I J C T A, 10(20), 2017, pp. 83-95 ISSN: 0974-5572

Enhanced Transmission Based Channel Allocation over Backlog Attack in Manet

S. Kannan* and A. Rajaram**

ABSTRACT

Mobile Ad hoc network is an indivisible part of network where it has no infrastructure. In the past, Intrusion detection systems were used to detect intrusions in network effectively. Most of the systems are able to detect intrusions with high false alarm rate. In this paper, presents a Transmission based backlog Detection System (TBDS) for detecting malicious activities and providing authentication for packet transmission. Check whether node is true or fake node based on packet transmission, removes the fake node. Resource allotment based backlog detection is also presented for identifying and separating the backlog nodes in network. Throughput is also enhanced with the proposed TBDS with resource allotments to provide an efficient data transmission and message authentication. Simulation results shows that the TBDS provides minimized energy, minimum delay, improved network lifetime, increased efficiency, lesser packet loss rate and improved Throughput.

Keywords: Secure based backlog Detection System, Resource allotments, Energy, Packet loss rate, Throughput, Network Lifetime.

1. INTRODUCTION

MANET-Mobile ad hoc Network mobile nodes are move around in entire network, and dynamically updated its position in every time, it allows the nodes to exchange information using wireless infrastructures. Each and every node has a different behavior, causes lot of security issues for packet transmission. In previous attacks are gathers data packets during transmission and tries to launch another target in available network environment. Initially analyzing the behavior of each node and achieve certain reaction to the process of output. Sometimes attacker causes a packet loss during transmission, consider the quality of loss for packet transmission, and also cause overload packet that consume resources. For the duration of packet loss, intruder needs to modify in network, rejection of repair attack crack the network build a floods to damage TCP, UDP transmission support protocols in MANET, proposed a interruption detection algorithm. Quality of service, falls the packet is a vital DOS attack in Mobile Networks. Injuries have an effect on the high rate and reaches poor quality of result. Recent days a new attack called the shrew attack or quality dropping attacks is identified. Shrews injuries regularly minimize the result worth by strangle the TCP transmission rate a lot as an alternative of completely varying the clients form the route. Alternate of limiting its stable state capability, distinction minimizing injuries targets the systems adaptive routine. Transmitter and receiver IP spoofing are used by quality reducing intrusion. Quality reducing attacks are commenced all the way through multiple grouping and varying header packet in sequence, so that they can get away from trace back methods. In fact it is required to control the occurrence of injuries transmission. During attacking time, need to RTO –retransmits time out the packet, so that TCP-Transmission control protocol transmissions are not worthy [1].

Transmitter node IP addresses of the packet header are false, attack detection techniques are fatalities energy in packet overload. TCP-Transmission control protocol synchronizing the overflow injuries depends

* Research Scholar, Anna University, Chennai, India, *Email: kannan340@gmail.com*

** Professor, Department of Electronics and Communication Engineering, EGS Pillay Engineering College, Nagapattinam, India, *Email: gct143@gmail.com*

on use normal TCP link for three ways. Recipient once gather initial synchronization request from a transmitter node, receiver sends back an organization acknowledgement packets and waits for the final acknowledgement packet from transmitter. Target node relives coming up time for the fixed acknowledgement. Target node has imperfect buffer file for new links, neighbor node forward request packet is not maintained. Receiver is in middle stage of connection it waits for acknowledgement from sender. There are three way handshakes in TCP. In that situation, the receiver will need to whole the three-way greeting by retransmitting packets. Major goal is to reduce the break caused by network jamming and to enhance the network trustworthiness. Regular middle-open links are caused by network jamming else any irregular performance of networks. Irregular middle-open links are those which can be experimental on a receiver during DDoS attacks. Authentication key problem is to distinguish the irregular middle-open link from the normal middle-open link so that the irregular link can straight away be detached to use receiver resources. Well-known, the majority normal middle-open links arise from network jamming whereas irregular half-open links have no relevance to reduce interchange delay in network.Present work contains five sections are organized as follows: Section 2 presents the many works done and connected to the attacks discovery in Section 3, Present method Transmission based backlog Detection System (TBDS) detailed in this section. The network environment, simulation output analysis is presented in Sections 4 and the paper concluded in section 5.

2. RELATED WORK

Chang, et al. [2] proposed to select those kinds of problems by protocol a dynamic source routing-based processing techniques, then believe the CBDS Cooperative bait detection method, to merges the reward of both active and automatic protection architectures. In CBDS contains backward tracing method to attain an efficient report. Model information is providing, examine the misbehaving-node attacks present or not, the CBDS processing the dynamic routing, two acknowledgement, and BFTR-(Best effort fault tolerant routing protocols). Communication overhead is reduced and transmission rate is improved. Examine the option of changing present CBDS method to denote different kinds of combined attacks on mobile networks and then examine the combination of the CBDS with other well-known message authentication in order to build a complete secure routing structure to defend mobile network against attacks.

Gupta, et al. [3] presents SDN-Software Defined Networking could secure deployment and group of military uses reduce the communication cost and enhance a protection. Routing load of UAV networks move further than the needs of Mobile networks. Protocols are essential to turn into familiar to maximum velocity, dynamic topology updating, irregular links, energy usage and changing link worth. Present scheme gets unsuccessful and the network may get opening causes some packet latency and trouble progressiveness a vital design consideration. Imperfect existence of the node and changing of the network improves to the condition of imperfect given over researchers are centre at the process of mobile infrastructure. Energy consumption of UAVs is incomplete; some rules used in different layers should give in the various ways of the system. It construction efficiently enhance the multi UAV networks compared to previous works.

Wei, Zhexiong, et al. [4] presents guarantee from direct watching from a monitoring node, the hope value is artificial using Bayesian deduction, nodes changing their location in mobile infrastructures. An additional, not direct watching, is named as next-offer in sequence is taken from nearest neighbour nodes of the monitoring node, the unique value of node is fake using the DST- Dempster Shafer theory, it different kind of unsure analysis while the plan of attention can be copied by an not direct method. Integration the two mechanisms, success perfect results values of the simulation mobile nodes in mobile infrastructure. Nodes have least hope values can be occupied by the routing algorithm. Secure routing path can be identified by faulty network condition. Accessible method provides, additional correct trust can be obtained by allowing for various kinds of packets, indirect study from one-hop neighbours to other node, and it contains buffers of queue stores efficient data packet about nodes. Sometimes neighbour nodes loss packets.

Wang, Yanwei, et al. [5] this way can permit a alone node in mobile network to take improved safe protection decisions. Safety protection scheme consume so much of energy for all communication. It not only follow protection also regard as energy, packets are collected with efficient way. Proposed game theoretic methods for choose the node for communication in MANET. Minimum ability nodes obtain losing packet through a communication such nodes are faulty nodes. Huge count of attackers makes a delay but provide an efficient communication.

Paolo Bellavista, et al. [6] continuous packet delivery rate, proposed a unique output to join together and opportunistically exploit mobile ad hoc networks overlay, impromptu, and collaboratively formed against WSNs, to increase count of nodes for huge count of packet collection. Focus efficient solution for Intelligent Transportation Systems like sensor traffic sensor, and indoor smart spaces. It considering many organization operations: Energetic movement of nodes in various angles among the mobile infrastructure.

Bala, Laxmi, et al. [7] proposed a bottom up method to discover and prevention scheme the intruder such as DDoS in mobile network, presents an efficient worth of check for network, attack prevention. Throughout broadcast synchronization flooding attack that damage an entire routine of network. The Time to be minimized since so much of delay occurs during broadcast for route path allocation, which affects mostly the worth of service in network communication. Intruder nodes forward the packet to target and immediately receive reply message from target node like immediate acknowledged. The client node gives request packet the IP spoofing traces the Node acts likes a true to collect information's redirecting routing. Fault identification algorithm is used to find the attacks occurred in mobile infrastructure.

Liu, Wei, et al. [8] Present the original certificate revocation; present the CCRVC- to perform Cluster based resource allocation with justification Capability method. In particular, to enhance the reliability of the scheme, to get well fake nodes to take part in the certificate revocation process; to improve the accurate packet communication the fixed threshold value -based mechanism to evaluate and give good reason for warned nodes as rightful nodes or not, before improving them. The output of our scheme are evaluated by both numerical and simulation performance. Result indicates the certificate revocation is effective and efficient to organize protected communications between mobile nodes in network. New incentive method goes and recovers the rightful nodes, to improve the security for all mobile nodes. Use minimum possible nodes for efficient with immediate revocation. Best in revoking certificates of misbehaving attacker nodes, minimize the revocation time, and increases the accuracy and reliability of revocation report.

Marimuthu, et al. [9] proposed a mechanism called EOLSR-enhanced OLSR protocol, to keep the nodes from attacks with the OLSR scheme. This scheme is able to check the node is attacker else a true node or not by verify its Hello packets is used find the attacks in network. The experiment output shows protocol is able to achieve efficient routing with safety, improves in packet delivery ratio and minimizing packet loss rate. OLSR uses an easy authentication scheme of hello packets coming from neighbour nodes to find the malicious nodes in the network. Experimental reports notify large number of Packet received over the multiple attacker nodes in network.

Elhadi M. Shakshuki, et al. [10] presents the subject to intruders. Launch an efficient intrusion-detection scheme to protection a network from intruder. Changing a recent method is vital for believe it is possible protection issues. Proposed a new intrusion-detection system named EAACK-Enhanced Adaptive Acknowledgment particularly constructed for mobile ad hoc networks. Reply message has been huge count of misbehaving node identification rates in particular network form. Proposed scheme enhances a packet delivery ratio, attacker imitation the acceptance. DSA and RSA scheme provides exchange keys between nodes improves a network safety.

Guan, Quansheng, et al. [11] presents verification and topology control issues depend on throughput factor. Multi path is used for packet communication in network due to increasing security. Elevated level protection methods are used to find the misbehaving nodes available in network infrastructure. Changing

the state of channel in particular position at every time, this high level security protocol is constructed to improve the energy consumption of all nodes in network. Lacking channel information's are recognized and separate from a network; create a new routing for transmission.

Zhao, Shushan, et al. [12] presents an IBC protection uses in mobile ad hoc networks based on a study the appearance of IBC in 2001. Proposed also split insight into, future improvement of network and open research problems. IBC wants the experimental metrics be spread to all communicate users earlier to any messages can be encrypt or decrypted. It indicates the trustiness of mobile ad hoc nodes main opportunity of network. In those networks, combination intruders come jointly lacking any central node in control of the management and the group of the mobile network. Controller of network can authenticate the individuality of a node, and assign initial private key to it. Mobile ad hoc network that get together these needs, e.g., sensor networks, military se wearable mainframe, forwarding message systems for future public protection, urgent position and disaster applications, IBC is the most capable protection answer, but there seem no perfect outputs up till now.

Gang Xu, et al. [13] presents a Multi instance of a request association on different nodes busy in message only if these nodes place into result the same rules for both the purpose and underlying set of rules used by direction-finding. Nodes can form trusted uses centric networks. Earlier to allow a node to put in to such a mobile nodes, Satem verify its check true node with set of policy. With Satem protects the policy and the Software put into effect these policy from being tampered with node is compromise; Satem filter out the node from the network. In uses of the upper tier depends on the lower tiers to exchange information. Only secret nodes are authorized to add the network. Furthermore, exchange message between them is regulated by the rules at every tier. To make sure trustworthy rules enforcement, enhancement each node with a trusted essential part agent depends on the TCG TPM schemes.

Karim El Defrawy, et al. [14] it presents concentrate on a large number of issues are created in doubtful location tracking in mobile network set up and find a privacy-preserving and protected link state based routing policy. In ALARM finds the current position of each and every node in a network environment. In RSA cryptography method provides a safety in enhance key based approach. ALARM gives on group signature to construct an algorithm for position based packet transmission. It reduces the packet overload to find in different velocity model also provides an improved protection schemes.

Nitesh Saxena, et al. [15] Proposed a power-aware and fully minimum interactive self-certification policy based on bi-variate polynomial secret operation and a not inter converse certain fixed cross. Cost of the routing path is approximate with minimum level in mobile nodes. Totally non-interactive self-certification policy improves the network lifetime, mixture of bi-variate polynomial covert contribution and certain fixed BLS signature technique. B-BLS is improved ordered enhances communication, and energy consumption is reduced.

3. PROPOSED BACKLOG DETECTION SYSTEM

3.1. Monitoring Backlogs in Network

In MANET nodes are communicated with its updated position based on time that randomly moved in environment, radio range is important one for node communication, so monitor the coverage and connectivity range between nodes. Bandwidth of node is very low to the data packets transmission is slow for each time slot. Time allocation is main aim for communication in network, source node choose a channel for forward packet to reaches destination node. Destination gives the reply message if it successfully received. If any packet missing go to retransmit the packets through channel is very difficult to achieve the security channel allocation.

Network nodes are willing to transmit packets through neighbor node choose the channel not consider any attacks, does not analyzing the behavior of node. Mobility of the node is varied that also make a

attacks, more number of packets are pending transmission to destination node, Such a statement is then generate throughout the entire network, because the attacker node will be certain limit of the network.

It provides a wireless or connection less transmission medium, So there is not fully support the packet delivery, ordering and duplicate protection of packet transmission. Some bits are added to packet frames finally they are checked. There is no initial setup for channel allocation and they are performed communication using that channel. During transmission, packet is in waiting stage that causes the backlog attack. In waiting stage of packet indicates a delay time increased for every process.

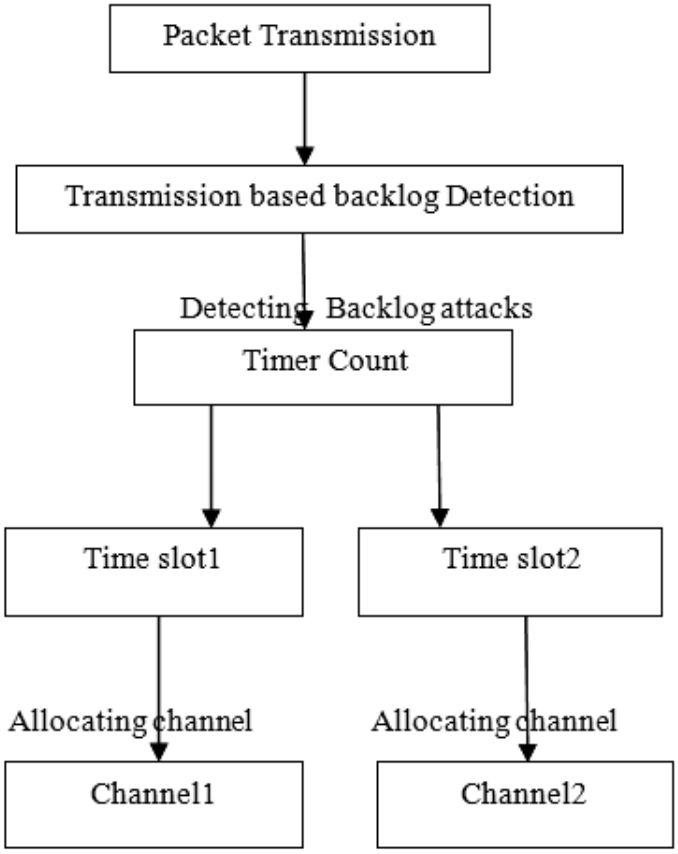

Figure 1: Block Diagram for Transmission Based Backlog Detection system

In Figure 1 shows the block diagram of Transmission based backlog detection system source node transmit packet to nearest neighbor node same time receives the acknowledgement is reply or error packet send to source from neighbor node. Timer count will be incremented for every slot, in particular time packet yet not transmitted, backlog is detected. Finding a new efficient channel for packet transmission based on time slot measurement. Allocate channel to obtain enhance communication over backlog in Mobile ad hoc Network.

3.2. Timer count Measurement

Source node sends packet to destination when its timer is set to add up the every slot, if it slow the heavy traffic occurred for transmission, receiver sends the acknowledgement packets then completely received request packet means receiver gives reply packet else it gives error packet, because not full packets are received within particular time. Present the Timer fixed in node count slots performed to reach threshold level it success. Otherwise choose the higher bandwidth node in channel selection to transfer packet.

Source node select the neighbor node in channel randomly with considers only distance (radio range) without consider any conditions like fake node, low energy node. Radio range is common for all present in

the network. All nodes are not having a constant energy, after the process nodes go to minimum energy level. Packets are forwarded through channel visits the every node timer starts and transmission finished timer stops. Packet size is high that gives the delay time is increased, more time is consumed for process. Maximum numbers of packets are pending for each transmission.

$$SOt = \alpha.SOt\ -1 + (1-\alpha).\ m + (1\ -\alpha\text{^}2) \tag{1}$$

$$DEt = \alpha.DEt\ -1 + (1\ -\alpha).\ m + (1\ -\alpha\text{^}2) \tag{2}$$

where SOt source node process start time and DEt destination node process end time, m is a range, α is a random parameter and a one of standard deviation. SOt and DEt are derived to find the time taken for each transmission.

Receiver node finds the attacks using Timer count measurement techniques presented in network. It continues up to reaches the end of network with centralized infrastructure, first focus the attacks available in channel find and disconnect the attack. Next, focus how securely transmits packets on allocated channel. Every time slot timer on and sends packets, individually focused until completely received packets.

1. Allocate Rxs and Txs queue memory- packets are forwarded in queue format; they are temporary maintained in queue buffer.
2. For each transmission pending packets are loaded into Queue buffer that causes the traffic, overload occurred in communication.
3. Nodes are appears in near of node presents in network, null channel allocations are very difficult one. Each channels having a different behavior.
4. Channel behavior are analyzed depends on transmission rate and energy usage for every time slots.
5. This output was clearly tells backlog occurring reasons based on traffic occurrence and time slots for every transmission.
6. Process is completed to destroy the timer to start a new packet transmission in another channel, it visit every node in a channel.
7. Nodes periodically exchanging the timer information through beacon frames in time synchronization. Each node in an IBSS-Independent Basic Service Set accepts a received timing if it is older than the nodes own TSF timer.
8. All nodes maintain a TSF timer counting in increments of microseconds in every transmission. Each nodes in the IBSS compete for beacon transmission every a Beacon Period time units. This time period is called a BP-beacon period.
9. At the beginning of each BP, there is a beacon message consisting of w + 1 slots each of length a Slot Time. Each node calculates a random delay uniformly distributed.
10. Whether a beacon reaches before the random delay timer has out of range, node rejects the waiting beacon transmission and the residual random delay time.

$$T = Trec + \{Tn - T0/2\} \tag{3}$$

Where T is Total time taken for communication, Trec is Time for receiver, Tn is end time and T0 is start time of transmission. This equation is used to Find the overall time consumption to end the process.

3.3. Transmission based backlog Detection System

Source node transmits a packet to destination node, through the channel. If currently allocated channel gets failed to go for another channel. Channel failure is caused by backlog attack; more number of packets is waiting in queue format overload occurred, the routing protocol wants to choose not only the optimal path

in-between different nodes, Also have the highest suitable communication channels on the path. Common-layer design contains a requirement because changes in routing channel in mobile node. It considers normal mobile networks that handle efficient channel.

The Network consider as all network node in equal manner. This report may not be efficient for MANET, because routers in MANET backbone and sender have differentiated the mobility and constraints. Packets are efficiently transmitted routing protocols that take into channel these differences are desired for MANETs. In sender node every request packet get transmitted, received the acknowledgement packet from receiver node. End to end connection established using TCP protocol, this process is repeated until all are channel allocated to Transmission.

If backlog attack occurred that goes to another path in network, every time slots same timer is maintained to detect and remove that type of attacks. Heavy load makes a trustless packet transmission; node routing table is maintained all information's about transmission. The loaded information updated every time during transmission acts like a buffer. Network lifetime have minimized any backlog attack occurred. The source and destination have CBR-constant bit rate traffic is used for every transmission.

$$Ttr = Tend + Treply + Trequest \quad (4)$$

Where Ttr is transmitting and receiving packet time, Tend is total packet transmission end time, Treply is Transmission reply packet start time, and Trequest is start time for Transmission request packet. Overall total Transmitting and receiving time is estimated based on its time slot during packet transmission. Packets are transmitted in every slot time that kind of data's are stored in buffer Queue.

Algorithm for Transmission based backlog Detection

For each channel

For each connectivity

If(Channel==Connectivity)

Send all packets through this channel //after //sending packets no other //channels are checked

If(channel==Time slot)

S-> Packet

Packet->channel 1

while(channel==failed)

channel++

// Increment the channel upto achieve best connectivity between nodes

Packet->channel n

Channel n->Packet

Packet->Destination

End while

End If

End If

If (Channel!=Connectivity)

S->null

Null->channel

No channel found

End If

End For

End For

In Transmission channel get failed allocate a new channel for communication, and then rechanneling method is apply to this proposed TBDS technique. New Channels are allocated and time slots are noted to establish the network connections, choose an efficient path for packet transmission, to reduce the energy usage. Network has a lot of connectivity channel time slots of each request packet transmission, and reply acknowledgement packet transmission, and reply error packet transmission taken time is calculated for all available channels in a network. The new updated channel is also checked to provide a efficient channel.

Packet ID: It contains individual identification information of a mobile node. It consists of a node's location and random movement identification in which it is deployed.

$$Node\ IDn = \{Xposition, Yposition\} \text{ where } 1 \leq n \tag{5}$$

Source ID	DestinationID	Queue Buffer	Rechanneling	Energy usage	Time slot checking
2	2	4	4	4	2

Figure 2: Proposed Packet format

In figure 2: the proposed packet format is shown. Here the source and destination node ID field takes 2 bytes. Third one is Queue Buffer. The transmission of packets is travelled through selected channel that kind of information's are stored in queue buffer and it provide the first packet input as first packet output. In fourth field, the rechanneling is indicated. It determines how long the channel works for packet transmission between source and destination node. It also finds a channel condition it is efficient or not, efficient means choose a particular channel. In fifth, the energy usage is allotted to ensure minimum energy consumption. The last filed Time slot checking how much time taken to transfer the particular packet detection of backlog attack and find a new channel maintenance process.

6. PERFORMANCE EVALUATION

6.1. Simulation Model and Parameters

The proposed TBDS is simulated with Network Simulator tool (NS 2.34). In our simulation, 100 mobile nodes move in a 1000 meter × 1000 meter square region for 50 milliseconds simulation time. Each Mobile

Table 1
Simulation Setup

No. of Nodes	*100*
Area Size	1000 × 1000
Mac	802.11
Radio Range	250m
Simulation Time	100 sec
Traffic Source	CBR
Packet Size	150 bytes
Mobility Model	Random Way Point
Protocol	DSR

node move randomly, with varied mobility around the network environment. All nodes have the same transmission range of 250 meters. The simulated traffic is Constant Bit Rate (CBR) provides a constant speed of packet transmission in network. DSR- Dynamic source routing protocol is used to allocate dynamic channel for communication. In simulation settings and parameters are summarized in table 1

Simulation Result: Figure 3 show that the proposed TBDS method allocate channel is an efficient one compared with existing CBDS [2] and OLSR [9]. It enhances throughput to detect the attacks occurred in network, and also reduce the energy usage during transmission based on TBDS.

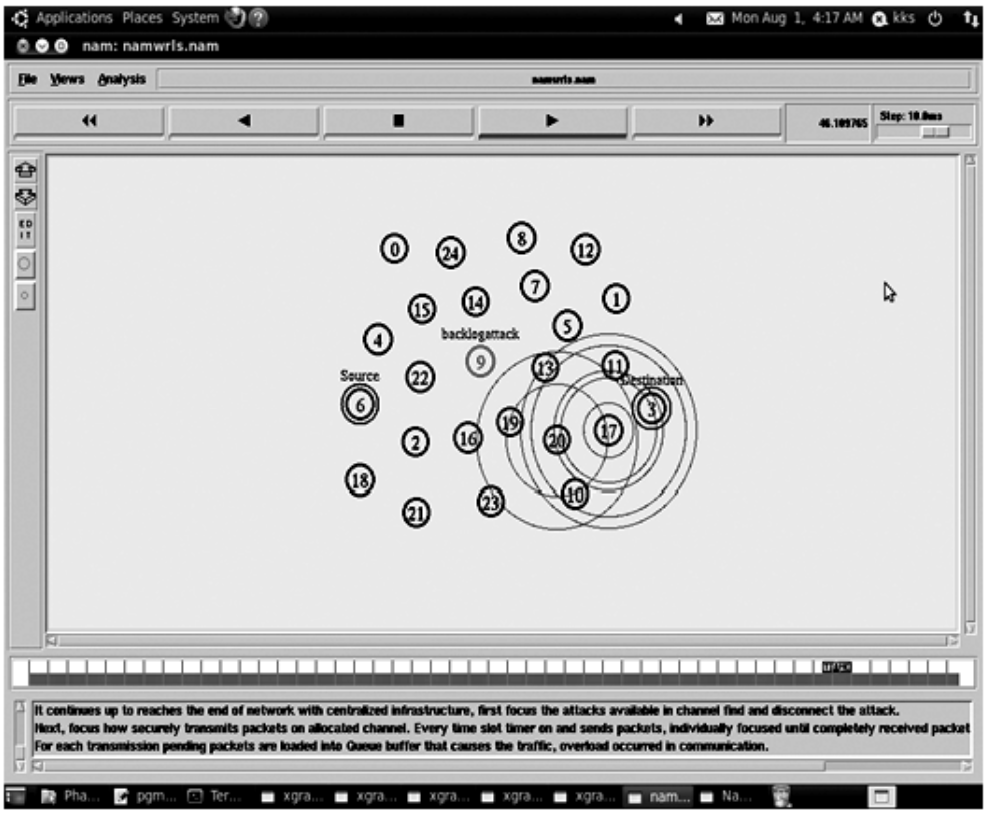

Figure 3: Proposed TBDS Result

6.1.1. Performance Analysis

In simulation to analyzing the following performance metrics using X graph in ns2.34.

*Delay***:** Figure 3 shows Time delay is calculated by the time taken to transmit packet from start point to end point, individual node is traced by IP address. In proposed TBDS method end to end delay is reduced compared to Existing method CBDS, and OLSR.

Packet Loss Rate: Figure 4 shows Packet falls during transmission between sender nodes to channel path that occurs when one or more packets, failure to reach the receiver node based on node capacity of network. Some node has lower capacity to achieve the receiver node. In proposed TBDS method Packet drop rate is minimized compared to Existing method CBDS, and OLSR.

Throughput: Figure 5 shows Throughput is measured by no of received sent from no of packet sent in particular speed. Speed instance is varied, but this simulation fixed speed is 100(bps). In proposed TBDS method Throughput is increased compared to Existing method OLSR, and CBDS.

Detection Efficiency: Figure 6 shows Detection Efficiency, Attack detection time with Overall time taken from source node to Destination node. The process takes how much time to detect the backlog attacks. In proposed TBDS method Detection Efficiency is increased compared to existing method CBDS, and OLSR.

Delay = End Time – Start Time

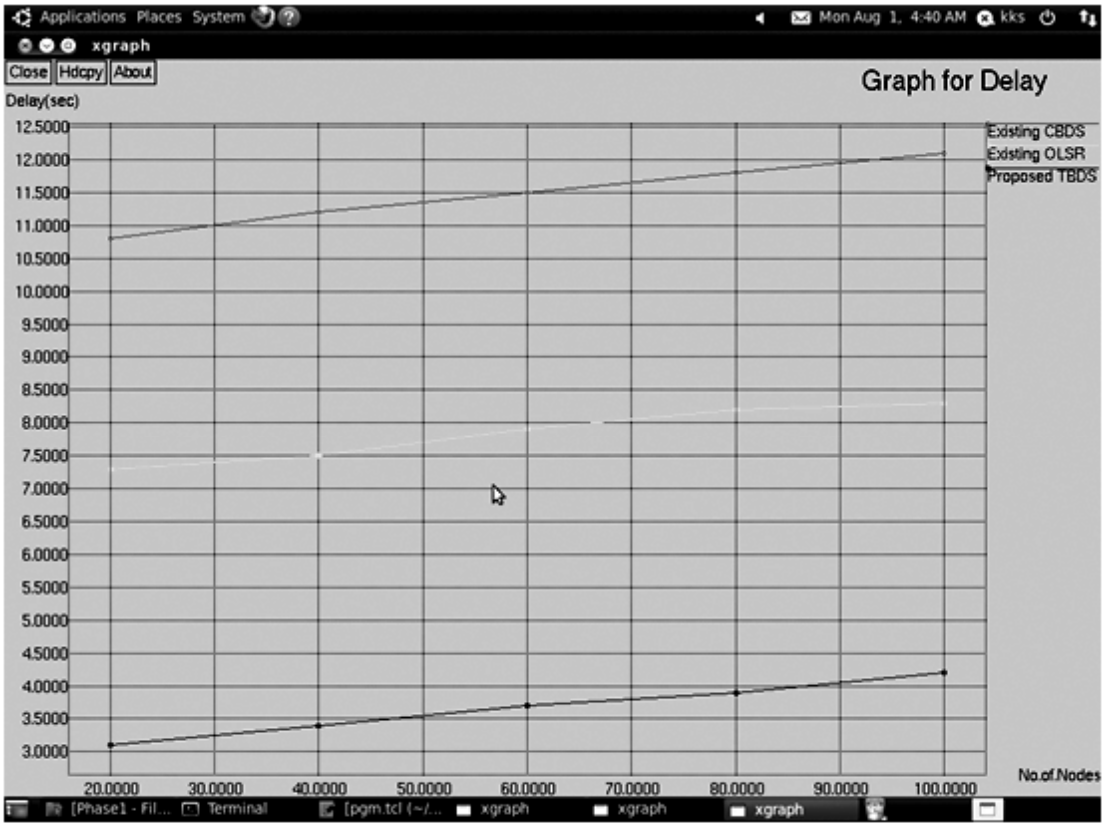

Figure 4: Graph for No of Nodes Vs. End to End Delay

Throughput= (Number of packet received/Sent)*speed

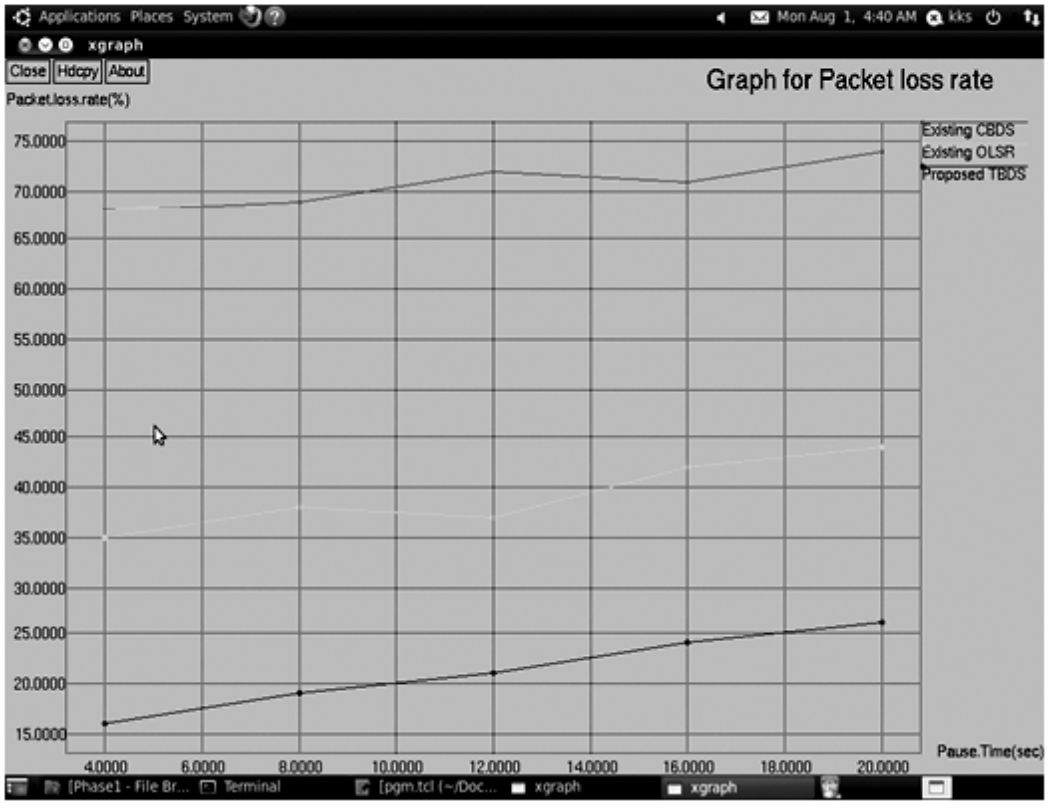

Figure 5: Graph for Mobility Vs. Throughput

Packet Loss Rate= (Number of Packet Losses/Received)*100

Figure 6: Graph for Pause Time Vs. Packet Loss Rate

Detection Efficiency= Attack detection time/overall time

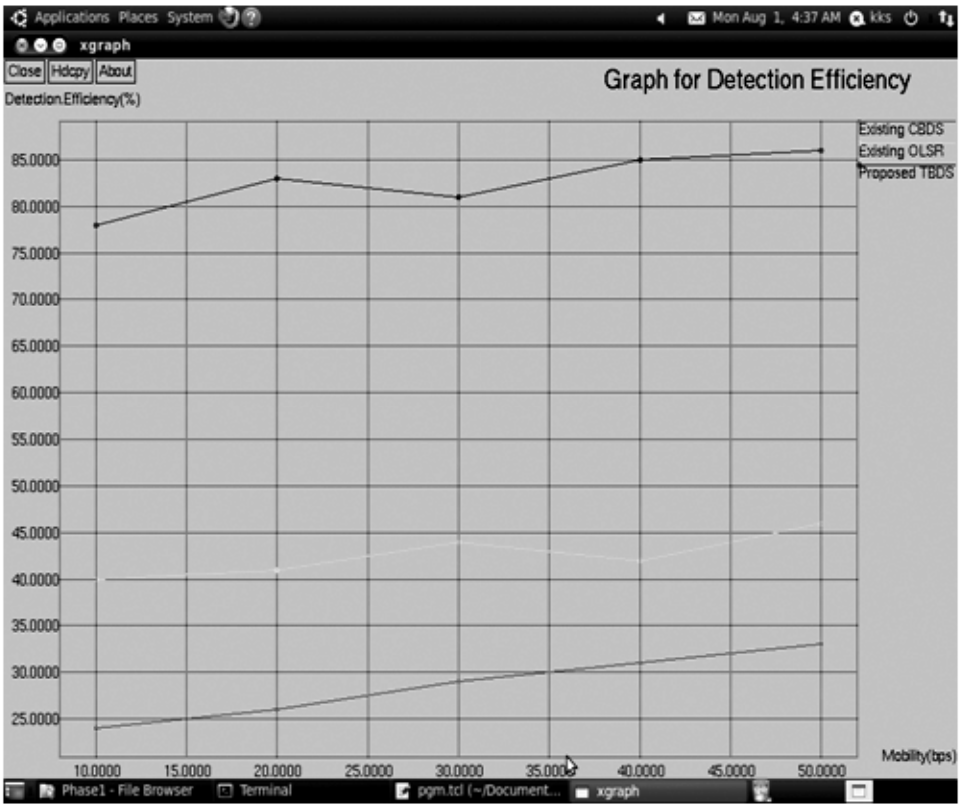

Figure 7: Graph for Mobility Vs. Detection Efficiency

Energy: Figure 7 shows energy consumption, how long energy spend for particular packet transmission, that means calculate energy consumption initial energy to final energy level. In proposed TBDS method energy consumption is reduced compared to Existing method CBDS, and OLSR.

Energy Consumption= Initial Energy-Final Energy

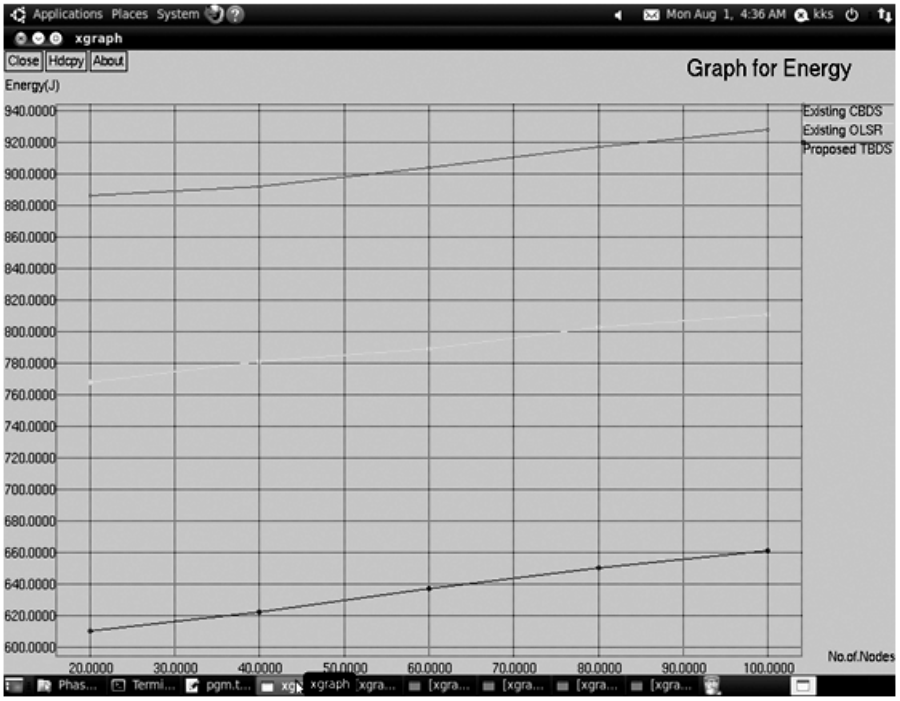

Figure 8: Graph for No of Nodes Vs. Energy

Network Lifetime= length of energy usage/overall energy

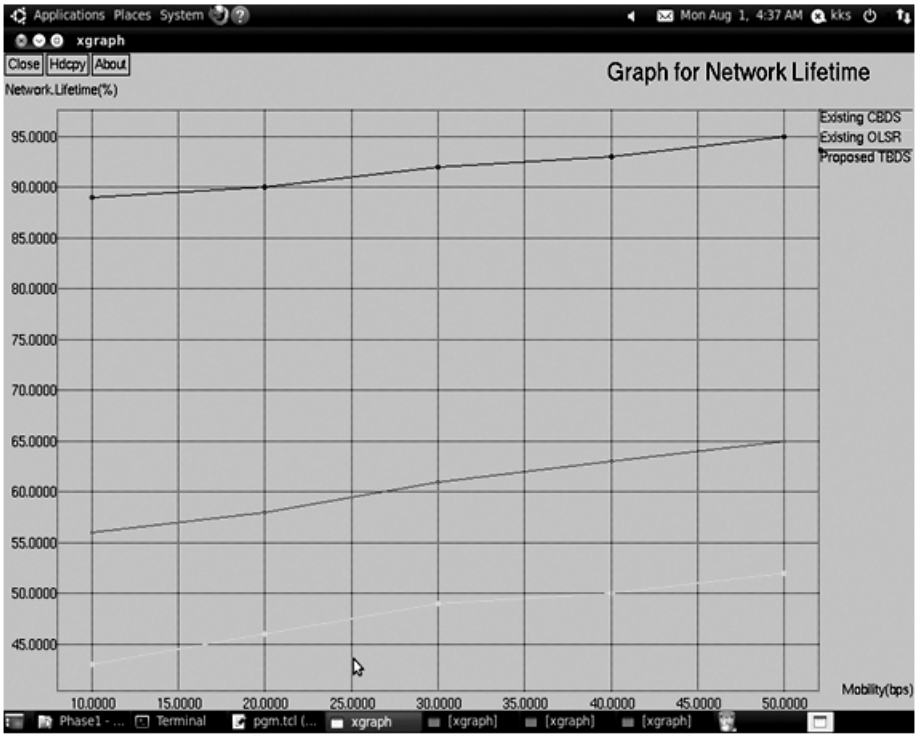

Figure 9: Graph for Mobility Vs. Network Lifetime

Network Lifetime: Figure 8 show that Lifetime of the network is measured by nodes process out of energy at particular time instance from starting to ending of the process.In proposed TBDS method Network Lifetime is improved compared to Existing method CBDS, and OLSR.

7. CONCLUSION

Mobile ad hoc Network are arranged based on source node and Destination node is created. To enhance the throughput using proposed Transmission based backlog Detection System (TBDS). Timer count to monitor the every time slots, maintain an efficient communication channel between source node to destination node in network. Each and every channel in network is checked with timer count to establish connections for improved packet transmission with detection of backlog attacks. This backlog attack not forwarding packets it block the information, because of insufficient capacity of that attacker node, network checks the next channel to set up a links in well-organized manner. Network lifetime is improved; nodes are not working in out of energy condition. Simulated in NS2, is a discrete event simulator, Proposed TBDS method minimize energy, reduce delay time, achieve minimum of loss rate, improve Throughput, maximize network lifetime and increased detection efficiency. In future use enhanced cross layer with backlog detection algorithm, to analyze the Throughput.

REFERENCES

[1] T. Bhaskar, N. Kamath and S.D. Moitra, "A hybrid model for network security systems: Integrating intrusion detection system with survivability," International Journal of Network Security, vol. 7, no. 2, pp. 249–260, 2008.

[2] Chang, Jian-Ming, et al. "Defending against collaborative attacks by malicious nodes in MANETs: A cooperative bait detection approach." IEEE systems journal 9.1 (2015): 65-75.

[3] Gupta, Lav, Raj Jain, and Gabor Vaszkun. "Survey of important Issues in UAV communication networks." IEEE Communications Surveys & Tutorials 18.2 (2015): 1123-1152.

[4] Wei, Zhexiong, et al. "Security enhancements for mobile ad hoc networks with trust management using uncertain reasoning." IEEE Transactions on Vehicular Technology 63.9 (2014): 4647-4658.

[5] Wang, Yanwei, et al. "A mean field game theoretic approach for security enhancements in mobile ad hoc networks." IEEE Transactions on wireless communications 13.3 (2014): 1616-1627.

[6] Bellavista, Paolo, et al. "Convergence of MANET and WSN in IoT urban scenarios." IEEE Sensors Journal 13.10 (2013): 3558-3567.

[7] Bala, Laxmi, and A. K. Vatsa. "Quality based Bottom-up-Detection and Prevention Techniques for DDOS in MANET." International Journal of Computer Science and Network Security (IJCSNS)13.8 (2013): 35.

[8] Liu, Wei, et al. "Cluster-based certificate revocation with vindication capability for mobile ad hoc networks." IEEE Transactions on parallel and distributed systems 24.2 (2013): 239-249.

[9] Marimuthu, Mohanapriya, and Ilango Krishnamurthi. "Enhanced OLSR for defense against DOS attack in ad hoc networks." Journal of Communications and Networks 15.1 (2013): 31-37.

[10] Shakshuki, Elhadi M., Nan Kang, and Tarek R. Sheltami. "EAACK—a secure intrusion-detection system for MANETs." IEEE Transactions on Industrial Electronics 60.3 (2013): 1089-1098.

[11] Guan, Quansheng, et al. "Joint topology control and authentication design in mobile ad hoc networks with cooperative communications." IEEE Transactions on vehicular technology 61.6 (2012): 2674-2685.

[12] Zhao, Shushan, et al. "A survey of applications of identity-based cryptography in mobile ad-hoc networks." IEEE Communications Surveys & Tutorials 14.2 (2012): 380-400.

[13] Xu, Gang, Cristian Borcea, and Liviu Iftode. "A policy enforcing mechanism for trusted ad hoc networks." IEEE Transactions on Dependable and Secure Computing 8.3 (2011): 321-336.

[14] El Defrawy, Karim, and Gene Tsudik. "ALARM: anonymous location-aided routing in suspicious MANETs." IEEE Transactions on Mobile Computing 10.9 (2011): 1345-1358.

[15] Saxena, Nitesh, and Jeong Hyun Yi. "Noninteractive self-certification for long-lived mobile ad hoc networks." IEEE transactions on information forensics and security 4.4 (2009): 946-955.