I J C T A, 10(20), 2017, pp. 111-124 ISSN: 0974-5572

Enhanced Query Arising for Position Based Intrusion Monitoring with Multipath Random Selection in Manet

S. Kannan* and A. Rajaram**

ABSTRACT

In mobile network mobile nodes are move randomly along the network. Mobile application is widely used in military applications. In previous work during packet transmission node behaves good or bad manner alternatively in network. It causes the network overhead during process. To overcome these problems, an Enhanced Query Arising Technique (EQAT) algorithm proposed for detecting intrusion in the network. In this work, multipath random selection scheme to choose efficient path updated in network. Source node communicate with destination node in mobile network through neighbor node cause attack, dual face attacks are detected. If any attack occurred go to next path checking until reaches the efficient transmission path in network. In Enhanced Query Arising technique, attack involved in process receiver node generate query in reply packet send to sender node. In network simulator used, the proposed EQAT attains efficient performance than previous works namely TDRT and TKQP.

Keywords: Enhanced Query Arising, Multipath selection in random manner, updating position of node, dual face attack, end to end time delay, Detection efficiency, and network overhead.

1. INTRODUCTION

A MANET-Mobile Ad Hoc Network [1] is a set of mobile nodes exchange information with each other using multi-hop connectivity with no support from message centre in network environment. Mainly mobile nodes work with help of MAC protocol. Shortest path selection based packet transmission in multi hop, every time hop count incremented in network. Multi hop technique is easy way to design in Mobile ad hoc network, nodes move frequently along its range, packets are waiting queue it causes the communication delay in network. Lesser hop path creates the delay in communication so choose efficient alternate path. Routing protocol not efficient, to balance load in minimum hop count. Neighbor node activity information is analyzed by MAC layer mobile node queue length also estimated. Heavy load makes packet dropping in transmission, with high power consumption on definite node, unequal allocation packet exchange cause to high packet loss. In route selection method choose the minimum time delay path in minimum hop count to reduce load traffic attack occurred. So, choose the alternate routing path to reduce the packet drop. Each and every node faces neighbor nodes and also the neighbors of its neighbors in the medium contention technique. Since the range of possible medium contention of a mobile node is broad, medium contention times maximize the end to end delay significantly. QoS-Quality-of-Service is a popular feature for MANETs towards the expansion of multimedia usage [2]. Many techniques have introduced to provide guarantee in connectivity between nodes. The Performance of the wireless medium, and wired network based on QOS not affect the Mobile ad hoc network. Presents an efficient QoS routing protocol minimizes the time delay in network environment and evaluates the presentation of the present algorithm by simulation takes varied speed and heavy load. Set of rules need to change and enhance the QS-AODV to find path with minimum

* 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*

load and maintain the required Qos, it choose paths with minimum load and packet exchange in route for route preservation. Protocol evaluates node delay actively and destination node check the strength of the paths by minimizes the end delay and choose effective path for packet transmission. Existing paper [3] takes only lesser hops in the path selection method.

Remaining part of the paper is planned as follows. Section II indicates a related works. In section III, Describe the details of proposed Enhanced Query Arising Technique (EQAT). Multipath selection in randomly, dual face attack detection, and Query Arising techniques. Section IV provides simulation performance results analysis obtained under various metrics. At last section V concludes the paper with future direction.

2. RELATED WORKS

Raushan Kumar et al., [6] proposed a black hole attack is a kind of misbehaving attack in which black hole node gives reply packet, route request packet to destination with maximum sequence number and minimum hop count to the sender. Source node forward data packets to attacker node not forward to destination, it drops the packet or misuse information. Remove black hole attacks in AODV it contains secure route detection. In secure route detection the destination node and the source node checks the sequence numbers in the Route Reply and Route Request messages correspondingly. Present method include extra purpose at source node efficient as destination node while a RREP or RREQ packet transmit to the individual node it verifies the sequence number of the packets and distinguish with the certain range. Different methods to give security to ad hoc on demand distance vector routing protocol. Present approach for protecting AODV against black hole attacks in network. Performance result indicates that the present approach improves the packet delivery ratio for three various coverage fields with node speed.

JeeSook Eun et al., [7] proposed attack route analysis, perform process depends on routing table. Routing table contains the path for routers detected by path identifier; also path identifier receives the packet. Whether attack is finding by injured party, nearest path the injured node initiate the attack route analysis depends on path identifier. It blocks one attacker at router nearest to attacker and worried about number of attacker available independently in network. It confirms a probability of present method on Linux system construction. PID for sender and receiver routers depends on communicating information and Make the node added it to packet received. While attack is identified by injured party, injured party creates an attack warning message include in PID captured and forwards to its local nodes. Local nodes capture packet, the packet is transmitted to the router near to intruder. In confirmation possibility for present method, then constructed it. Simulation output shows method attack reply time straight proportional to hop count and want one analysis packet for single attack. Present monitor with large scale attacks quickly compared to the minimum bandwidth consumed by previous method. It monitor the attack process not any external storage maintenance.

Jeong Yun Kim et al., [8] Present determined Request-Routing System forward each requests contains the same content to a particular content node in direct to use a single multicast stream only during the packet length, it introduces the mixed CDN -Content Delivery Network system, it effectively join novel content routers in underlie with previous CDN servers in overlie by working prefix caching and multicast methods correspondingly. Analyze the ability of CDN server, we estimate and judge the output of two multicast methods for the delivery cost minimization in indicates length of packet in network gathering in the present system. The merged CDN system, depends on network gathering, by fixed the novel content routers in underlie to the usual CDN system. Constructed the effective prefix length in network, gather minimizing the delivery cost for a group of content with highly twisted status by compare the multicast methods.

Seryvuth Tan et al., [9] proposed network nodes easy to join or leave from particular area in dynamic manner with time free. Normally MANET causes different types of attacks, it reduce network performance. MANET provides black hole attack is sole for malicious attack easy to disrupt the network process. If black hole node gives reply to request packet quickly in minimum distance path and the maximum receiver

seriously. Black hole node not provide efficient path to a particular destination, communication black hole node drops the packets. Present method that provides Secure Route Discovery for the AODV protocol (SRD-AODV) way to avoid black hole nodes. Sender and receiver node checks the sequence number in RREQ and RREP fix some threshold value, then provide connectivity between sender and receiver node for communication. Ad hoc Network is vulnerable for misbehaving nodes contains black hole attack nodes. Survey the previous work and launch new present attack identification and removing in secured manner. Speed of node movement cause some changes in network performance.

Shibao Li et al., [10] present probabilistic algorithm to transmit request packets closer the receiver. There is not positioning, the algorithm uses meet history to guess the route to destination and fix various transmission probability for various neighbor nodes in network. Simulation output show present algorithm minimizes 70% routing cost compared to flooding and 20% compared to pure probabilistic method. Also, the innovative algorithm also gives best performance than other methods. The performance of innovative algorithm with flooding and pure probabilistic algorithm checks in various node count availability. In simulation performance result shows verify the advantage of the present algorithm. The new algorithm also shows good performance in delivery chance and delay time.

H´eberte F. Moraes et al ., [11] proposed QoE -Quality of Experience a significant problems for the designing of applications. Multi-hop technique used in Packet transmitting includes size of packets, increase intrusion in network cause collision. In REP protocol for mobile network presents reduction in problem for efficient communication, REP has communication protocol that generates minimal disturbance in communication medium like intermediate nodes. REP launches the APs-Active Prefixes, a new method for location monitoring, packet transmission, and central communication. AP is collected of prefix (P) and interest (I), which every device construct P and each running application set I. REPD, using REP protocol, was deployed in Ubuntu and Android. REP API gives basic communication process that cases the construction of central applications.

Gundeep Singh Bindra et al., [12] present method to identify and protect blackhole and grayhole attacks in network. The result in present method removes these attacks by contains an EDRI -Extended Data Routing Information Table node information are maintained in routing table in AODV protocol. This method is capable of detecting a malicious node. It also maintains historical information of the node's earlier malicious instances to description for the gray performance. Packets are refresh, renew, BHID, Further request and further reply packets are also used in addition to the existing packets (RREQ and RREP). This method is capable of identifying sequence of cooperative misbehaving nodes which fall down packets an important part of transmission. DRI Table to generate the EDRI Table which is able to hold the Gray nature of the nodes as effective. The present solution can be applied to first recognize many black/gray hole node cooperate with each other in a MANET; and second Determine safe paths from source to destination by avoid many black/gray hole node performing in support. Restriction of result that the malicious nodes have to be repeated even as performing in support detect by the algorithm. Aim to improve result so that alternative supporting nodes can be detected as even. Goal to perform process in this algorithm, get optimized effective packet transmission.

Jeba Veera Singh Jebadurai et al., [13] present MANETs attacks are mainly routing protocol attacks. The sinkhole achieve caused by try to inform all traffic load to misbehaving node transmit false shortest path routing packets. Sinkhole attack identified and separate as early as probable. The detection method gives assurance maximum detection efficiency and minimum cross over error efficiency. Present a novel method to find the sinkholes that initial monitoring of mobile node activities attacks that affect overall network performance. Sinkhole intrusion detection method should identify the sinkholes takes minimum time for detection and with increased success rate of detection. Present detection method that monitors the network environment. Simulation gives efficient output that find all type of attacks with enhanced characteristics.

Dong-Won Kum et al., [14] presents an effective on demand routing approach includes DF-directional flooding, that fitting for wireless network with partial speed. In path finding process to arrive at intermediate,

DF method can minimize the number of RREQ route request packets transmission by using a limited directional flooding method. The output results indicates AODV-ad hoc on-demand distance vector with DF can considerably minimize the routing overhead by Request packets and improves the performance of overall process compared with previous method. Yet while mesh routers and regulars have a minimum speed, also much improved its performance still over Previous AODV protocol. Consequently, AODV-DF should additional proper than original AODV to reduce traffic occurrence acts gateway, that mesh routers and clients are either inactive. Simulation indicates a particular gateway, but AODV-DF also can be applied for WMNs with many gateway intermediate nodes.

Sangman Moh et al., [15] present MANETs link quality aware routing protocol for resulting in robust delivery and high performance to identifying a reliable path with well-built links. In path finding, the well-built links are effectively broken by transmitting request packet in maximum link quality else SINR signal to interference plus noise ratio in the middle of many Request packets received by receiver node. Distinguish with AODV conventional protocols such that simply the first-arrived Request is transmitted remaining are removed, the present method there is no minimum hop-count path but many number of hops. Finding path is a reliable path have higher packet transmission rate because it contains of well-built links, resulting in maximum performance as good healthy routing. LAAODV -link quality aware AODV removing the request forwarding algorithm, shows output in strong packet delivery and high network characteristics.

Tsung-Chuan Huang et al., [16] present hybrid routing protocol with k-hop clustering environment in MANETs. Sender needs to transmit packets to the destination node straight to neighbor node information's are stored in sender node table, else source passively transmit the RREQ -route request packet to start the communication. Receiver node accepts the transmitted RREQ in communication between the sender and receiver node, the RREP-route reply packet is transmitted through the nodes available in clusters that the RREQ transmitted to identify path. Path designing to avoiding cluster head, cluster head confuse network to make overhead. Distinguish with Cluster Based Routing Protocol (CBRP), the present protocol can allocate the transmission load starts with cluster heads to non cluster head node, depending on cluster size the number of node transmission is minimized, it cause node drops packet during transmission. The path between the sender and receiver node is construct, receiver node accept the RREQ packet from sender, and receiver gives reply message to sender node in network. Path construction is not best for only cluster also for present method is best compared to CBRP. Besides, the cluster size is flexible to put up a different network structure.

Pradeep Macharla et al., [17] present protocol find out path depends on time delay with hop count path protection is best one than previous methods. Dynamically AODV node movement consider only stable value in QS-AODV method. Simulation output denotes, it is obvious present AODV and QS-AODV minimum speed and traffic load. Performance of protocol is efficient for trustworthy communication in mobile applications with MAC layer protocol included. Present protocol gives extract time delay for communication. It reduces the collision in path stores a path of accumulate wait value field like Acc_Delay. Present optimize the effective path. In AODV-D evaluate node delay energetically with static values in previous work QS-AODV.

S. Padma Priya et al., [18] Proposed LR-WPAN security structure are analyzed to handle different type of problems and an ESF -effective security structure is introduced. It removes routing attack and data forwarding attack. Structure includes identification of malicious nodes by misuse routing and separation of misbehaving nodes by with multi-signature based ticket in network. Identification of misbehaving node is processed by each node by tracking the RREQ packet transmitting process to intermediate nodes. Introduce the ticket regeneration and revocation method using the mixed signatures of multiple certified servers.

Jin Seok Yang, Kyungran Kang et al., [19] the problem of collecting data packets in network node energy level is not enough. Present energy aware multipath routing protocol-PAMP, is used for constant network. Aim of the paper is enhancing the availability of the wireless as well as ensures trustworthy

delivery by utilize the minimum energy node. Present PAMP is constructed as an addition of AODV protocol. It wires energy condition with multiple paths, launches data elements in request packet, reply packet, and the routing table. Then evaluate the performance of PAMP with LAMOR, PAOD and AODV. The simulation output indicates which PAMP provides increased packet delivery ratio and maximum network lifetime cause the more routing overhead.

Rakesh Kumar et al., [20] present on demand delay based QoS-quality of service routing protocol to guarantee that delay not maximize its threshold value in mobile nodes. Proposed method determination considers MAC layer channel disagreement information and packets count in the boundary queue in addition to least hops. In MAC layer disagreement information gives an extract evaluation of intermediate nodes performance load in queue length itself at the mobile node. The present method also considerably minimize path find out latency due to ease of use of support paths in source node routing table. Present work analyzes the end- to-end delay, contention delay, queuing delay, processing delay among in hop count. It keeps away from a attacker path by keeping way of accumulated delay value. Previous work the processing delay based on routing path in mobile nodes, it gives not accurate evaluation end-to-end delay. Present Method, it minimizes the latency of communication and justification supports routing hit messages in network. In QoS routing protocol efficient result compared to previous work.

3. OVERVIEW OF PROPOSED SCHEME

Mobile nodes are moved randomly across the network, attacks are detect and removed from network during communication between source node to destination node. That time nodes because dual face attack, attacker node behaves as efficient node otherwise behave like fake node alternative manner is called as dual face attack.

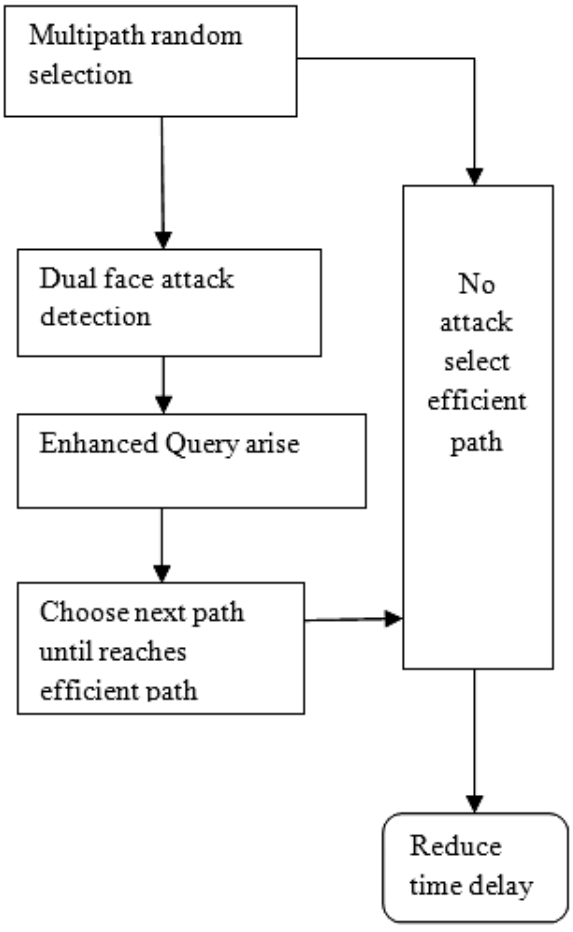

Figure 1: Block Diagram of Enhanced Query Arising based Intrusion detection

Figure 1 shows the Enhanced Query Arising Intrusion detection Techniques sender node selects the path in random manner, if any dual face attack involve query arise from reply packet in the receiver node, sender convey that query and choose next node for communication it continues until efficient path reached in network.

In Dual face attack is difficult to identify, because it act some times as good node else act as bad node, Dual face attacker have two operating mode on and off mode, normally on mode node forward the original data to neighbor node in a network. In off mode node misuse the data forward to out of coverage node or unauthorized node in network environment. Propose an enhanced query Arising based intrusion detection to detect attacker node with help of query arise from reply packet.

3.1. Multipath selection in random manner

In proposed multiple channels or paths are selected to broadcast packet from source node to destination node in network. Packet transmission initially on first path and then go to next path until got efficient path for communication between source to destination node. Source node analyze the neighbor node history, if it satisfy the condition node choose next neighbor node in mobile network. If it not satisfy the condition search for another node in particular path, and then repeat the process to make a path. Condition is coverage and connectivity of each node.

Already deployed nodes contains group of nodes, goal to simulate multiple paths in a random manner at every time data packet transmitted to neighbor node, in that group of nodes obtain by different packets stay altering in excess of time. In output more number of paths is created in each source and destination communication. Some disturbance occurred during packet transmission, through each relay nodes, there is sudden energy loss or transmission path corrupted. MANET normally updated its location, so the location updated efficient path attains is very difficult one.

Nodes are frequently forward packets if any path failure goes to next path in a mobile network. Node gets failure broken the link connection too much of energy is consumed. So network lifetime is reduced, not achieve efficient communication. Overcome this energy usage, generate randomized multipath routes, nodes change their path for its convenient among the mobile ad hoc network. Packet size is varied in transmission so go for multipath routing. Data forwarding to every hop increment to next hop in a path, up to reaches the destination node.

3.2. Detection of Dual Face attack

Mobile network efficient packet transmission is very difficult to achieve, because position updating randomly is carried on every time in network. In node transmits packet based on coverage and connectivity, current connectivity is checked and further forward packets to neighbor node. Source node forward data packet to neighbor node in particular location that node initially behaves like a god node and after sometimes it behaves like a bad node, node is dual face attacker node. Node behaves normally but sometimes it behaves as abnormal condition in network, abnormal behaviour are misuse packet, it hide important information received from source node, attacker not forward the original information, this kind of attack is very dangerous in network environment.

Normally information exchanges between nodes in a particular time, the position information, history of node behaviour is analyzed and gives response message to sender node. Sender node received two messages m and n from neighbor node in path $\{m|n||initial\ position\ v\}$, *to* $\{m|n||updated\ current\ position\ c\}$ based on the rules information in these two messages have to assure terms.

$$\{m|n||initial\ position\ v\} \tag{1}$$

$$\{m|n||updated\ current\ position\ c\} \tag{2}$$

Break the path any of the node attack is find. The initial status of each node is arranged and create path, neighbor node find next node like a chain and repeat the process until achieve efficient path. In packet transmission data transmitting and receiving time is noted, that is if $mi < mj$, and single if $ni < nj$, where m is request packet message start time is mi and end time is mj. Then n is reply packet message start time is ni and end time is nj. Next focus the node connectivity, node check whether neighbor is in nearest distance or else in longer distance. Node initial position is v and modified position is c the all positions are noted, that information's are also attached in reply packet. Check if v and c are equal go to packet forwarding use that path, else the v greater than c goes to connectivity replace the node forward packet to replaced node, else the v less than c goes to connectivity replace the node forward packet to newly added nodes in network in particular time intervals.

Time interval is monitored obviously $|tp - tq|$ path speed is analyzed by using each packet transmission on every time slots Speed. Packet transmission in path takes maximum speed attains efficient path, otherwise it takes minimum time for packet transmission is worst path, worst path have attacker node, dual face attacker capture information and misuse the information so go for best path with maximum speed.

$$Speedmax * |tp - tq| \tag{3}$$

$$Speedmin * |tp - tq| \tag{4}$$

Condition number of nodes that m sender node meets between tp and tq must be equal or lesser to the more possible neighbor nodes it convenes time interval |tp – tq|.

$$|mi - mj| \le \left(Speedmax \times |tp - tq| \right) \times 2max \tag{5}$$

Node availability also considers for process in network, each packet transmission node range is estimated. So easy to detect the attacker node is available or not in MANETs.

Algorithm for Position based Intrusion Monitoring

Time interval Input: m, Pack, tp
Time interval Output: n, Pack, tq

Step 1: function *Source* –> (*m*, *Pack*, *Tp*)
Step 2: If $m = n$, m evaluates
Step 3: $tp \leftarrow Time\ (m, mi < mj)$ Estimate time tp for m.
Step 4: $tq \leftarrow Time\ (n, ni < nj)$ Estimate time tq for n.
Step 5: else
Step 6: if m convenes n at particular time t (t ± Δ) then
Step 7: $Destination \leftarrow v\ (m, |tp - tq|)$ Evaluate the position information to send.
Step 8: end if
Step 9: $Destination \Leftarrow Messagem \rightarrow n || c\ Messagem \rightarrow n$, sent from m to n at time tp, sent to position c (m, |tp-tq|).
Step 10: else
Step 11: Return not answer n stops the coverage process on m.
Step 12: end if
Step 13: if all *Message* $m \rightarrow n$ received at the position $(m, |tp - tq|)$ are steady with each other then
Step 14: end if
Step 15: end function

3.3 Enhanced Query Arising based Intrusion Detection

In enhanced query arising method generate query when intrusion detected on network, source node transmit packet to intermediate node along the broadcasting path in network, sender send packet that contains node ID, position of node, and time. Receiver node receives that packet and send reply packet that contains node ID, position of node, and time, else it contains node ID, position of node, time, and query arise. The query is arising, when dual face attack is detected during transmission between two nodes. To get the best node only in path applying Enhanced Query Arising Technique (EQAT), Query contains the failure report, dual face attack have two faces on and off. On face act as true node, and else off face work as false node in alternative manner. Only off face cause the attack it forward packet to wrong node such that out of coverage node in a network.

Query arise packet forwarded in wrong direction in network, which affect the overall network performance in network. Sender accept the reply, triggers to next efficient path in network to attains the effective communication between source node to destination node, improves throughput rate and detection efficiency, minimize the resource utilization like energy consumption in network.

Algorithm for Enhanced Query Arising Technique

Step 1: IF source node forward packet to neighbor node

Step 2: neighbor node is dual face attacker node forward RREP with query arise.

Step 3: else not an attacker forward packet to next neighbor node in a particular path, top n search is used.

Step 4: ELSE discard the RREQ

Step 5: the node reaches destination end forwarding the RREQ Packet.

Step 6: END IF

Step 7: Process continues until reaches the efficient path in network.

In MANET use the Enhanced query arising operates on top n searching manner, Toper true node is select only to achieve efficient communication between source node to destination node. Top n method searches the node during transmission; n is best true node, dual face attack off mode best node converted to false node in network. Top n analyzes the historical reference of node; dual face attacker is easy way too detected. It stores the visited node characteristics and creates Query based on the history and transmits to receiver node in same path, to minimize end to end delay time

Packet ID: It consists of all mobile node historical information. It also has node's position and normal updates identification it deployed in network infrastructure.

In figure 2: the EQAT packet format is available. The source node ID field consumes 2 bytes and 2 bytes are hold by destination node ID field. Third one is Multipath random contains 4 bytes. During packet transmission choose multipath in random way. In fourth field occupies 4 bytes, the Enhanced Query creating is indicated, evaluate the node history detect intrusion to generate query from reply packet. In fifth occupies 4 bytes, the position of each node in transmission, update the current location of every node in network. The last filed Top n search occupies 2 bytes, to categorize the network nodes present.

Source ID	*Destination ID*	*Multipath random*	*Enhanced Query Arising*	*Position of node*	*Top n search*
2	2	4	4	4	2

Figure 2: EQAT Packet format

6. PERFORMANCE EVALUATION

6.1. Simulation Model and Parameters

The proposed EQAT is simulated with Network Simulator tool (NS 2.34). In our simulation, 100 mobile nodes move in a 900 meter × 900 meter square region for 51 milliseconds simulation time. Each Mobile node goes random manner among the network in different speed. Mobile nodes have coverage area is 250 meters. CBR Constant Bit Rate provides a constant speed of packet transmission in network to limit the traffic rate. DSR- Dynamic source routing protocol is used to allocate dynamic channel for communication. Table 1 indicates Simulation setup is analyzed.

Table 1
Simulation Setup

No. of Nodes	*100*
Area Size	900 × 900
Mac	802.11
Radio Range	250m
Simulation Time	51ms
Traffic Source	CBR
Packet Size	150 bytes
Mobility Model	Random Way Point
Protocol	DSR

Simulation Result: Figure 3 show that the proposed EQAT method detect the dual face attack use Query arise technique is best compared with existing TDRT [4] and TKQP [5]. EQAT sincerely monitors the packet transmission to block bad node activities. It improves the detection efficiency for identifying dual face attacks in network.

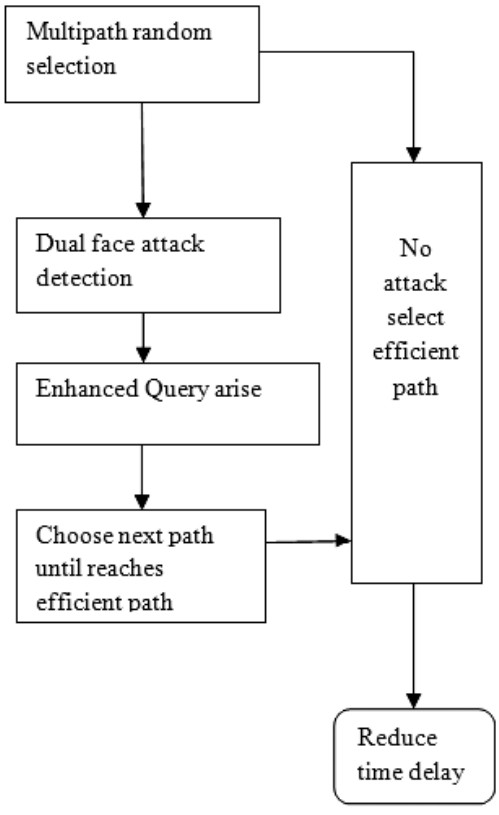

Figure 3: Proposed EQAT Result

6.1.1. Performance Analysis

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

End to End Delay. Figure 4 shows end to end delay is estimated by amount of time spent to transmit packet from starting node to ending node, individual node is traced by IP address. In proposed EQAT method end to end delay is reduced compared to Existing method TDRT, TKQP, TBDS, EMCPT, and GSPR.

End to End Delay = End Time – Start Time

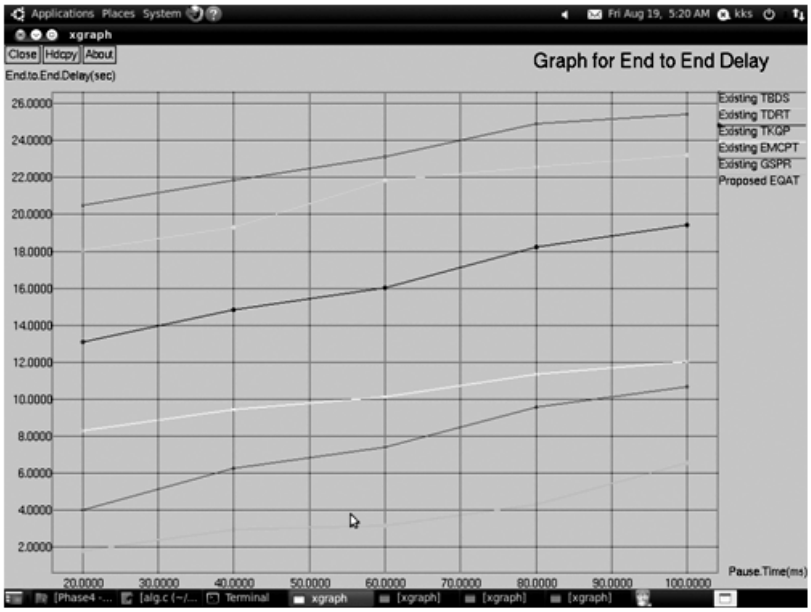

Figure 4: Graph for Pause time vs. End to End Delay

Network overhead: Figure 5 shows Network overhead is decreased when source need to forward packet to destination node, relay node available in network, if they required minimum energy, relay or intermediate node can't receive or transmit packet. In proposed EQAT method Network overhead is minimized compared to Existing method TDRT, TKQP, TBDS, EMCPT, and GSPR.

***Network overhead = (Number of Packet Losses/Received)* * 100**

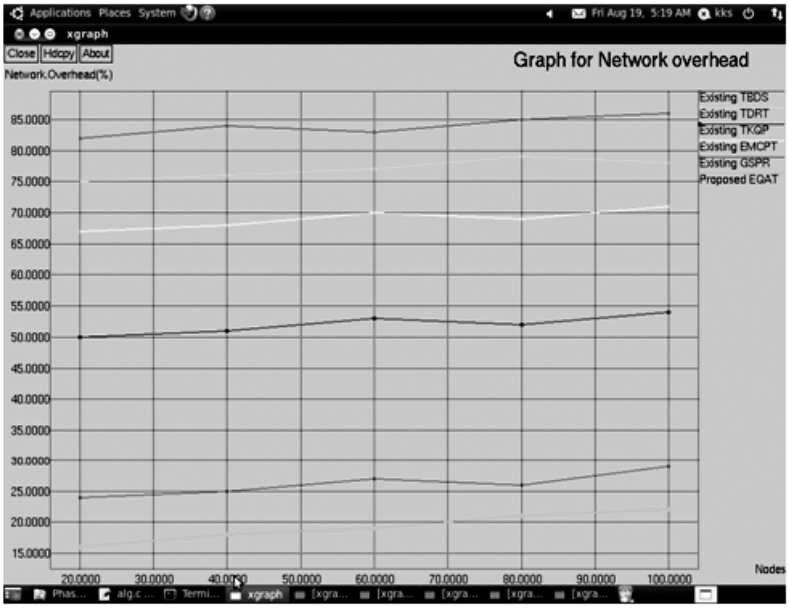

Figure 5: Graph for Nodes vs. Network overhead

Throughput: Figure 6 shows Throughput is measured by no of received from no of packet sent in particular speed. Mobility or speed not a constant, simulation mobility is set to 100(bps). In proposed EQAT method Throughput is improved compared to Existing method TDRT, TKQP, TBDS, EMCPT, and GSPR.

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

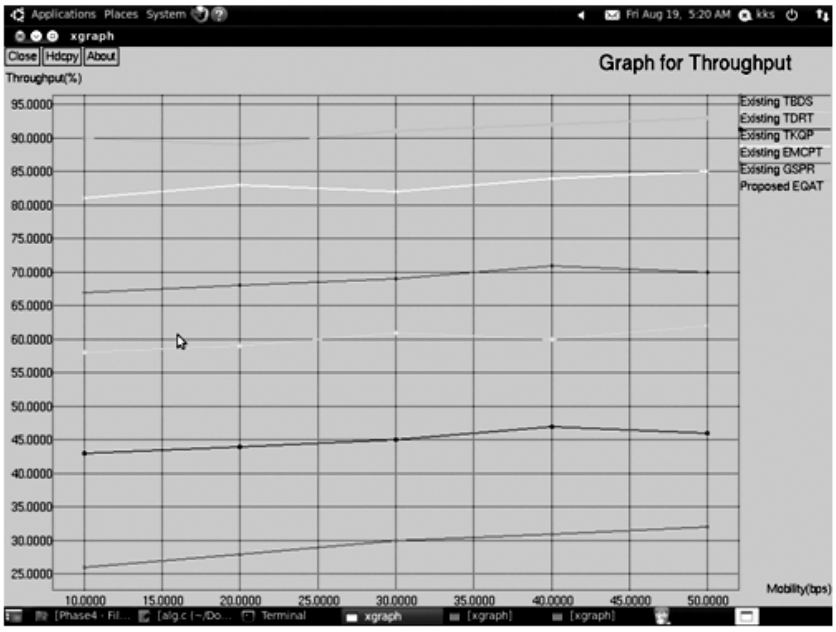

Figure 6: Graph for Mobility vs. Throughput

Detection Efficiency: Figure 7 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 dual face attacks. In proposed EQAT method Detection Efficiency is increased compared to existing method TDRT, TKQP, TBDS, EMCPT, and GSPR.

Detection Efficiency = Attack detectin time/overall time

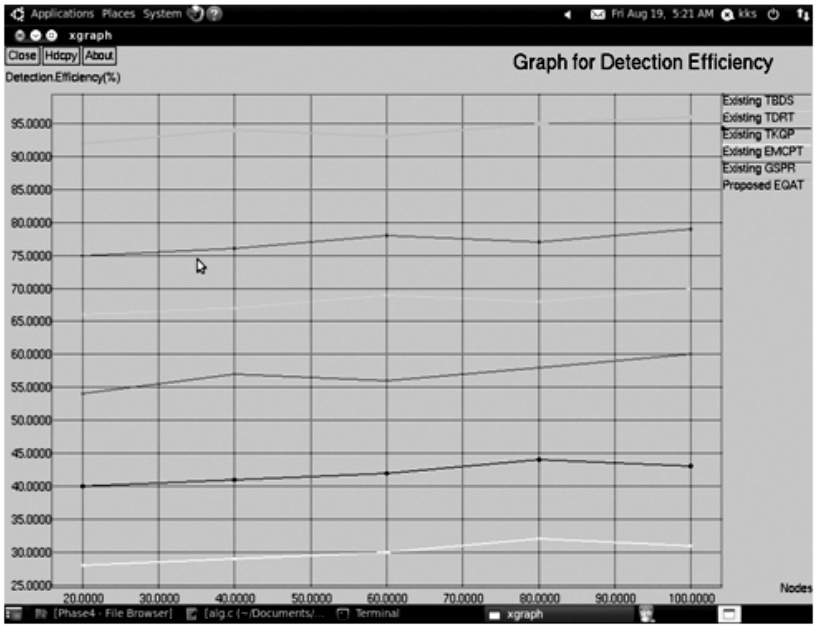

Figure 7: Graph for Nodes vs. Detection Efficiency

Energy: Figure 8 shows energy consumption, how long energy spend for particular packet transmission, that means calculate energy consumption initial energy to final energy level. In proposed EQAT method creates query for every time if any misbehavior occurred in network, energy consumption is compared to Existing method TDRT, TKQP, TBDS, EMCPT, and GSPR.

Energy Consumption = Initial Energy – Final Energy

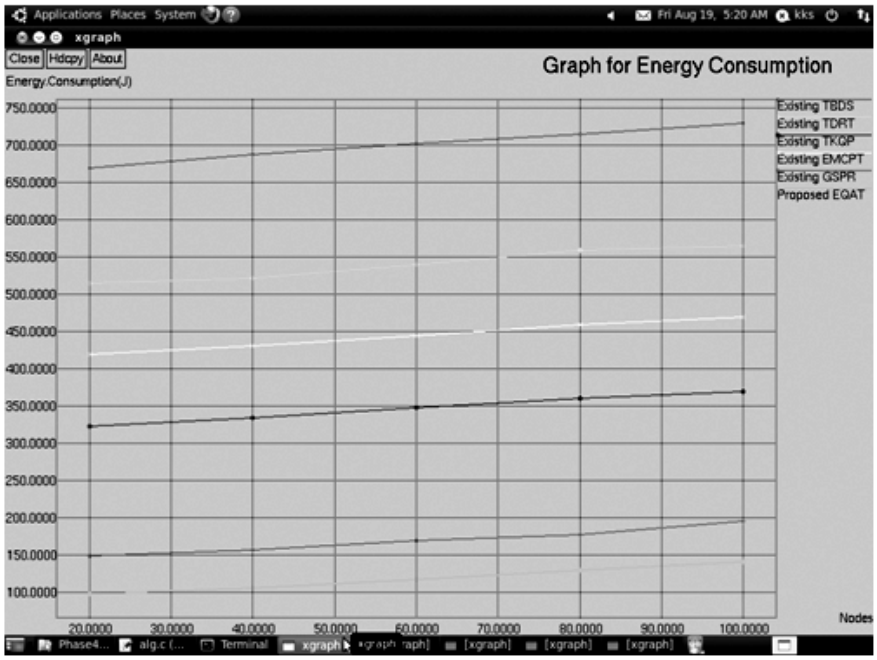

Figure 8: Graph for No of Nodes vs. Energy Consumption

Network Lifetime: Figure 9 show that Lifetime of the network is measured by nodes process out of resource utilization in at particular time instance from starting to ending of the process. In proposed EQAT method Network Lifetime is improved compared to Existing method TDRT, TKQP, TBDS, EMCPT, and GSPR.

Network Lifetime = length of energy usage/overall energy

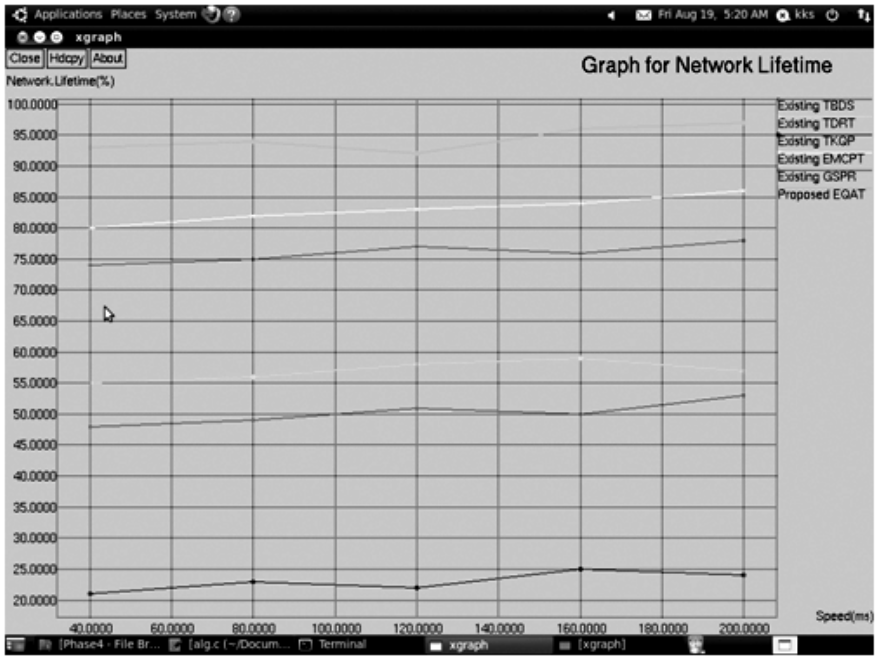

Figure 9: Graph for Speed vs. Network Lifetime

7. CONCLUSION

MANET mobile nodes are moved among network random manner, source node need to transmit packet to destination node in particular path, that time use multipath packet forwarding method, packet forwarded on first path if it get failure and then go to next path if it get success go to same path else search efficient attack free path. During transmission time path failure caused by dual face attack, it act good or bad, it detected by Proposed Enhanced Query arising Technique (EQAT), arise the Query if any attack or damage occurred from Reply packet of attacker node. It reduces the energy usage, delay time, increase throughput and network lifetime. In future propose Query arising with link connectivity based intrusion detection, to analyze the packet delivery ratio in updated network.

REFERENCES

[1] Marker, J., and M. Corson. "Internet Engineering Task Force (IETF) Mobile Ad-Hoc Networks (MANET) Working Group Charter." 2007-02—12.

[2] Ghosekar, Pravin, Girish Katkar, and Pradip Ghorpade. "Mobile ad hoc networking: imperatives and challenges." IJCA Special Issue on MANETs3 (2010): 153-158.

[3] C.E. Perkins, and E.M. Belding-Royer, "Quality of Service for Ad Hoc On Demand Distance Vector Routing," draft-perkins-manet-aodvqos-02.txt, Mobile Ad Hoc Networking Working Group Internet Draft, 14 October 2003.

[4] Movahedi, Zeinab, et al. "Trust-Distortion Resistant Trust Management Frameworks on Mobile Ad Hoc Networks: A Survey." IEEE Communications Surveys & Tutorials 18.2 (2016): 1287-1309.

[5] Tsuda, Takuji, et al. "Top-k Query Processing and Malicious Node Identification Based on Node Grouping in MANETs." IEEE Access 4 (2016): 993-1007.

[6] Kumar, Raushan, Abdul Quyoom, and Devki Nandan Gouttam. "To mitigate black hole attack in AODV." Next Generation Computing Technologies (NGCT), 2015 1st International Conference on. IEEE, 2015.

[7] Eun, Jeesook, and Heeyoung Jung. "A technique to make a path table for blocking Distributed Denial-of-Service attacks." 2015 9th International Conference on Future Generation Communication and Networking (FGCN). IEEE, 2015.

[8] Kim, Jeong Yun, Gyu Myoung Lee, and Jun Kyun Choi. "Efficient multicast schemes using in-network caching for optimal content delivery."IEEE Communications Letters 17.5 (2013): 1048-1051.

[9] Tan, Seryvuth, and Keecheon Kim. "Secure Route Discovery for preventing black hole attacks on AODV-based MANETs." High Performance Computing and Communications & 2013 IEEE International Conference on Embedded and Ubiquitous Computing (HPCC_EUC), 2013 IEEE 10th International Conference on. IEEE, 2013.

[10] Li, Shibao, Linlin Lou, and Li Hong. "Directional probabilistic broadcast in wireless mobile ad hoc networks." Computational and Information Sciences (ICCIS), 2013 Fifth International Conference on. IEEE, 2013.

[11] Moraes, Héberte F., et al. "On developing interest-centric applications for ad hoc networks." World of Wireless, Mobile and Multimedia Networks (WoWMoM), 2012 IEEE International Symposium on a. IEEE, 2012.

[12] Bindra, Gundeep Singh, et al. "Detection and removal of co-operative blackhole and grayhole attacks in MANETs." System Engineering and Technology (ICSET), 2012 International Conference on. IEEE, 2012.

[13] Jebadurai, Jeba Veera Singh, A. Alfred Raja Melvin, and Immanuel John Raja Jebadurai. "Sinkhole detection in mobile ad-hoc networks using mutual understanding among nodes."Electronics Computer Technology (ICECT), 2011 3rd International Conference on. Vol. 3. IEEE, 2011.

[14] Kum, Dong-Won, et al. "An efficient on-demand routing approach with directional flooding for wireless mesh networks." Journal of Communications and Networks 12.1 (2010): 67-73.

[15] Moh, Sangman. "Link quality aware route discovery for robust routing and high performance in mobile ad hoc networks." High Performance Computing and Communications, 2009. HPCC'09. 11th IEEE International Conference on. IEEE, 2009.

[16] Huang, Tsung-Chuan, Kuan-Ping Kho, and Lung Tang. "Hybrid Routing Protocol Based on the k-hop Clustering Structure for MANETs." Intelligent Networks and Intelligent Systems, 2009. ICINIS'09. Second International Conference on. IEEE, 2009.

[17] Macharla, Pradeep, et al. "A QoS routing protocol for delay-sensitive applications in mobile ad hoc networks." Communication Systems Software and Middleware and Workshops, 2008. COMSWARE 2008. 3rd International Conference on. IEEE, 2008.

[18] Priya, S. Padma, and Jayaram Pradhan. “An Efficient Security Framework for Detection and Isolation of Attackers in Low Rate Wireless Personal Area Networks.” Security Technology, 2008. SECTECH’08. International Conference on. IEEE, 2008.

[19] Yang, Jin Seok, et al. “PAMP: power-aware multi-path routing protocol for a wireless ad hoc network.” 2008 IEEE Wireless Communications and Networking Conference. IEEE, 2008.

[20] Kumar, Rakesh, Manoj Misra, and Anil K. Sarje. “A Routing Protocol for Delay-Sensitive Applications in Mobile Ad Hoc Networks.” Ad Hoc and Ubiquitous Computing, 2006. ISAUHC’06. International Symposium on. IEEE, 2006.