Mitigating the DDoS Attacks Using PDDoS Efficient Networking Protocol in MANET for Military Applications

Jhum Swain[1], Binod Kumar Pattanayak[2], Bibudhendu Pati[3]
[1]*Siksha 'O' Anusandhan University, Bhubaneswar, Odisha*
[2]*Siksha 'O' Anusandhan University, Bhubaneswar, Odisha*
[3]*C. V. Raman College of Engineering, Bhubaneswar, Odisha*

Abstract— In military applications mobile ad hoc network plays very important role because it is specifically designed network for on demand requirement and in situations where set up of physical network is not possible. This special type of network which takes control in foundation less correspondence handles genuine difficulties prudently, for example, very vigorous and dynamic military work stations, gadgets and littler sub-arranges in the combat zone. Therefore there is a eminent demand of designing efficient routing protocols ensuring security and reliability for successful transmission of highly sensitive and confidential military information in defense networks. Distributed denial-of-service (DDOS) attacks remain a noteworthy security issue, the alleviation of which is hard particularly with regards to profoundly conveyed botnet-based attacks. The early discovery of these attacks, although challenging, is important to secure end-clients and additionally the costly system framework assets. With this objective, a energy efficient network layer routing protocol in the network for military application is designed and setup BIAS variation for observe the flow of routing process. Here using network simulator-2 and design a network to overcome effect of DDOS attack and increase reliability and network performance up to a high level of routing.

Keywords— *MANET, AODV, QOS, MAC Layer, Network Layer, BIAS Variance, PDR*

I. INTRODUCTION

The gigantic technological rejuvenation of wireless communiqué [1] has been emerged in the system of mobile ad hoc networks (MANETs) in current decade. MANETs are excellent networking structure that is based with no settled framework. Because of the highly dynamic, extremely mobile and self-configurable nature of its autonomous nodes, performance of this network is outstanding in terms of transmission, throughput and reliability.

Mobile ad hoc networks [1] have very important application and operations in battle fields and in disaster situations such as deployment of networks, high security measures in the network, any end to end transmission, mobile connectivity without failure, anti jamming mechanism, etc. All network activity must be done spontaneously without any link failure even in micro second level. The soldiers during on line battle should be able to remain continuously connected with each other in order to get any latest information, or command from their chief or to discuss before any action. Sometimes penetration of the satellite signals is not desirable to caves or dense forest or under sea places where it is again challenging to sustain connectivity.

Many research works have focused on the security of MANETs. Most of them [11] deal with prevention and detection approaches to combat individual misbehaving nodes. In this regard, the effectiveness of these approaches becomes weak when multiple malicious nodes collude together to initiate a collaborative attack, which may result to more devastating damages to the network. The lack of any infrastructure added with the dynamic topology feature of MANETs make these networks highly vulnerable to routing attacks such as black hole and gray hole and DDoS attacks. In DDoS attacks, the incoming traffic flooding the victim originates from many different sources. This effectively makes it impossible to stop the attack simply by blocking a single source.

In this paper, we are utilizing Ad Hoc Distance Vector Routing Protocol for network routing. It known as a receptive protocol that it asks for a route when required and that it doesn't keep up routes for that those nodes that don't effectively participate in that a correspondence. A critical element of AODV is that it utilizes that a goal grouping number in that, which compares to a goal node that it was asked for by a directing sender hub. The goal itself giving the number along that route it needs to taken to reach from the demand sender node up to the destination node. On the off chance that there are multiple routes from a demand from sender to a receiver, the sender brings that route with a higher arrangement number itself. This guarantees the impromptu system convention remains circle - free.

- *DDOS*

Distributed denial of service (DDOS) attacks still constitute a major concern [2] even through many works have tried to address this issue in the past [3]. As they developed from moderately humble megabit beginnings in 2000, the biggest DDOS attacks have now grown a hundredfold to break the

100Gb/s, for which the dominant part of ISPs today need proper foundation to alleviate them [2].

Latest works go for countering DDOS attacks by battling the fundamental vector, which is typically the utilization of botnets [4]. A botnet is a large system of traded off machines (bots) controlled by one substance. The master can dispatch synchronized assaults, for example, DDOS, by sending requests to the bots by means of a Command and Control channel. Unfortunately, identifying a botnet is additionally hard, and effective arrangements may require to take an interest effectively to the botnet itself [5], which raises critical ethical issues, or to first recognize botnet-related malevolent activities, which may delay the alleviation.

To maintain a strategic distance from these issues, this paper concentrates on the location of DDOS attacks and per area not their hidden vectors.

In spite of the fact that non-conveyed denial of service attacks typically misuse defenselessness by sending few precisely manufactured packets to disrupt a service, DDOS attacks are for the most part utilized for flooding a specific victim with gigantic movement as featured in [2]. In fact, the popularity of these attacks is because of their high adequacy against any sort of service since there is no compelling reason to distinguish and abuse a specific service particular imperfection in the victim. Thus, this paper concentrates only on flooding DDOS attacks.

II. RELATED WORKS

Over last decade's most of the researchers have come out with different intelligent proposals some of which are based on energy efficiency, delay management and few of them are based on cross layer architecture. Agbaria1 [6], et al. formulated extrapolation based system that considered dynamic planning, resource management, speed, multipath search to give continuous and QOS need of a MANET. Sivakumar and Duraiswamy [7] introduced effective calculation to support Quality of Service (QoS), by the utilization of load-circulating and congestion avoidance routing strategy. Their proposed calculation computes the cost metric in view of connection loads. The connections [1] having lighter burdens were preferred for sending activity to maintain a strategic distance from congestion. Srivastava and Daniel [8] exhorted a energy efficient routing to enhance the connection use by balancing the energy utilization between effectively abused and underutilized elements. Their protocol manages few key components like remaining energy, transmission capacity, load and hop count mean route discovery. Ahmed [9], et al. has given ant colony based load balanced approach in MANET. They analyzed routing [1] by linking it with resource scheduling problem. Their algorithm adaptively alters fragment estimate in view of node movement and limits the transmission time.

Madhan Mohan & Selvakumar [13] has proposed PC-AODV which is another cross-layer design approach that uses power control strategies to send data and control packets of both network layer and data link layer. In this approach, various routing entries are made according to the left level of power in the nodes. As per necessary power level a path is selected during the route discovering process. This protocol incorporated power level logic in route identification and route preservation phases. According to the routing table values, various power levels (PL) are applied with different packets. So there is compatibility of power levels in both the layers. This algorithm exhibits better performance in lowering the energy consumption and a higher packet delivery ratio. Another layered approach for Improving power efficiency in MANET [14] has been used which is different from customary style of design and it gears the cross-layer communication between three important layers physical, MAC and network layer. A new scheme called cross layer power control (CLCP) is used to augment the transmission power by using an enhanced strategy to find an appropriate route between two nodes. NS2 was used to simulate this approach, which shows better result. A detailed survey on real time MANET protocols have been carried out by Rath & Pattanayak7. Similarly mobile agent intruder detection systems with delay and [15] power issues are analyzed by Pattanayak & Rath [16].

III. POWER AND DELAY OPTIMIZED PROTOCOL

The main core module in our proposed power delay optimized AODV protocol [12] is a routing engine that is the controller of all functions in the mobile work station. Sequentially it performs three important tasks during static or mobile position of a node and after a packet arrives to a node such as the channel sensing, the mini database handling module and the intelligent decision taking sub module. In the first sub module of channel sensing, status messages are transmitted periodically with formal interruption of time by the node in order to broadcast presence of that node in the channel. In the next sub module a small database is maintained to reserve and recall routing information's regarding a particular path, which can be referred next time data transmission takes place between same sender and receiver. A threshold value is calculated in particular procedure to select the next hop station as per the algorithm as given below, which will be used in the routing decision module to finally select a suitable station.

A. Algorithm (selection for node):

```
Step1: For every intermediate node b_ node from source to destination access
Step2: For every neighborhood node p_node of b_node
Step3: Find all the acquaintance nodes of p_node from routing_table of p_node
Step4: Calculate the cost_func of every node using calc_Threshold()
Step5: Sort the neighbor nodes of p_node in ascending order their cost function
Step6: Store the sorted values in temp storage_buffer_system
Step7: For every node j_node in temp_buffer check status
Step8: If (j_node(!congested_node))
Step9: Then go to step 11
Step10: Else select the next_node
Step11: If cost_func > req_cost_func
Step12: Select node as next_node
Step13: Else go to step2
Sub_routine calc_threshold()_value
Begin
Return (power_level*packet_size*no_packets)
End
```

We existed a cross layer mechanism between the data link layer and the system layer by introducing a friendly packet between the two layers. To reduce the overhead of route finding in terms of delay and power consumption we suggest that this friendly packet provides necessary information from the data-access link layer to its upper network layer. Developed an improved channel access technique at the MAC layer make it compatible to work with PDO-AODV.

B. Cross-layer communication:

As explained above [12], a friend packet is sent by the info link layer to provide quick service and support to the network layer PDO AODV protocol during path finding process. The packets contain the broken link (BRL) field that provides the possibility of broken link due to mobility of the forwarding node. The neighbor node detection (NND) field sends the nearest updated neighbor node information which can be quickly updated in the routing table. Signal to noise ratio (SNR) field provides strength of noise in wireless channel while the packet is transmitting. RTS/CTS packets convey the control information like request to send data to that particular node and clear to send data that offers total time for which the channel remains eventful.

IV. PROPOSED SYSTEM

Our proposed system operates on batches of consecutive readings of sensors, proceedings ion several stages. In the primary stage we give an underlying assessment of two noise parameters for sensor users, bias and variance. Based on such an estimation of the bias and variance of each sensor, in the next stage of process, we give an underlying assessment of the reputation vector ascertained utilizing maximum likelihood estimation. The next process of proposed scheme, the initial reputation vector gave in the second stage is utilized to evaluate the dependability of every sensor in view of the separation of sensor readings to such initial reputation vector. In this process, final stage of process suggests a novel collusion detection mechanism for eliminating the contributions of compromised nodes.

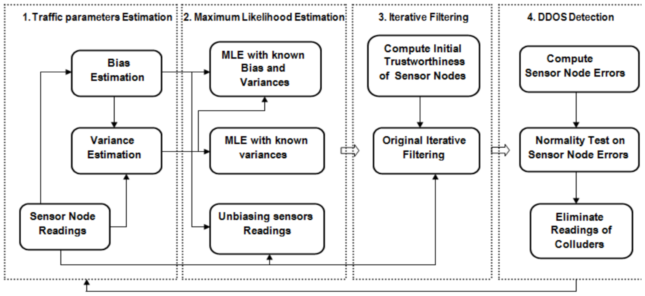

1. Traffic parameters Estimation
2. Maximum Likelihood Estimation
3. Iterative Filtering
4. DDOS Detection
Bias Estimation
Variance Estimation
Sensor Node Readings
MLE with known Bias and Variances
MLE with known variances
Unbiasing sensors Readings
Compute Initial Trustworthiness of Sensor Nodes
Original Iterative Filtering
Compute Sensor Node Errors
Normality Test on Sensor Node Errors
Eliminate Readings of Colluders

Fig.1. Prevention of DDoS attack framework

The detection of colluders in a sophisticated collusion attack is that at least one of the compromised nodes will have the highly non stochastic behavior. Here the error of non-traded off nodes, not withstanding when it is extensive, originates from countless components, and in this way should generally have a Gaussian appropriation. Therefore, rather than taking a look at the root mean square greatness of blunders of every sensor, we take a look at the measurable dissemination of such mistakes, evaluating the probability whether they originated from a typically appropriated irregular variable. Nodes that are very improbable to have originated from a regularly dispersed arbitrary variable, potentially with a bias, are disposed of.

Figure.1 illustrates the novel approach of estimating the bias and variance of noise for sensor nodes based on their readings. The variance and bias of a sensor noise can be interpreted as the distance measures of the sensor readings to the accurate value of the signal. In fact, the distance measures obtained as our estimates of the bias and variances of sensors also make sense for non-stochastic errors.

According to the proposed work scenario, the attacker exploits the vulnerability of the IF algorithms which originates from a wrong assumption about the initial truthfulness of sensor nodes. Our contribution to address these weaknesses is to employ the results of the proposed robust data aggregation technique as the initial reputation for this algorithm. Moreover, the initial weights for all sensor nodes can be processed view on the distance of sensors of readings to such an initial reputation.

A. Proposed Output process

- *Cluster head selection*

```
Cluster Formation at 6.001358
Cluster - 1: 14 15 16 21
Cluster - 2: 12 13 18
Cluster - 3: 0 11 23
Cluster - 4: 9 10
Cluster - 5: 17 19 24
Cluster - 6: 1 2
Cluster - 7: 3 4 5 7
Cluster - 8: 6 8 20 22
Distance from node 14 to its neighbor 14 15 16 21
0.000000 136.014705 125.299641 206.002427
Distance from node 15 to its neighbor 14 15 16 21
136.014705 0.000000 101.980390 86.353923
Distance from node 16 to its neighbor 14 15 16 21
125.299641 101.980390 0.000000 112.680966
Distance from node 21 to its neighbor 14 15 16 21
206.002427 86.353923 112.680966 0.000000
Cluster Head (CH) is node: 16
```

- *Routing table*

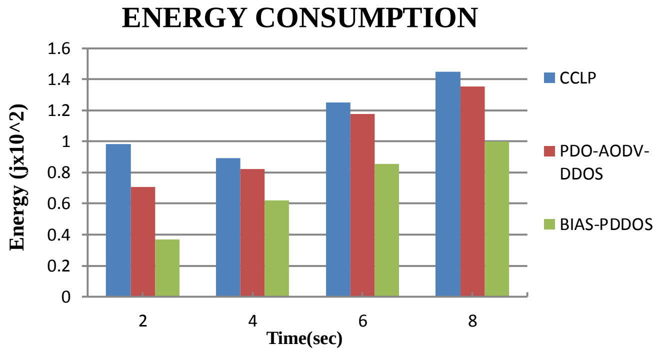
```
NODE: 9t
 CURRENT_TIME---------:2.0059t
 rt->rt_dst-----------: 10t
 rt->rt_nexthop------------:10t
 rt->rt_hops ------------:1t
  rt->rt_seqno--------------------: 10t
 rt->rt_flags--------------------: 12.0059t
 ------------------:1
NODE: 2t
 CURRENT_TIME---------:2.0107t
 rt->rt_dst-----------: 1t
 rt->rt_nexthop------------:1t
 rt->rt_hops ------------:1t
  rt->rt_seqno--------------------: 14t
 rt->rt_flags--------------------: 12.0107t
 ------------------:1
```

- *Computation*

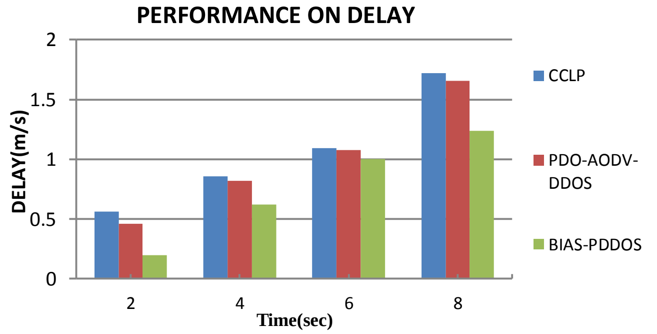
```
Final score-computation
Final score value of node 0 is 0.129085
Final score value of node 1 is 0.369669
Final score value of node 2 is 0.283473
Final score value of node 3 is 0.129085
Final score value of node 4 is 0.129120
Final score value of node 5 is 0.129085
Final score value of node 6 is 0.434951
Final score value of node 7 is 0.129120
Final score value of node 8 is 0.334080
```

V. SIMULATION RESULTS

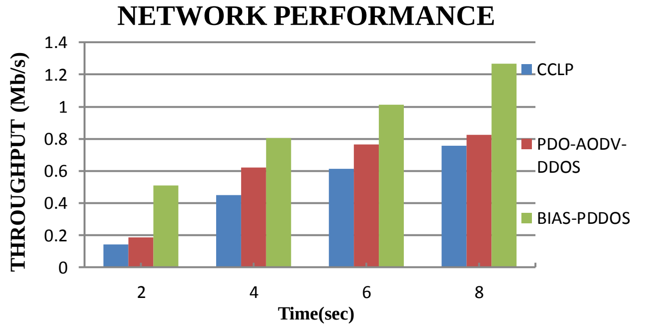
In this section, shows the parameters considered for simulation of our protocol with effective method. The objective of our experimental results is to evaluate the robustness and efficiency of our approach for estimating and detecting the DDOS attack and mitigating the DDOS in the sight of our proposed system. For each process of network, we calculate the delay, energy and throughput then solving the problem of network it effects by DDOS.



The above graph represented as Energy consumption, and it can be depends on time to vary the output. The performance of the Bias variance mechanism improves energy values compare to Power and Delay Optimized-AODV with DDOS attack algorithm and Cross Layer Power Control method.



The above graph represented as End to End Delay, and it can be depends on time to vary the output. The performance of the Bias variance algorithm improves delay time it means decrease the delay between communication nodes compare to Power and Delay Optimized-AODV with DDOS attack algorithm and Cross Layer Power Control method.



The above graph represented as Throughput, and it can be depends on time to vary the output. The performance of the Bias variance algorithm improves the throughput compare to Power and Delay Optimized-AODV with DDOS attack algorithm and Cross Layer Power Control method.

Table 1: Parameters description

PARAMETER	VALUE
Application traffic	CBR
Transmission rate	5 packets/ms
Radio propagation model	Two ray ground
Packet size	512 bytes
Channel type	Wireless channel
Maximum speed	120 Kbps
Simulation time	8000ms
Mobile nodes	25
Network size	1000x500
MAC type	Mac/802_11
Routing protocol	AODV
Simulator	Ns-2.35

VI. CONCLUSION

In this study, setup the issue of power efficiency, node selection and unfair load balancing for mobile ad-hoc networks using an interaction based cross layer mechanism. They focused on optimizing link cost based on power and delay metric to mitigate this severe issue restoring precious network resources. We have used an optimized channel access method in MAC protocol of data link layer which sends a friend packet to the system layer that contains critical information such as broken link, updated neighbor list and signal quality which helps the router in network layer during route search by consuming less amount of residual energy. Here DDOS attack effect applicable to existing protocol. So here this attack is more effect to the routing process. We propose effective bias variance method to existing method. We give an underlying approximation of the integrity of sensor nodes which makes the algorithms collusion powerful, as well as more exact and quicker converging. This protocol solves the resource constraint with DDOS attack problem of ad hoc network to a great extent and the simulation study shows that it shows better performance than other leading different approaches based on similar cross layer approach.

VII. REFERENCES

[1] Mamata Rath, Binod Kumar Pattanayak and Bidudhendu Pati, - Energy efficient MANET Protocol using Cross Layer Design for Military Applications -, vol.66, no.2, March 2016, pp.146-150.

[2] A. Networks, Arbor, Lexington,MA, - Worldwide ISP security report -, Tech. Rep., 2010.

[3] T. Peng, C. Leckie, and K. Ramamohanarao, - Survey of network-based defense mechanisms countering the DoS and DDoS problems -, Comput. Surv., vol. 39, Apr. 2007, Article 3.

[4] E. Cooke, F. Jahanian, and D. Mcpherson, - The zombie roundup: Understanding, detecting, and disrupting botnets -,in Proc. SRUTI, Jun. 2005, pp. 39–44.

[5] T. Holz, M. Steiner, F. Dahl, E. Biersack, and F. Freiling, - Measurements and mitigation of peer-to-peer-based botnets: A case study on storm worm -, in Proc. USENIX LEET, 2008, Article no. 9.

[6] Agbaria, A.; Gershinsky, G.; Naaman N. & Shagin, K, - Extrapolation-based and QoS-aware real-time communication in wireless mobile ad hoc networks -, In the 8th IFIP Annual Mediterranean Adhoc Networking Workshop, Med-Hoc-Net 2009. pp.21-26. doi: 10.1109/MEDHOCNET.2009.5205201

[7] Siva, K. & P. Duraiswamy, K, - A QoS routing protocol for mobile ad hoc networks based on the load distribution -, In the IEEE International Conference on Computational Intelligence and Computing Research (ICCIC), 2010, pp.1-6. doi: 10.1109/ICCIC.2010.5705724

[8] Srivastava, S.; Daniel, A.K.; Singh, R. & Saini, J.P, - Energy efficient position based routing protocol for mobile ad hoc networks -, In the IEEE International Conference on Radar Communication and Computing (ICRCC), 2012, pp.18-23. doi: 10.1109/ICRCC.2012.6450540

[9] Ahmed, M.; Elmoniem, Abd; Ibrahim, Hosny M.; Mohamed, Marghny H. & Hedar, Abdel Rahman, - Ant colony and load balancing optimizations for AODV routing protocol -, Int. J. Sensor Networks Data Commun., 2012, 1. doi: doi:10.4303/ijsndc/X110203

[10] K.Prathap, Vallamkonda Manjunath, - Defending Against Malicious Attacks in MANETS using Cooperative Bait Detection Approach - ,Research in applied science and engineering, Nov.2015, vol.3 issue XI, ic value-13.98.

[11] Deepali R. Tambekar, Hema kumbhar, - CBDA: To Detection of Collaborative Attack in MANET'S -, advance engineering and research development, Dec-2015, Vol.2. issue 12.

[12] Mamata Rath, Binod Kumar, Pattanayak and Bibudhendu Pati, - Energy efficient MANET Protocol Using Cross Layer Design for Military Applications -, Vol.66.2, March 2016, pp.146-150, DOI:10.14429/dsj.66.9705.

[13] [13] MadhanMohan, R. & Selvakumar, - K. Power controlled routing in wireless ad hoc networks using cross layer approach. Egyptian Info. J., 2012, 13, 95-101. doi:10.1016/j.eij.2012.05.001

[14] Ahmed, A.; Kumaran, T. Senthil S.; Syed, Abdul Syed & Subburam, S, - Cross-layer design approach for power control in mobile adhoc networks. Egyptian Info. J., 2015, 16(1), 1-7. doi:10.1016/j.eij.2014.11.001

[15] Rath, M. & Pattanayak, B.K, - A methodical survey on real time applications in MANETS: Focussing on key issues. *In* International Conference on High Performance Computing and Applications (ICHPCA), 2014, pp.1-5. doi: 10.1109/ICHPCA.2014.7045301

[16] Pattanayak, B.K. & Rath, M, - A mobile agent based intrusion detection system architecture for mobile adhoc networks. J. Comput. Sci., 2014, **10**(6), 970-975. doi:10.3844/jcssp.2014.970.975