Novel Security Mechanism against DDoS Attack in Mobile Wireless Sensor Network

Kanchan Bala, Pawan Thakur

Abstract: ***In modern time, Mobile Wireless Sensor Networks (MWSN) technology has gained tremendous popularity and is widely used in various applications. MWSN is a temporary network designed for a specific purpose. The dynamic nature of these networks makes them more usable in different fields. The autonomous systems of these wireless mobile nodes can be established anytime, anywhere. However, due to its high mobility, lack of centralized authority and the nature of open media, MWSN is more vulnerable to a variety of security threats and hence more vulnerable to security issues than traditional Wireless Sensor Networks (WSN). MWNs are extremely vulnerable to various types of threats, which will greatly reduce network performance in different situations. In this article, we first provide the general description about MWSN along with its component used and then reviewed the well-known work done by various researchers to detect distributed denial-of-service attack (DDoS). The review thoroughly identified different aspects of the proposed methodology. In addition, we also provide comparative analysis of various analyzed parameters that are examined to determine the effectiveness of the designed protection network against DDoS attack.***

Keywords **: *Mobile Wireless Sensor Networks, DDoS attack, MANET, Throughput, Packet Delivery Ratio, Detection Accuracy.***

I. INTRODUCTION

Mobile wireless sensor networks (MWSNs) play a very important role in today's lifetime in which the data transmission is done through the mobile sensor nodes. MWSN is more flexible in contrast to static WSN because sensor nodes can be installed in any situation and respond to rapid topology changes [1]. The main components that are included by the MWSN are: microcontroller, multiple sensors (i.e. light, temperature, humidity, pressure, mobility, etc.), along with transceiver units and all are powered by a battery [2]. The main application found by MWSN is in environment monitoring, healthcare, navigation, military applications and many more. MWSN mainly faces two challenged namely hardware and environment. In hardware the structure is mainly restricted due to the battery usages and in case of environment; the nodes are deployed in remote areas [3].

Revised Manuscript Received on March 30, 2020.
***** Correspondence Author
Kanchan Baka*, Research Scholar, School of Computer Science Engineering, Carrier Point University, Kota, Rajasthan, India. Email: kanchanbala.sm@yahoo.com
Dr. Pawan Thakur, Professor and head of school of Computer Science Engineering, Govt. PG College, HPTU University, Dharmshala, India.

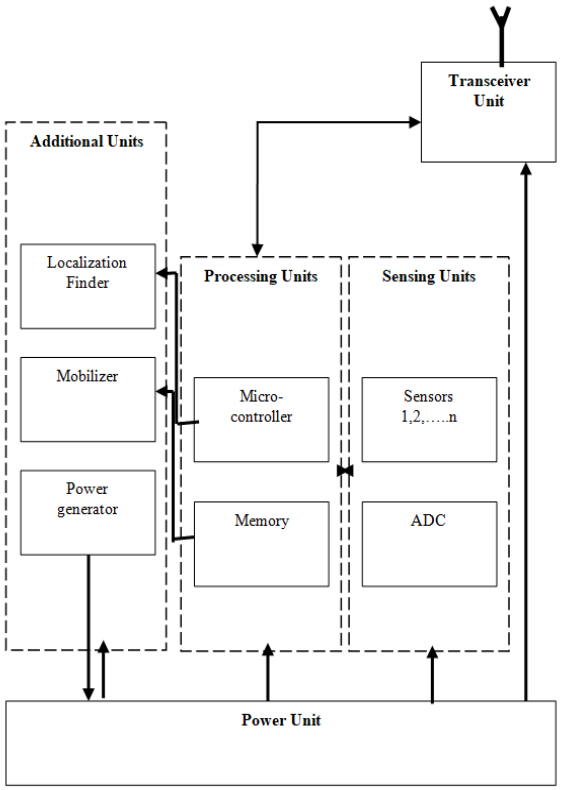

Fig. 1. Architecture of MWSN

The general structure of MWSN is shown in Fig. 1. Normally, the sensor nodes are deployed with different sensing units such as to sense: temperature, humidity, pressure, moisture and so on. The MWSN is a combination of different units such as processing units, sensing units, radio transceiver, and battery power [4]. The uses of sensing nodes are limited because of their storage and battery power usages. The architecture of MWSN is identical to the traditional WSN architecture. But, the MWN architecture consists of some additional elements such as localization finder, Mobilizer and power generator as listed under additional unit of Fig.1. The purpose of localization finder is to search the position of the mobile node. The mobilize is used to offer mobility for a sensor node. The power is delivered to the entire network by power generation unit [5].

A. Mobile WSN Challenges

To focus on the mobility of WSNs, it is important to first understand how common assumptions about statically deployed WSNs change while introducing the mobile entities.

Table-I: MWSN challenges

Challenges	Description
Localization	In a stationary network, the position of nodes is determined during their initialization. However, the position of mobile nodes must be known while the nodes are changing their position within the sensing area. This process of finding position of mobile nodes requires extra time and effort, as well as requires fast localization services.
Dynamic Network Topology	Due to the mobile nature of sensor nodes in MWSN, the topology is also dynamic, which requires novel routing as well as Medium access control (MAC) protocols. Due to the mobile nature of MWSN, the prior information of route stored into the routing table is outdated quickly. Also, the route discovery process must be performed repeatedly, which increase the usages of power, bandwidth as well as require more time.
Power Consumption	Power consumption required high compared to traditional WSN, which increase the energy cost. Also, the MWSN nodes must be equipped with high energy or having self charging capability.
Mobility of Sink	In few of MWSN systems, mobile base station is used to pass the collected data to the desired destination node. The utilization of mobile base station helps to minimize the transmission hops.

B. Energy Conservation

The main problem with MWSN is to save energy. There are many ways to save energy, and many scientists have carried out research related to this. Fig. 2 depicts the classification of energy-saving approaches utilized in WSN [7].

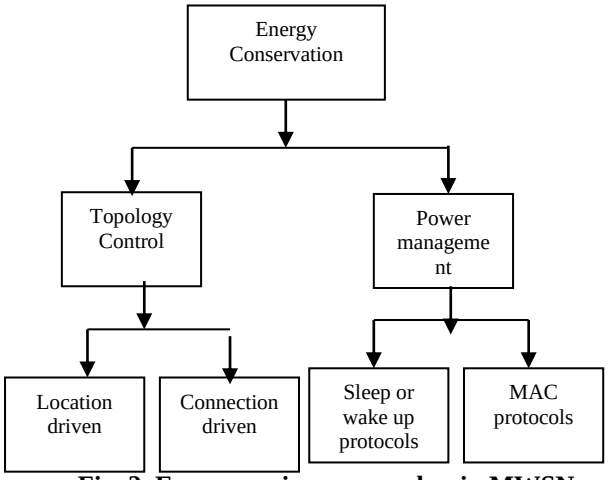

Fig. 2. Energy saving approaches in MWSN

C. Topology control

Topology control in WSN is a technique to decrease the network topology so that the nodes of the network can be reduced and hence utilized less energy. It can also reduce the interference between transmissions nodes simultaneously [8].

D. Power management

Power management algorithm based mainly on connecting radio stations or inactive nodes. This is mainly used for the management of charged batteries. Energy management is primarily designed for battery life. These are based on sleep, waking time, space, geographical factors and active or sleep mode of sensor nodes. Power management is classified into two methods.

- Power grating – In this technique, the energy is harvested by introducing an automatic switch between the chips and the power supply line.
- Power Matching Methods – In this, the battery selection is done as per the cell size. This is the optimal battery-powered choice. It allows the use of steady downstream power. The power is controlled by transmitter and receiver nodes along with internal nodes [9].

A distributed denial of service (DDoS) attack can be stated as an open attack that exhausts the resources of the victim node. It deploy multiple nodes to launch an attack by sending a packet stream to the victim node, thereby consuming the victim node's resources and preventing legitimate source nodes from using them. This type of attack can also be defined as an attacker, which is trying to flood a victim node with number of requests and data, making it impossible for legitimate nodes to use it [10]. When an attack is performed by single node in the network, a denial of service attack (DoS) is defined. When multiple nodes attack the legitimate node, the attack is termed as DDoS. As a result, the victim node becomes unable to process multiple packets and hence denies service.

In the presence of DDoS, the attacker node flooded multiple packets so that the genuine node is blocked. DDoS attack is mainly categorized into two categories: (i) bandwidth depletion and (ii) resource depletion. In the former case, the aim of the attacker node is to flood the affected node with a large amount of data so that the actual information cannot be forwarded to the legitimate node [11]. For the resource depletion case, the attacker's goal is to degrade the important resources of the affected node to avoid legitimate users from utilizing these resources. The existence of DDoS attack affects the network performance such as throughput, packet delivery ratio (PDR), and delay. In this paper, a comparative analysis of different research performed by various researchers has been performed. The main aim is to know how the researchers have worked to protect mobile WSN against the DDoS attack [12].

II. RELATED WORK

In practical MANET, security is the main area of concern. In modern time, different prediction methods have been proposed to enhance the MWN against attacks. A state- of art related to the MWSN protection against DDoS attack has been reviewed in this section along with the summary detail provided in Table. 2.

Khare et al. (13, 2017) have introduced the concept of node trust calculation, which is used to analyze the trust value of every node. For the detection of wormhole, DDoS and Black hole attack in mobile environment the fuzzy logic technique has been used. For the selection of shortest patch while transmitting data Ad-hoc on demand distance vector (AODV) routing protocol has been used.

Initially, zero trust value is assigned to each deployed node and during the initialization of communication trust value is determined during the reception of message from the processor node.

The algorithm used for the detection of DDoS attack is as follows;

Arunmozhi et al. (14, 2011) have presented a flow monitoring technique to prevent network against DDoS attack. The designed mechanism has used the information of medium access control (MAC) layer for the detection of attacker node. For protection of the network bandwidth reservation with distribute rate manage mechanism has been used so that after the identification of attacker node, all incoming messages have been blocked. The resource is available to the genuine user.

Shams and Rizaner (15, 2018) have integrated Intrusion Detection System (IDS) in MANET to provide a reliable solution. Support vector Machine (SVM) has been used to detect the DoS attack with high detection rate in short time. Also, it has been shown that the network efficiency has not been affected by the network size. It has also been proved that the routing protocols such as AODV, OLSR and DSR are all provide equal outputs while using during the communication process in the presence of DOS attack. From the experiments it has been examined that the SVM approach is highly suited for the prevention of mobile network from DoS attack.

Kesavamoorthy and Soundar (16, 2018) have introduced an autonomous multi-agent system in addition to particle swarm optimization (PSO) approach to protect mobile network against DDoS attack. The multi agent system helps to increase the decision rate accuracy while detecting the attacker node. The attacker node is found by examine the entropy along with covariance mechanism. Using this concept, the monitoring agent keeps their eyes on the network resources. If the system found anything wrong, it generates the detection mechanism. The result shows that the security as well as the performance of the system increases in an efficient way.

Mehmood et al. (17, 2018) have presented a secure Internet of Things (IoT) structure against DDoS attack. Naïve Bayes classification algorithm has been integrated with IDS, which was deployed in terms of multi agent in the entire network. This is used to sense the misbehavior activities of the data traffic of the nodes. Naïve Bayes classifier algorithm has been utilized to distinguish the normal and abnormal activities of the network nodes. It is basically a supervised learning approach, which works on the Bayes' theorem.

$$P((J \mid K)=(P(k \mid J)P(J))/(P(K)) \quad (1)$$

$$P((J \mid K)= P(K\_1 \mid J)\times P(K\_2 \mid J)\times P(K\_3 \mid J)\times \cdots\cdots\cdots\cdots P(K\_n \mid J)\times P(J) \quad (2)$$

By using the above equations, one can compute the probability of J events conditioned on the K data. This is done by determining the probability of K conditioned by the event J and then multiply the probability of event J. In the case of attacker detection, this can be calculated by determining the probability of an attack based on some data by first calculating the probability that some previous data is part of that type of attack, and then multiplying by that type of attack Probability occurs, reducing normalization of P (K).

Kolandaisamy et al. (18, 2018) have presented a new Multivariant Stream Analysis (MVSA) system, which maintains the number of stages for the identification of DDoS attack in Vehicular ad hoc network (VANET). The attacker node has been detected on the basis of different traffic conditions and the time frames. A set of rules has been defined for different traffic class in distinct time frame. The rule set has been designed based on the extracted node's features.

Sowah et al. (19, 2019) have presented ANN based IDS for MANET. Five number of nodes are deployed in the designed network among all N-5 is used as an administrative node, which monitors the activities of the other network nodes. Based on the nodes features ANN is trained so that in future, the unwanted activities in the network can be identified.

Shona et al. (20, 2018) have presented an effective data mining based approach for IDS in MANET. For the detection of multiple attacks such as firefly algorithm in addition with genetic algorithm has been employed for feature selection of attacks. The combined algorithm proposed by the researcher is written as below.

Hybrid FA-GA feature selection algorithm

Attributes as an Input: Designed MANET Properties and Size of Population (N)
Attributes as an Output: Selected Properties of MANET
Step 1: Design a MANET Simulator using the N sensor nodes
Step 2: Deploy attackers with the network for simulation purpose.
Step 3: Design Create attack profile by stimulating the attacks
Step 4: Make a repository to store the properties of normal profile and attack profile nodes.
Step 5: Define the basic operators with N population size and Termination Criteria (TC)
Step 6: While (not reached at TC) // Loop for feature selection
Step 7: For k=1→N with increment
Step 8: With the help of RNN classifier, check the fitness of N
Step 9: Fitness of N = Classification Accuracy
Step 10: If Fitness of N is the best fitness value
Step 11: Best Fitness of N = Fitness of N
Step 12: End
Step 13: Crossover is performed on Best Fitness of N
Step 14: Firefly algorithm is used instead of mutation based on the light intensity (LI)
Step 15: LI=Maximum value as a Best Fitness of N in terms of the Properties of the MANET
Step 16: Check the TC and go ahead
Step 17: End
Step 18: Return: Selected Properties of MANET in term so the LI which act the input of the RNN
Step 16: End

The output obtained after applying the FA with GA is provided as input to the Replicator Neural Network (RNN) which categorizes the data.

Table-II: Comparative study of existing techniques

Author, publisher and Year	Technique Used	Objective	Performance Metrics	Number of deployed nodes and simulation area	Simulator	Outcomes
Khare et al. (2017)	Fuzzy logic with AODV	To protect network against three different attacks (wormhole, DDoS and blackhole)	PDR and Number of search packets broadcasted with respect to simulation time (s)	Nodes→50 Area→800×800	ns2-2.34	PDR around 90 % has attained.
Arunmozhi et al. (2011) Springer	Flow monitoring control mechanism	To design a network with high detection rate, low development cost	Bandwidth received (Mbps) and PDR with respect to number of attackers	Nodes→80 Area→1200 ×1200	NS2	PDR around 50 % has been acheived
Shams and Rizaner (2018) Springer	Support vector Machine	The aim is to detect the malicious node in less time with high detection rate	End to end delay (s) PDR (%) And detection rate (%) with respect to number of attacks	Nodes→10 Area→500 ×500	Ns2	Detection rate=94 % PDR=78 % End to End delay=0.1 s
Kesavamoorthy and Soundar (2018) Springer	autonomous multi-agent system in addition to particle swarm optimization (PSO) approach	To protect network against DDoS agent	Accuracy (%), False detection (%), Average attack detection time (ms) and attack recovery time (ms) examined with respect to number of attacker nodes	Nodes→16-512	For PSO implementation core java is used and for the creation of cloud environment IDE is used.	Detection accuracy around 98 % has been obtained.
Mehmood et al. (2018) Springer	The aim is to analyze the performance of the system while using naïve Bayes with multi agent system for the protection of wireless network.	Naïve Bayes classifier	End to end packet forwarding rate, delays is measured with respect to percentage of malicious node.	Nodes→400	NS 2.35	End to end packet forwarding rate→0.7 s Delays→ 1600
Kolandaisamy et al. (2018) Hindwai	The aim is to design a secure VANET communication network with high accuracy.	Multivariant Stream Analysis Approach	Throughput (5), Accuracy (%) , PDR ad Delay vs time in (ms) have been measured .	Nodes→5 to 113	NS 2.35	Throughput → 60% Accuracy→60 % PDR→60% Delay→50 %
Sowah et al. (2019) Hindawi	The aim is to secure network with high performance	ANN approach	Precision, recall, f-measure and accuracy	Nodes→5 to 19	Java software tool named "MitmProtectorWithWeka	Precision→ 50 % Recall→ 81% Accuracy around 88.235% has been attained.
Shona et al. (2018) IEEE	The aim is to detect attacker node with high speed in a simple way.	Firefly with GA with Replicator Neural Network (RNN) as classifier.	Precision, recall, f-measure and accuracy	Nodes→10	NS2	Precision→ 95.8 % Recall→ 96.1% Accuracy→ 96 %

III. RESULTS

From the above explained existing work related to the protection of wireless WSN from DDoS attack, it has been examined that the researchers were tries to improve the performance of the network by applying various techniques. The performance has been measured on the basis of PDR, Accuracy, precision, recall, F-measure, Delay and throughput, which are defined below.

A. Packet delivery rate (PDR)

It is measured by total packets received at the destination node divided by total packets transmitted by the source node multiplied by 100 %. The formula is written below:

$$PDR = \frac{\sum_{i=1}^{n} Y_i}{\sum_{i=1}^{n} Z_i} \times 100\% \quad (3)$$

Here, Y_i and Z_i are the total number of received packet, total number of transmitted data packets.

B. Throughput

It is determined by totality amount of data packets reached at the destination node in the designed Mobile wireless network divided by difference of end and begin time of simulation time. Mathematically can be represented as:

$$Throughput = \frac{\sum_{i=1}^{n} Z_i - \sum_{i=1}^{n} Y_i}{T_{end} - T_{begin}} \quad (4)$$

T_{end}, T_{begin} is the time at which data transmission is started and the time at which the data transmission is completed.

C. Accuracy

This parameter is the used to find correctly detected attacker node. Mathematical equation used for determine accuracy is written below:

$$Accuracy = \frac{\sum TP + \sum TN}{\sum TP + TN + FP + FN} \quad (5)$$

The formula used for precision, recall and F-measure is written below.

$$Precision = \frac{TP}{TP + FP} \quad (6)$$

$$Recall = \frac{TP}{TP + FN} \quad (7)$$

$$F - measure = 2 \times \frac{pecison \times Recall}{Precision + Recall} \quad (8)$$

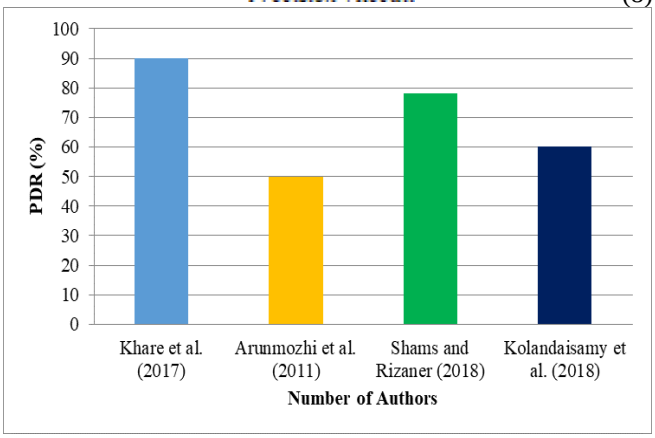

Fig. 3. Comparison of PDR

Fig. 3. represents the comparison of PDR examined by the number of researchers denoted along the x axis of the graph. From the fig. 3. It is clear that the PDR observed by author Khare et al. is high compared to other three researchers. This is obtained as the researchers have used fuzzy rule set for the detection of attacker node and the detection rate of about 90 % has been attained.

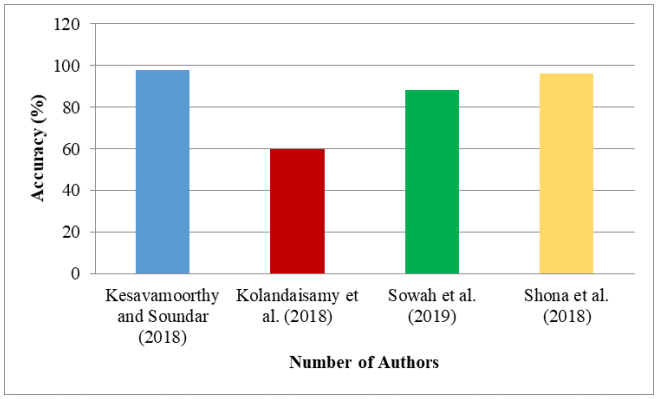

Fig. 4. Accuracy

Fig. 4. represents the comparative graph for the detection accuracy obtained by number of researchers while working to detect DDoS attack in MWSN. From the Fig. 4. ,It is clearly seen that the Kesavamoorthy and Soundar (2018) have obtained highest accuracy compared to other past work. This is obtained as the features of the nodes are extracted using swarm based optimized technique.

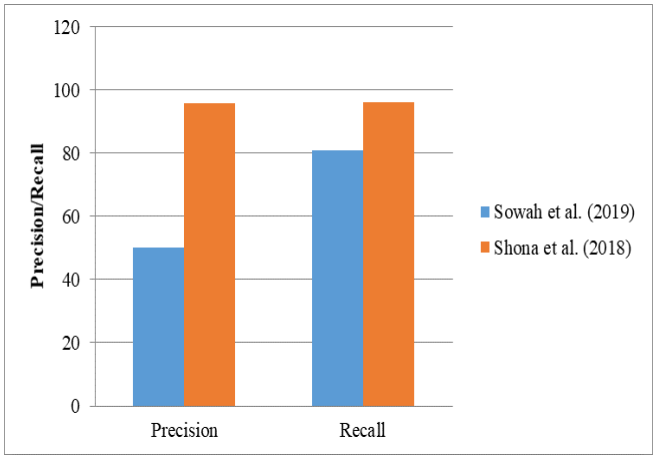

Fig. 5. Precision and recall

Fig. 5. represents the precision and recall values analyzed by Sowah et al. (2019) and Shona et al. (2018) to protect the network from the DDoS attack. From the graph shown in Fig. 4. , It has been analyzed that the better precision and recall values of the network designed by Shona et al. (2018) has been obtained.

IV. CONCLUSION

In the past decade, MANET security has become one of the key research areas. Various researchers have proposed various secure routing schemes. The purpose of this work is to conduct a detailed review of existing methods in different types of mobile wireless networks. It should be noted that the comparison of different methods proposed by distinct researchers is sometimes impractical because different methods have been developed for different situations and applications. However, each method has its own limitations. In this work, it was concluded that mobile Wireless Sensor Network are decentralized networks where the location of mobile nodes changes at any instant of time. Due to this nature of the network, various types of active and passive attacks may be affected the performance of network.

This article reviews the various techniques used to isolate malicious nodes specifically DDoS attacker node and the performance of that network is analyzed on the basis of different parameters. From the comparison, it has been examined that when techniques such as fuzzy logic or optimization technique (PSO) has been used in the network, the performance of the network is enhanced.

REFERENCES

1. Munir, S. A., Ren, B., Jiao, W., Wang, B., Xie, D., & Ma, J. (2007, May). Mobile wireless sensor network: Architecture and enabling technologies for ubiquitous computing. In 21st International Conference on Advanced Information Networking and Applications Workshops (AINAW'07) (Vol. 2, pp. 113-120). IEEE.
2. Amundson, I., & Koutsoukos, X. D. (2009, September). A survey on localization for mobile wireless sensor networks. In International Workshop on Mobile Entity Localization and Tracking in GPS-less Environments (pp. 235-254). Springer, Berlin, Heidelberg.
3. Heo, N., & Varshney, P. K. (2003, March). A distributed self spreading algorithm for mobile wireless sensor networks. In 2003 IEEE Wireless Communications and Networking, 2003. WCNC 2003. (Vol. 3, pp. 1597-1602). IEEE.
4. Schmidt, S., Krahn, H., Fischer, S., & Wätjen, D. (2004, August). A security architecture for mobile wireless sensor
5. Khan, A. U. R., Madani, S. A., Hayat, K., & Khan, S. U. (2012). Clustering-based power-controlled routing for mobile wireless sensor networks. International journal of communication systems, 25(4), 529-542.networks. In European Workshop on Security in Ad-Hoc and Sensor Networks (pp. 166-177). Springer, Berlin, Heidelberg.
6. Rezazadeh, J. (2012). Mobile wireles sensor networks overview. International Journal of Computer Communications and Networks (IJCCN), 2(1).
7. Wang, Y. (2010). Study on energy conservation in MANET. Journal of Networks, 5(6), 708.
8. Muchtar, F., Abdullah, A. H., Hassan, S., & Masud, F. (2018). Energy conservation strategies in Host Centric Networking based MANET: A review. Journal of Network and Computer Applications, 111, 77-98.
9. Chaudhry, R., & Tapaswi, S. (2018). Optimized power control and efficient energy conservation for topology management of MANET with an adaptive Gabriel graph. Computers & Electrical Engineering, 72, 1021-1036.
10. Khan, S., Hashim, F., Rasid, M. F. A., & Perumal, T. (2018, July). Reducing the Severity of Black Hole and DDoS Attacks in MANETs by Modifying AODV Protocol using MAC Authentication and Symmetric Encryption. In 2018 2nd International Conference on Telematics and Future Generation Networks (TAFGEN) (pp. 109-114). IEEE.
11. Nehra, D., Dhindsa, K. S., & Bhushan, B. (2019). Clustering based Model to Provide Defense against DDoS attacks in MANETs. Journal of Communication Engineering & Systems, 9(1), 7-13.
12. Dhindsa, K. S., & Bhushan, B. (2020). Clustering-Based Technique to Defend DDoS Attacks in Mobile Ad Hoc Networks. In Proceedings of ICETIT 2019 (pp. 48-58). Springer, Cham.
13. Khare, A. K., Rana, J. L., & Jain, R. C. (2017). Detection of wormhole, blackhole and DDOS attack in MANET using trust estimation under fuzzy logic methodology. International Journal of Computer Network and Information Security, 9(7), 29.
14. Arunmozhi, S. A., & Venkataramani, Y. (2011, January). A new defense scheme against DDoS attack in mobile ad hoc networks. In International Conference on Computer Science and Information Technology (pp. 210-216). Springer, Berlin, Heidelberg.
15. Shams, E. A., & Rizaner, A. (2018). A novel support vector machine based intrusion detection system for mobile ad hoc networks. Wireless Networks, 24(5), 1821-1829.
16. Kesavamoorthy, R., & Soundar, K. R. (2018). Swarm intelligence based autonomous DDoS attack detection and defense using multi agent system. Cluster Computing, 1-8.
17. Mehmood, A., Mukherjee, M., Ahmed, S. H., Song, H., & Malik, K. M. (2018). NBC-MAIDS: Naïve Bayesian classification technique in multi-agent system-enriched IDS for securing IoT against DDoS attacks. The Journal of Supercomputing, 74(10), 5156-5170.
18. Kolandaisamy, R., Md Noor, R., Ahmedy, I., Ahmad, I., Reza Z'aba, M., Imran, M., & Alnuem, M. (2018). A multivariant stream analysis approach to detect and mitigate DDoS attacks in vehicular ad hoc networks. Wireless Communications and Mobile Computing, 2018.
19. Sowah, R. A., Ofori-Amanfo, K. B., Mills, G. A., & Koumadi, K. M. (2019). Detection and Prevention of Man-in-the-Middle Spoofing Attacks in MANETs Using Predictive Techniques in Artificial Neural Networks (ANN). Journal of Computer Networks and Communications, 2019.
20. Shona, D., & Kumar, M. S. (2018, July). Efficient IDs for MANET Using Hybrid Firefly with a Genetic Algorithm. In 2018 International Conference on Inventive Research in Computing Applications (ICIRCA) (pp. 191-194). IEEE.

AUTHORS PROFILE

Kanchan Baka, Research Scholar, School of Computer Science Engineering, Carrier Point University, Kota, Rajasthan, India.
Email: kanchanbala.sm@yahoo.com

Dr. Pawan Thakur, Professor and head of school of Computer Science Engineering, Govt. PG College, HPTU University, Dharmshala, India.