A new approach for DDoS attacks to discriminate the attack level and provide security for DDoS nodes in MANET

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: Mobile Ad Hoc Networks (MANETs) enable versatile hosts to frame a correspondence arrange without a prefixed framework. In military applications portable specially appointed system assumes essential part since it is particularly planned network for on request necessity and in circumstances where set up of physical network isn't conceivable. Despite the fact that it gives high adaptability, it likewise conveys more difficulties for MANETs to battle against malicious assaults. In any case, the property of mobility and excess additionally motivates new plans to outline safeguard procedure. In this paper, we propose a procedure to relieve DDoS assaults in MANETs. Expect that a malicious attacker ordinarily targets particular victims. The attacker will surrender if the assault neglected to accomplish the coveted objectives after a specific length of assaulting time. In our assurance system, we exploit high excess and select a protection node. Once a DDoS attack has been identified, the suspicious movement will be diverted to the protection node. The victim will work typically, and it is sensible to expect that the attacker will stop the trivial endeavors. Through escalated recreation test utilizing NS-2, we have confirmed the viability of our approach and assessed the cost and overhead of the framework**.**

Keywords: MANET, AODV, QOS, MAC Layer, Network Layer, DDoS Attack Mitigation, Redundancy, Protection Node

1. Introduction

Security of Mobile Ad hoc Networks (MANETs) has been an interesting issue in the exploration group. Because of the absence of prefixed physical framework, the dynamic system topologies bring one of kind difficulties. What's more, different issues likewise add to its powerlessness, for example, the open design, shared radio channels, and constrained assets, and so on. Without a reasonable system limit, it is amazingly hard to build up an exhaustive impromptu security technique for MANETs. At present, MANETs are helpless against different assaults including pantomime, message twisting, listening in, Denial-of-Service (DoS), and Distributed DoS (DDoS). These attacks can be generally isolated into two classifications: routing attacks and packet forwarding attacks.

Mobile ad hoc networks [1], [25] 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 keeping in mind the end goal 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.

The objective of routing attacks is to keep real nodes from building the right steering tables. This is regularly proficient by upsetting the foundation of routing tables, redirecting directions of packet sending, or altering the directing data being traded among nodes. For instance, in routing cache harming attacks, two malicious nodes infuse distorted directing message into the system with a specific end goal to pretend that there exists joins [2].

Conversely, the packet sending attacks maliciously infuse intemperate information or control packets into the system that saturate the system interface data transmission and processing assets. The staggering system activity keeps the guiltless authentic clients from getting to organize based administrations. As one sort of DoS assaults, for instance, in hurrying assaults, the malicious nodes continually send steering demands and, henceforth, run out valuable system assets, for example, transmission capacity and CPU cycles [3].

Although different security procedures have been received broadly in wired systems, they can't be connected in MANETs straightforwardly. It is all the more difficult in MANETs to fulfill the basic security prerequisites, for example, data classification, information honesty, and administration accessibility. Research has been led in past decades that try to incorporate security arrangements over secure steering conventions. To date, in any case, it is as yet a progressing research on methods to battle against malicious practices, for example, burrowing attack and DoS [24].

In this paper, we propose a novel way to deal with reduce the effect of DoS or DDoS assaults in MANETs in view of AODV (Ad hoc on request Distance Vector) routing protocol. Our technique, which is named Protection Node based Strategy, depends on two major presumptions: to begin with, the assailant isn't capricious; and second, the MANETs receive a various leveled engineering, and the nodes are ordered into various levels as per their significance. This plan is reasonable to be connected in conditions where bring down level nodes will secure more elevated amount nodes.

Normally, the more elevated amount nodes have higher need, and they are more vital. To accomplish better system benefit accessibility, we will utilize bring down level nodes to secure larger amount nodes. Assurance nodes are chosen to manage malevolent streams, and in the interim, to ensure the victim nodes. Our plan is intended to alleviate DoS or DDoS assaults once they are distinguished. The DDoS assault location issue is past the extent of this paper, and various inquires about have been directed [4], [5], [6].

2. Related work

The exploration in MANETs is an expansive subject covering engineering, directing, and security. Despite the fact that there are many research papers about the DDoS assaults guard methodologies in MANETs [5], [7], [8], this area just gives a concise talk about research that is firmly identified with the possibility of this paper.

MANETs are more powerless against security assaults when contrasted with wired systems because of the absence of an incorporated expert, dynamic system topology, easy eavesdropping, and low bandwidth. Albeit many sorts of security assaults have been examined in MANETs, similar to black hole attack, wormhole attack, jellyfish attack, Denial of service attack, rushing attack, sinkhole attack, Dynamic denial of service attack, however, the most spearheaded assault is a dynamic denial of services assault (DDoS) in view of their potential effect [26].

In light of the methodologies that the nodes hubs adjust to accumulate the directing data, routing protocols in MANETs can be characterized into two classes: on-request directing conventions and table-driven conventions. The notable on-request directing conventions incorporate AODV (ad hoc on-demand distance vector) [9], [25], DSR (dynamic source routing) [10], and TORA (temporally-ordered routing algorithm) [11]. Conventions in this class don't keep in time directing data. At the point when the source node needs to send information to the destination node, it will start a course discovery system to discover a route to the destination node.

The correspondence is done through more than one hop, where packet ventured into through numerous nodes to reach up to the goal. It has numerous attributes like framework less, versatile topology and simple to convey. Ad hoc systems are broadly utilized for applications like gathering, battleground correspondence, get together occasions, in the observing frameworks and fiasco conditions. The principle target of directing towards MANET to locate the ideal course to the goal regarding least delay, the most limited way likewise it should get together some requirement like least power and data transfer capacity utilization [27].

Madhan Mohan & Selva kumar [12] 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 [13] 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 & Pattanayak. Similarly mobile agent intruder detection systems with delay and [14] power issues are analyzed by Pattanayak & Rath [15].

Examples of table- directing convention incorporate include OLSR (optimized link state routing protocol) [16], TBRPF (topology dissemination based on reverse-path forwarding) [17], DSDV (destination-sequenced distance vector routing) [18], WRP (wireless routing protocol) [19], and STARA (system and traffic dependent adaptive routing algorithm) [20]. In this class of routing protocol, each node keeps up at least one routing tables by exchanging routing tables with peers periodically. These tables include all the routing information of the network. The AODV convention is one of the conventions that have been broadly suggested in MANETs, and our technique depends on AODV condition [25].

A DoS attack [24], defense strategy has been proposed by Liu and Shen [21]. In this scheme, every individual node is assigned the duty to supervise its neighbors. Each node arranges its buffer consistently to each neighbor nodes. For instance, if there are N neighbor nodes, each one of them will get 1/N buffer space. In the event that any of them consumes more buffer space than 1/N, succeeding packets will be dropped from it. What's more, each node assigns needs to its neighbors based on the transmission rates. In particular, if a neighbor node sends M packets per second, then its priority value is set as 1/M. A node handles the incoming packets according to the priority values of the senders.

Previously, a strategy had been proposed that is capable of tolerating DoS attacks using a power and delay efficient network [22]. Power and delay networks are proven effective in handling the controller of all functions in the mobile work station to support continued network access. Although this process does not effect for complete node level, we are inspired by the idea to apply the principle in MANETs with protection algorithm to achieve our goal.

3. Power and Delay Optimized Protocol

The main core module in our system power delay optimized AODV protocol [23] 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.

3.1. 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
```

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.

3.2. BIAS-PDDoS algorithm

The 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.

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 assessing the bias and variance of noise for sensor nodes in view of their readings. The variance and bias of a sensor noise can be deciphered as the separation measures of the sensor readings to the exact estimation of the flag. Truth be told, the separation measures acquired as our assessments of the bias and variances of sensors also make sense for non-stochastic errors.

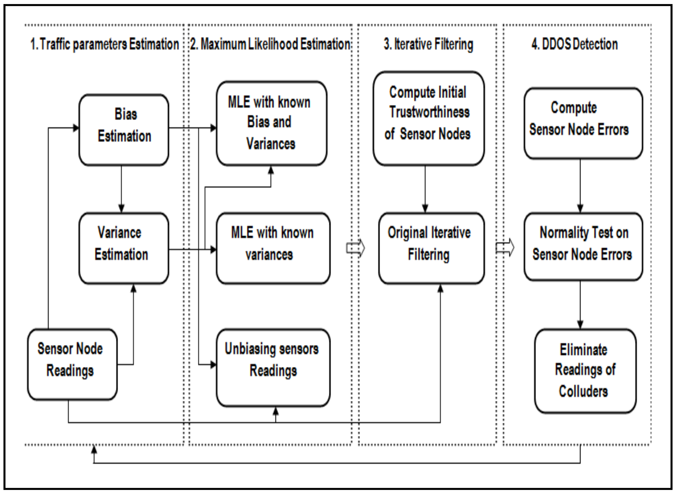

1. Traffic parameters Estimation
2. Maximum Likelihood Estimation
3. Iterative Filtering
4. DDOS Detection
Bias Estimation
Variance Estimation
Sensor Node Readings
MLE with known Bias and Variances
MLE with known variances
Unbiasing sensors Readings
Compute Initial Trustworthiness of Sensor Nodes
Original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

Figure 1. Prevention of DDoS attack framework

4. Proposed algorithm

4.1. Protection node selection

Propelled by the SAODV conspire, we embrace the various leveled arrange design in which the nodes are partitioned into different levels as per their significance. Lower level nodes are utilized to ensure abnormal state nodes. In particular, every node will be appointed a lower level node as its security node, which is named as a goal assurance node or Local Protection Node (LPN). They ensure the objective of DoS assaults. For the most reduced level nodes, a neighbor of a similar level will be chosen as its security node.

Then, at the well spring of the DDoS assaults movement, a node can be utilized to screen the malevolent node.

In our system, when an assault route is manufactured, the node that is the primary bounce from the source node will likewise be doled out as a security node. This sort of insurance node is named a Remote Protection Node (RPN), which is utilized to screen the assault source node. On the off chance that the source node is distinguished as a malevolent one, the packets from it will be dropped by the RPN. What's more, the new RREQ from the malevolent node will be dropped by RPN, as well. Consequently it keeps the DoS assault specialist from setting up another route.

In our framework, each more elevated amount node chooses its LPN when it joins the MANETs. Because of the dynamical system topology, the LPN of a secured node should be refreshed intermittently. Once the LPN node is chosen, it will be embedded into the route whose goal is the ensured node. The LPN will fill in as the last hop before the destination node, and all packets to the destination node will be sent through the LPN. Along these lines, the LPN screens the movement whose destination is the node under security.

4.2. Local protection node (LPN) selection

A three- advance-handshake approach is embraced to discover an LPN for a larger amount node that should be ensured. In the initial step, the more elevated amount node communicates the LPN query packet (LPNREQ) to its neighbor lower level nodes. Once the demand is gotten, the neighbor nodes unset their new labels. At that point ensuing LPNREQ packets from other nodes won't be acknowledged.

In the second step, the recipients send an affirmation packet (LPNACK) back to the sender. This LPNACK message fills two needs: 1) the receiver advises the sender that it will fill in as the LPN; and 2) the arrangement of the LPNACK messages enables the sender to settle on a choice. The generator of the principal got LPNACK packet is chosen as the LPN.

In the third step, the secured node will communicate an LPN affirm (LPNCFM) message. Other than advising the LPN node that it is chosen, the LPNCFM message gives other unselected nodes a chance to reset their fresh tag that enables them to be chosen by different nodes. After the three steps, the ensured node-LPN match can be set up.

Figure 3 represents how a recently chose LPN is embedded into the route as the last hop node goes toward the destination. A source node communicates RREQ to develop the route, and just if the LPN gets the RREQ will the INROUTE label estimation of the RREQ be set. At the point when the secured node gets a RREQ, it checks the INROUTE label first and final acknowledges the RREQ with the set tag. On the off chance that the label esteem isn't valid, the LPN must not be in the route. In the situation that an intermediate node receives a RREQ, but it has a fresh enough route to the destination node, the new route will still be built with the old one in it. Because in the first time the LPN will be included in the route, we can ensure that, when the above situation happens, the LPN will also be included in the route.

4.3. DDoS attack Mitigation

Figure 2 presents a scenario in which LPN protects the victim node of a DDoS attack. The LPN node filters all the attacking packages in the traffic whose destination is the victim. In addition, the LPN recognizes the source IP addresses corresponding to the malicious traffic, and an Attack Notification Message (ANM) is sent to the victim node. The ANM includes the source IP addresses of involved malicious attack agents. Then, the victim node broadcasts an Attack Information Message (AIM) packet towards the remote protection node (RPN). With the information in AIM, the RPN nodes filter off all the malicious packets at the source side. This mechanism aims to recover the service for destination protection node and to tell every other node to drop the RREQ from the malicious node. After doing this, the malicious nodes cannot send out traffic or build a route.

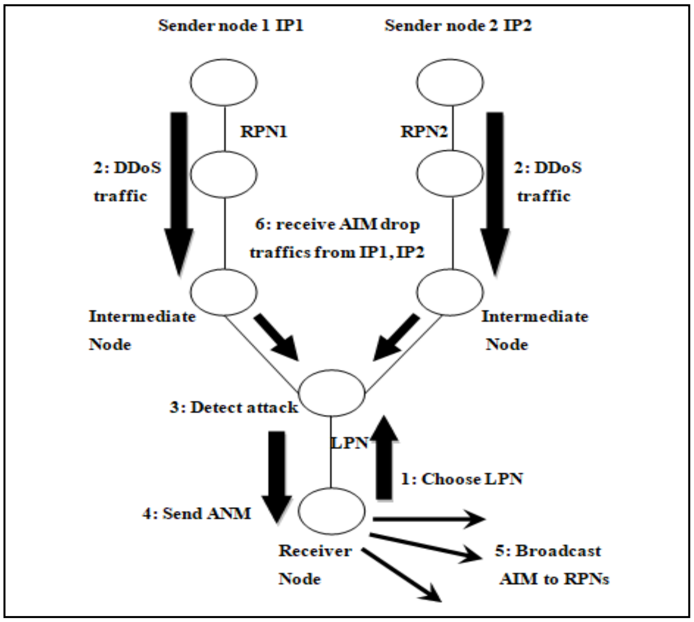


Figure 2. Process of defending DDoS attack

Essentially, this protection node-based DDoS attack mitigation approach is a trade-off of the redundancy in the route for higher system availability. The false positive alert leads to impact on throughput of legitimate traffic while it blocks the malicious traffic efficiently.

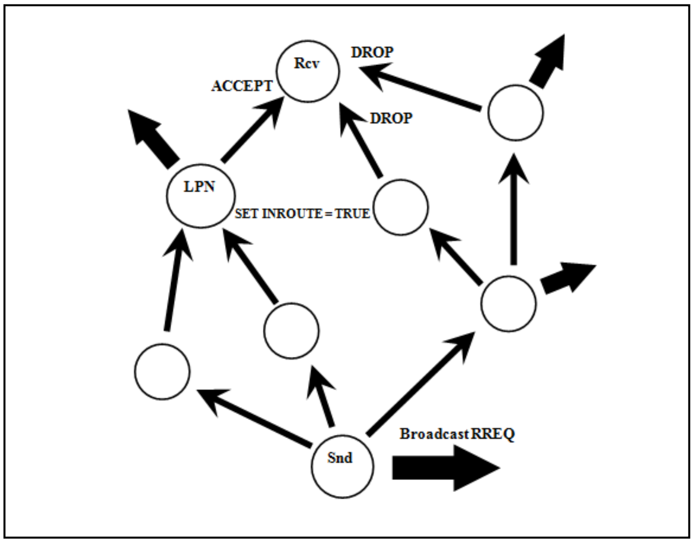


Figure 3. Process of adding LPN to route

5. Experimental study

5.1. Experimental setups

Our experiments are conducted using the NS-2 simulator. We conducted the experiments in two steps. The initial step is to check the viability of our plan, and then deeper study is investigation is done to assess the cost and overhead in more detail.

In the first step, there are 25 mobile nodes in the network, and four nodes are sending traffic concurrently to the same destination node. None of the individual traffic rate goes beyond a certain threshold, but the sum of them does. Another malicious node will send traffic to the same destination after 600 ms to check if the soft state of the protocol can go back to the initial status. Then it will be able to react to new attacks properly.

All of the nodes randomly move at an average speed of 10m/s. The simulation time is 8000 ms; three malicious nodes send their traffic at 7004 ms, and another malicious node sends traffic at 7068 ms.

The connections among mobile nodes are UDP connections, and we send CBR (Constant Bit Rate) traffic in each communication channel. The CBR rate of the connections is 512Kb/s, and the threshold of the agent is 1.5M/s, so two nodes sending the traffic to the same destination node will not cause an alert but three nodes will. The size of the scenario field is 1000m x 500m. The queue drop mechanism is tail drop. The routing protocol we use is a revised AODV routing protocol that integrates our LPN, RPN methods. The LPN re-select interval is 200 ms.

In step two, we assess the execution of our new DDoS attack mitigating scheme in a different network scale. The configurations of different network scale are shown in Table 1. The traffic of node is applicable to our network process.

Table 1. Network scale configurations

Node number	Field size (mxm)	Number of high level nodes	Number of connections
2	200x100	1	2
4	350x250	2	4
8	600x500	4	8
16	1000x500	8	16
32	1200x1200	12	32

Five metrics are adopted to conduct a comparison study between our protection node-based DDoS attack mitigation approach, Bias variance mechanism and the original P-AODV protocol with formation of DDoS. The main purpose is to check how much overhead has been caused in order to mitigate the DDoS attacks. The five metrics are defined as below:

Packet propagation delay: average time for one packet to propagate from the source node to destination node.

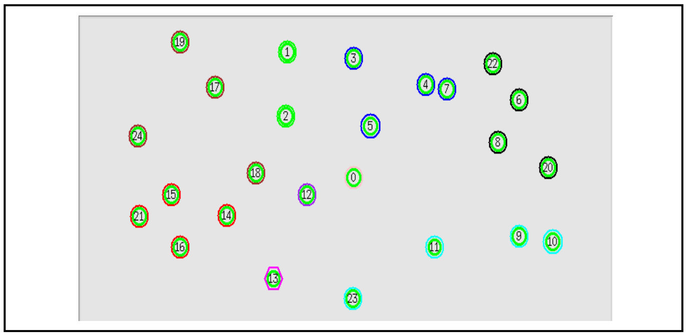


Figure 4. The Network Topology

Packet drop rate: drop rate of packet in the whole simulation.

Energy levels of node: the energy level of nodes uses per second.

Network routing load: the number of other control packets that transmitted for transmit one data packet.

Network performance: the number of transmitted packets calculated Mega bits per sec

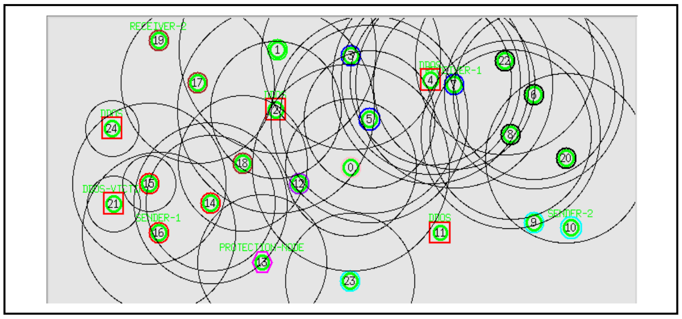
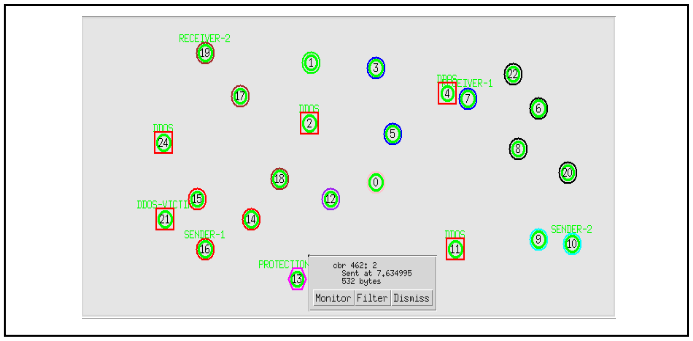


Figure 5. The Protection node is broadcasting AIM packet



cbr 462: 2
Sent at 7.634995
532 bytes

Figure 6. The packets are diverted into protection node

5.2. Result analysis

The first experiment is used to verify the effectiveness of our strategy from the perspective of DDoS attack mitigation. And the second step is conducted to evaluate the cost, particularly the performance of network process compared to the P-AODV protocol and Bias-variance process.

5.2.1. Verification of effectiveness

In the first experiment, 25 nodes are randomly generated, and one of the topologies is shown in Figure 4. Four malicious nodes that send attacking traffic are node 2, node 4, node 11, and node 24 that are marked in red. All of them send attack traffic at almost the same time. The destination of all the traffics is node 21, a high level node, which is marked in red as the DDoS attack victim.

During the simulation, the LPN of this victim node is node 13, which is marked in magenta. The RPNs that dropped the traffic of malicious nodes are marked in blue, which include node 3, node 5, node 9, and node 18. The LPN sends ANM packets to the victim node, which broadcasts AIM packets to the entire network as shown in Figure 5. The RPN nodes that are allocated close to the malicious nodes filter off the attacking traffic. All the other nodes will record the malicious IDs and then drop all the packets sent from the malicious nodes. Therefore, during the simulation, we have observed that the malicious nodes have tried to rebuild the route many times, but the neighbor nodes never accept their requests.

The impact of malicious node on neighboring nodes during source node sending packets to destination node is avoided by diverting packets into protection node. Figure 6 presents diversion of packets into protection node.

The simulation results have verified that our protection nodes are capable of mitigating the DDoS attacks and allowing the victim node function normally. In addition, it has also shown that the protocol can recover and return to its initial state after handling a DDOS attack.

5.2.2. Performance analysis

Figures 7 to 9 present the experimental results of the three performance metrics measured on our new protocol, original P-AODV protocol and Bias-variance mechanism. The lines with green color present the performance of new routing protocol, while the lines with red color present the performance of modified AODV as Bias-PDDoS protocol and blue color present the performance of PDO-AODV protocol.

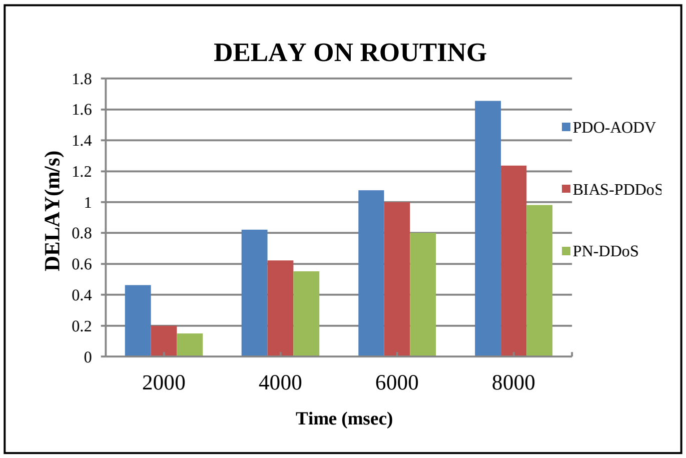


Figure 7. Delay time in network

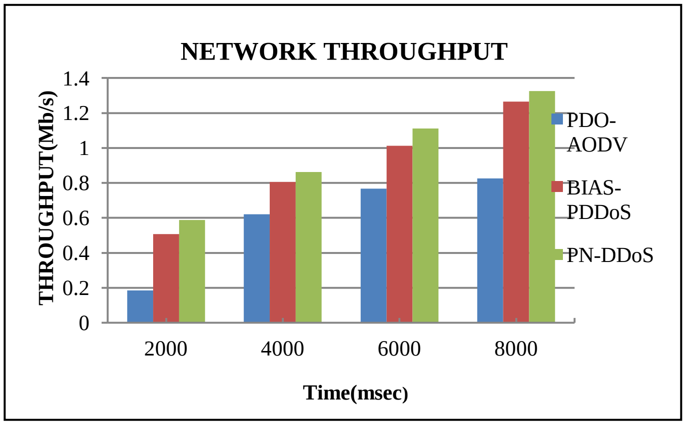


Figure 8. Throughput of network

The experimental results have shown that our DDoS attack mitigating protocol does not bring significant overhead to the performance of network. Meanwhile, Figure 7 shows that the delay is a little higher when the node acts as DDoS node. When a normal node wants to communicate with a high level node, it will buffer some packets first and then start the route discovery process. As one high level node only has one LPN at certain time, the broadcasted RREQ may spend more time finding it and will include it in the route. For instance, in our experiment, the RREQ traversed around almost half of the network to find the LPN. As a result, the first buffered packets will be delayed for a longer time before getting to the receiver. With the increase of the number of high level nodes and network scale, the probability of this situation increases and its effects on average delay are more obvious.

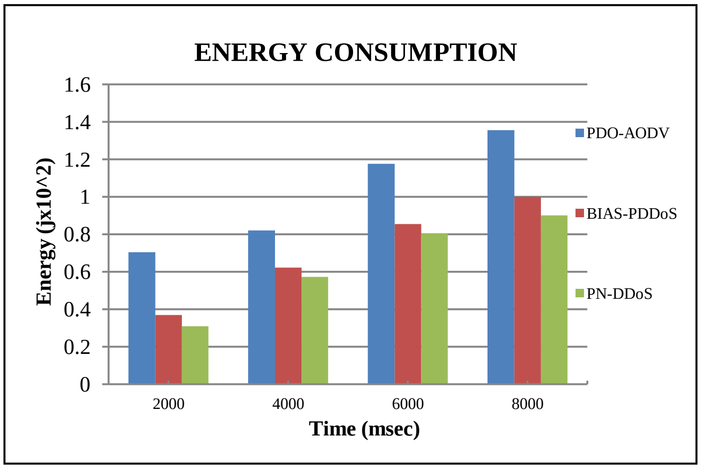


Figure 9. Energy consumption in network routing

Our protocol does not affect the less number packets delivered per minimum time interval. Figure 8 shows that, before data delivering check the all nodes RREQ and RREP, the network throughput remains as high as the Bias-PDDos and PDO-AODV protocol while the network scale grows. Figure 9 shows that, individual node energy levels based on network routing process and routing levels more efficient it will be effect to process of attack levels.

Table 2: Simulation parameters

PARAMETER	VALUE
Application Traffic	CBR
Transmission rate	100 packets/sec
Radio range	250m
Packet size	512 bytes
Maximum speed	25m/s
Simulation time	8000ms
Number of nodes	25
Area	1000x500
DDOS nodes	4
Maximum number of packets	10000
Protection node	1
Routing protocol	AODV

In summary, the experimental results show that our DDoS mitigating strategy is capable of protecting the victim node and isolating the malicious attacking agents. The cost is small, and there is not significant impact on the performance of the network. In fact, in order to examine the performance in extreme situations, we made all the traffic connections high level node related. Therefore, the performance must be better for normal situations in which there would be connections between normal nodes.

6. Conclusion

This paper presents a novel strategy that protects critical nodes from DDoS attacks in MANETs. Considering the different roles that certain nodes play in a MANETs, it is assumed that there are some important nodes that should be protected with higher priority. Lower level nodes would be allocated as protection nodes to handle the incoming traffic to the higher level nodes.

Through intensive simulation experiments using NS-2, we proved that every functionality works well, and DDoS attack can be mitigated effectively. We compared different parameters in routing as existing mechanisms with proposed protocol. We have also evaluated the cost of the protocol, and the results are encouraging. The overheads are small to implement the DDoS mitigating scheme on top of the well known AODV protocol. This paper presents the initial results of our work. More comprehensive studies are being conducted, including the impact of different setting of LPN updating period, the assignment of LPNs in multi-level networks, etc. More results will be reported in our future papers.

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] K. Sanzgiri, B. Dahill, B. N. Levine, C. Shields and E. M. Belding-Royer, “A Secure Routing Protocol for Ad Hoc Networks,” the 10th IEEE International Conference on Network Protocols (ICNP 2002), Paris, France, Nov. 12 - 15, 2002.

[3] Y.-C. Hu, A. Perrig, and D. B. Johnson, “Rushing Attacks and Defense in Wireless Ad Hoc Network Routing Protocols,” ACM Workshop on Wireless Security (WiSe), San Diego, California, September 2003.

[4] I. Aad, J.P. Hubaux, E.W. Knightly, “Impact of Denial of Service Attacks on Ad Hoc Networks,” IEEE/ACM Transactions on Networking (TON), vol. 16 (4), pp. 791-802, 2008.

[5] A. Nadeem and M. Howarth, "Adaptive Intrusion Detection & Prevention of Denial of Service Attacks in MANETs," International Conference on Communications and Mobile Computing, Leipzig, Germany, 2009.

[6] W. Ren, D.-Y. Yeung, H. Jin, and M. Yang, “Pulsing RoQ DDoS Attack and Defense Scheme in Mobile Ad Hoc Networks,” International Journal of Network Security, Vol. 4, No. 2, Mar. 2007.

[7] M. Alicherry, A. D. Keromytis, and A. Stavrou, "Evaluating a Collaborative Defense Architecture for MANETs," *IEEE Workshop on Collaborative Security Technologies* (CoSec), December 2009.

[8] M. Carvalho, "Security in Mobile Ad Hoc Networks," *IEEE Security & Privacy*, March/April 2008.

[9] C. Perkins, E. Belding-Royer, and S. Das, “Ad Hoc On-Demand Distance Vector (AODV) Routing,” *RFC 3561*, July 2003.

[10] D. Johnson, Y. Hu, and D. Maltz, “The Dynamic Source Routing Protocol,” *RFC 4728*, Feb. 2007.

[11] V. Park and S. Corson, “Temporally-Ordered Routing Algorithm (TORA),” draft-ietf-manet-tora-spec-00.txt.

[12] 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

[13] 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

[14] 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

[15] 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

[16] T. Clausen and P. Jacquet, “Optimized Link State Routing Protocol (OLSR),” RFC3626, Oct. 2003.

[17] R. Ogier, F. Templin, and M. Lewis, “Topology Dissemination Based on Reverse-Path Forwarding (TBRPF),” RFC3684, Feb. 2004.

[18] C. E. Perkins and P. Bhagwat, “Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers,” ACM SIGCOMM Computer Communication Review, Vol. 24, Issue 4, Oct. 1994.

[19] S. Murthy and J. J. Garcia-Luna-Aceves, “An efficient routing protocol for wireless networks,” Network and Distributed System Security Symposium (NDSS), San Diego, California, February 2003.

[20] P. Gupta and P. R. Kumar, “A system and Traffic Dependent Adaptive Routing Algorithm for Ad Hoc Networks,” the 36th IEEE Conference on Decision and Control, San Diego, California, Dec. 10 -12, 1997.

[21] Y. Liu and L. Shen, “Defense of DoS Attack Focusing on Protecting Resource in Mobile Ad Hoc Networks,” Computer Knowledge and Technology 2007 3(16), 2007.

[22] jhum swain, binod kumar pattanayak and bibudhendu pati, “Mitigating the DdoS attacks using PDDoS efficient networking protocol in MANET for Military applications” IJRECE, Vol.5, Issue 3, July-Sep-2017.

[23] 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.

[24] R.Kavitha, Dr.G.Padmavathi, “Advanced Random Time Queue Blocking with Traffic Prediction for Defense of Low-rate Dos attacks against Application Servers”, IJCNIS, Vol.9, No.1, April 2017.

[25] Moussa Ali cherif, Sofiane Boukli Hacene, “An Energy-Conserving Predictive Preemptive Multipath Routing Protocol for Adhoc Networks: A Lifetime Improvement’, IJCNIS, Vol.8, No.1, April 2016.

[26] Bhavin Joshi, Nikhil Kumar Singh, “Mitigating dynamic Dos attacks in mobile ad hoc network”, Colossal Data Analysis and Networking (CDAN), Symposium on, IEEE conference, 18-19 March, 2016.

[27] Parveen Kakkar, Krishan Saluja, “Performance investigations of reactive routing protocols under flooding attack in MANET, Computing for Sustainable Global Development (INDIAcom), international conference, 16-18 March, 2016.