International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878 (Online), Volume-8 Issue-2, July 2019

Improved Provoking Trustworthy Routing using Warning Packet Arising Algorithm In Wireless Ad Hoc Network

Febin Sheron P S, K.P.Sridhar

Abstract:*In WAHN nodes are ready to broadcast data packets frequently with maximum usage of energy, unsecure and nodes resource utilization is important they are not controlled bycertificate revocation scheme. Key mixing is difficult to take much time, so sometime the routing nodes, work as well and they are changed to fake mode depending on its behavior. It affects the security of packet transmission.Nodes transmission is broken by wrong link established by intruder nodes. Proposed an Improvedprovokingtrustworthy Routing (IPTR) schemetomeasure the nodes behavior, attacker works good else bad alternatively so they are easily identified based on historical information for particular node which are present in routing path.The warning packet arising algorithm is implemented to provide warning message to next neighbor node in routing path. Current node changes its operating mode to bad state gives a warning signal, so time delay is reduced and improve network lifetime.*

Keywords: *Improved provoking trustworthy Routing, Warning Packet rising algorithm, good else bad mode of operation.*

I. INTRODUCTION

Nowadays, supportive communication isavailable as a capablemethod to increase the communication trust worthinessagainst the difficulties in wireless network [1]. Supportive Communicationdevelops user diversity to emulate multiple-antenna schemes, manufacture use of the packet sharingenvironment of the wireless intermediate nodes forwarding the traffic packets from sender to target node [2]. Thoughsupportive communication brings importantmerits, thisgenerates severe protectionproblems. This is probable for misbehaving nodes to add the network and intermediate nodeunwanted data to the target node, thuscompromise the environment. The obverse of protection, verification is vital for the protection construction [3].Because many hop packet transmissions are used in this networks also supportive communication, it follows hop by hop communication with verification and information reliability are need to secure the network from tamper with and forge of packets by misbehaving nodes.Protection has become the main worry and blockage for generallyfixed in wireless uses [4].

Revised Manuscript Received on 30 July 2019.
***** Correspondence Author
Febin Sheron P S*, Phd Research Scholar, Department of ECE, Karpagam Academy of Higher Education, Coimbatore,India
Dr.K.P.Sridhar, Associate Professor, Department of ECE, Karpagam Academy of Higher Education, Coimbatore,India

These problemsshould have two characteristic: Initial one is the unlockingcollective access intermediatenode is susceptible to intrusion. Another one is the wireless possessionsareseverelyunnatural.
In exacting, supportive communicationhavelot of difficulties to protect the packet transmission, sharing the keys, and organization, applyattack identification withsecurity [5]. Those difficulties are credited to the irregularity of Mobile network, such multihop communication and packet broadcasting, need of network environment, updatableconditions, and node assistance. Protection ismeasured using parameters latency and transmission rate for every packet [6]. This is attractive to adaptively obtainprotectionbased to the accessible resource lacking much presentationpoverty in the network environment.
Securitymanaging is a methodin whichit obtains network behavior in a huge amount of nodes in networkstandpoint. Because the mainperformanceconcerned in management are neighbor finding and rulesassociation, this rulesmanaging is vital role to problem in Mobile network environment, where topologies are updating against time as nodes are changingitsbroadcastingmetrics fortime period [7]. Thenupdatable conditions in mobile network contain importantcrash on the quality of service,mainly for the point to point transmission rate in mobile networks. Conditionmanage is considered to as choosing a group of intermediate nodes to launch rational connections and energeticallychange the broadcasting metrics[8].

It determined on changing the physical layerelse mediumaccess control layer metrics, such as packet transmission energy with intrusion, to improvethe entire network process are energy usage, intrusion [9], and network capability for Mobile network environment. Nowadays, some protection based schemeto control the misbehaving activity of nodes. It attempt to keep outmisbehavingnodes in the network condition when maintaining link,it reduces the damage to the network. Indeed, conditionsmanages thebroken to form a secured network for keysharing, packet sharing, with network management [10]. Though,protection is not a single-layer problem. It should be consideredspanning against the overallconditionload for the entire network communicationenhancement.

Residual of the paper is designed as follows. Section II provides a related works. In section III, we present the details of proposed Adaptive Key Shuffling (AKS) methodobtains a secured communication between wireless nodes, the best routing path is presented. Section IV provides simulation performance results analysis obtained under various metrics. At last section V concludes the paper with future direction.

II. RELATED WORKS

Liu, Wei, et al., [11] presentschemeprovidespermit revocation to separate intruders from further contribute in network characteristics. In fast and correctpermit revocation is applied to the CPRVC-Cluster-based permit Revocation with evidenceabilitymethod. Specifically, to enhances the dependability of the method, toget better the warn nodes to receive part in the permit revocation communication; then improve the accurateness, present the threshold depending method to measure and justify warned nodes as rightful nodes otherwise rejected, earlier thanimproving them. Experimental characteristics of this methods are estimated by eacharithmetical and simulation investigation. Widespreadoutput shows that the presentpermit revocation method is efficient, and capable, to assuranceprotectedpacket transmissionin network environment.

Guan, Quansheng, et al., [12]Proposed both verification and topology manage. In particularly, tomeasure the efficienttransmission rate with upper layer verificationmethods and physical-layer schemes connected to path allocation rules and communicatechoice. JATC joint authentication and topology control method is used to increase the transmission speed. It is invent as a separate stochastic optimization issues that does not need prior best pathpositionexcept only channel approximation. Toconfirm the tracking junctionpossessions and the union rate of the separate stochastic optimization method is implemented. Experimental outputindicates the scheme can significantlyincrease transmission ratio in Mobile network with communication coverage range.Changes the metrics of up-layer securityrulewith PHY-layer communicationimplemented to improve resource consumption, and transmission rates forrouting paths. Aseparate stochastic estimate methodis designed in JATC to contract with the defectiverouteinformation and the energeticallyaltering conditions. Experimental output is proposed to indicate that operates better compared to previous method.

Priyadharshini, et al., [13] propose time with energy for recurrent cluster update and key update. To prevent the out of coverage nodes from availableinformation transmitting, composite key also known asassembly Key is being created. The confidentiality of the assembly key is being stored. Cluster key prevents the problem of certificate and next neighbor nodeparticipation. Commonmodifications the option of key blockswith sharing permissionis minimized. Experimental output indicatestransmission rate, lifespan of network also connection steadiness is improved with lesser energy usage. Present methodobtains minimum packet latency. It also maintains the best connection steadiness between nodes compared to existing scheme.

Thandavarayan,.et al., [14] present new nodeadds into a region itprovides its covert key until dual count of neighbor node list and it transmitstheir covert keys by using asymmetric key encryption. Inall nodescommunicationregion is distinctindividually using its coverage. Whilethere is a misbehavingaction in the network infrastructure the verification algorithm is started to separate the misbehaving nodes. Experimental output, the environment should needs to successfullyseparate themisbehaving nodes in network. Duringwidespreadexperimental investigationin simulator, it obtains that this scheme isresourcefulmethodin the direction ofprotection and simply foridentification of themisbehaving nodes in network environmentwith the minimumenergy utilizedsuccessfully.

Pavlatos, Nikolaos, et al., [15] proposed a several path routing technique depends on the practical OLSR-Optimized Link State Routing protocol known as R-OLSR release OLSR, constructed as anstarting method of the EU-ICT releaseplan. The condition develops its ability to discover and broadcast data packets through several paths depend on dual various relay methods called asSRR-Simple Relay Routing with anARR-Advanced Relay Routing. These conditions are success is substantiating among a simulation situation within a mobile network. The obtainoutputshows that a biasedlosing of packets to improves the chance of acceptingaccurate data packets, increasing the communicationtrustworthiness and communication characteristics.

Le, Tuan, HaikKalantarian, et al., [16] presentdual stage broadcastingMethod which optimize each the estimateconsumption of energy with transmission rate. This reducestheCommunication cost by bunchmany acceptor node into aIndividual data packet copies, also broadcaster countsthe transmission possibilities. This dynamic tree branching method allowscommunicationRoutes to be efficiently communicatedbetweentarget node. Present method to estimatesingle and many hop transmission success ratebased on relay node choosing in routing path.it obtains maximum transmission rate and minimum resource utilization compared to existing method.

Nishanthini, C., et al., [17] present Cooperative communication that provokes limit value crosses by node. It focused on amount of packet and node density. It providessolution against attacker affect communicationalso supports multi packet sharing with same time. Those issues are handledby present cooperative communication. It distinguish its performance with previous method AODV and CORMAN, it obtains higher transmission rate and minimum packet loss during packet transmission time.The overall efficiency of network is improved so time delay is minimized.

Obaidat, Mohammad S., et al., [18] present substitute the security based method by the TDES-Triple Data Encryption Standard, elastic the secure routing technique, main aim to investigate the behavior of the technique anywhere mobile devices that are mismatched with encryption section of mobile network nodes. Indicator in the form of confusion codes is contained in the data packets to support consolidates the data truthfulness. Experimental output shows to confirm the present secure routing technique better compared to previous methods. Present method time delay is reduced, transmission success rate is improved, and amount of packets passing through the wormhole connection.

Zhang, Xin Ming, et al., [19]proposedaintermediate node coverage-based possibility retransmissionmethod for minimizing routing traffic in mobile network. Sequentiallysuccessfullyuse the intermediate coverage information, novel retransmissionlatency to measure the retransmissiondirect,

and then alsoachieve the more accurate extrareporting ratio by monitoringintermediate coverage information. Itslink establishment to obtain the node count. To merging the extra coverage rate and link factors, fixlogical retransmissionchance. This method merges the merits of the intermediate coverage information and the possibility method, it reduce retransmission rate, traffic rate, and increase network lifetime.

Meghanathan, Natarajan. et al., [20] present the opposite of the LET improves the network lifespan. Amongwidesimulation and distinguish with modernless count hop based and steadiness based routing method, to display that SILET findhigh lifespan routing path with minimum hop count value; it, reducing the steadiness hop count trade-off. By good quality of incur minimumpathidentificationmanage traffic occurrencewith minimum hop count per path allocation, the time delay per data packet is also reduced and analyze the minimum cost routing path in mobile network environment compared to existing methods.

III. OVERVIEW OF PROPOSED SCHEME

Ad hoc nodes are broadcast the packet to target node, they consider time and transmission rate. Node behavior is important to identify attacker nodes, normally nodes work in good state, then they are change itstate in bad state, it cause packet drop also time delay for packet transmission from one point to another point in network environment. General network alternative working of node causes difficult to achieve communication in secured manner. Sender sends packet through the available routes in network.

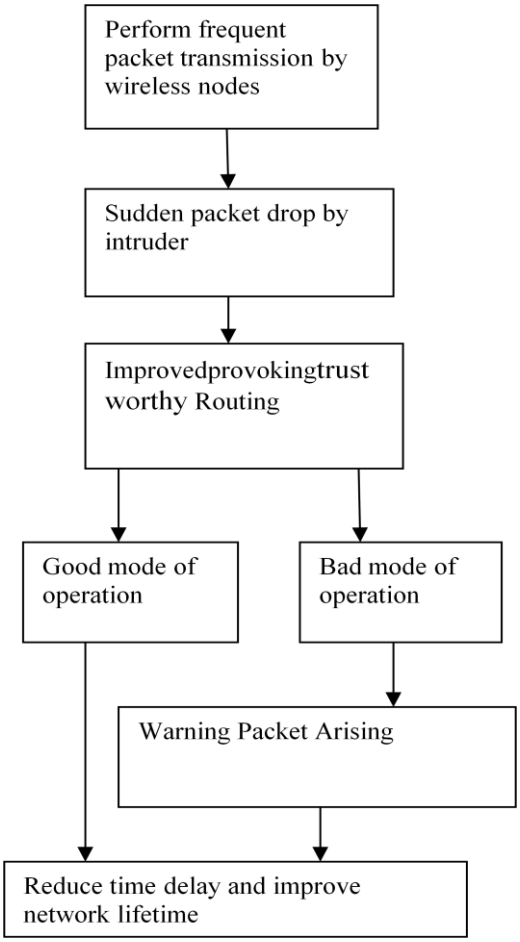


Figure 1: Block Diagram of Improved provoking trustworthy Routing

Figure 1 shows theImprovedProvoking Trustworthy Routing method gives intrusion free packet sharing between wireless nodes. Sender frequently broadcast the information to target node. IPTR scheme identifies the mode of operation for each wireless node, if it is good perform continuous communication else it is bad packet loss made that time warning packet arise to intermediate node, so lifetime of network is increased and time delay is minimized.

Sudden packet drop is made by attacker node, which operate two modes they are good and bad mode. Good mode is changed any time in network, node data's are forwarded constantlysome disturbance made, and they are detected by improved provoking trustworthy routing. Bad node loss packet warning packets are transmitted to remaining neighbor node, which are present in routing path.

3.1Frequent Data packet broadcasting through path

Sender transmits the several packets in frequent manner, through an intermediate nodePerform packet sharing. Startingbefore signed process is considered to operate in essentialend and wait, no packet shared since node energy is down so process is ended and node is busy so waiting stated. When packet is broadcasted by the sender, it is success also send reply packet by destination node through the routing path.Time is taken byPacket broadcasted in the routing path.Transmission rate is estimated based speed of node and resource usage of node. Packets are not directly broadcasted to target node. Regularly huge amount of packets are broadcasted to allocated path. Here a self-organized theory is used tobind the join in the group. Originally, a request packetis transferred withhigher energy consumed path also takes so much oftime. While thisrequest packet is received by all nodes in routing path, which are estimate thelocation and reservation of the intermediate nodes for next cycle of packet transmission. Sendernode choosesasuitableresource utilizationscheme. Single hop intermediate node is integrated in the request packet and broadcasted. While next relay node are available in the particular coverage area, then the range is minimizedat rest. $C(P)$ Continuous packet transmission, and Fre_{pack} is frequent allocation.

$$Fre_{pack} = C(P) - (1)$$

Occupy the connection between nodesalso neighbor node identification processes proficient by the sharing data packets. The connection searching process establisheswhether the link between wireless nodesalso its single hop nodes are transmit and receive packets based on antenna is bidirectional. It is proficientamong the applied of the connection group nodesthatmaintains each the single hop next neighbor nodes. All node surrounded by the network populate its connection group to provide a single hop packet transmission with their next neighbor nodes in routing path. Relaydiscovery process occupycount of the Neighbor also atwo hop Neighbor group thatcontains the databased on the connection and location of single and two hop intermediate nodes.

During the connectionsearching process nodes have previouslygenerate and modified the connection groups. Correspondingly to the Connection group, the intermediate node is consequentlychangeddepends on location details of single hop relays. Groupregularlygenerate, modifies and rejects the relaynodes depending on the uniquerouting. The two hop intermediate groupamong the interruptedsharing of packetsorganizes to comprisenodes that keepa constant connectionwith constant relay nodes. $T(s)+A$ is Transmission speed and accuracy, $LC*t$ is link connection with time slot.

$$C(P)=T(s)+A-(2)$$

$$T(s)=LC*t-(3)$$

All nodes generate and keeps a routing table that maintains data packet consider to every present paths to the target node location. Connection between node details and routing details are maintained in routing table and the condition set depends on theData acquired through the time based sharing of data packets. Itimplement the re-estimation of path stored in the routingtable subsequent the rules of secure routingwhen a modification occurred in the connection group, the intermediate group, the two hop neighbor group with the condition group.

3.2 Improved provoking trustworthy Routing

In initial statea rightful node accurately accuses an intruder node, output in the reproving node and attacker node initially detect in the current routing path, correspondingly.Next state is the pointing of a misbehaving node in the routing path since it transmits wrongallegationover a rightful node. Therefore, nodes in the routing path may be rightful nodes elseattacker nodes. Consequently, to enhance the dependability and correctness, nodes must be distinguished among the trust nodes and misbehaving nodes, so as to discharge trust nodes from the routing path alsocontain attacker nodes in the routing path. To separate thetrusty nodes from attacker nodes that are present in network environment, present provoking trustworthy routing scheme to estimate and discover trusty nodes from the routing path.

$$LC=\max_{s} C-(4)$$

Itconstructs a timer for the packet transmission, to trace the amount of accusationoverallattackernodes in routing path. Alng with that, the nodes continues toaccept the data packets over the blame node subsequent a timer count is increased when it successfully received otherwise timer does not increase that is applied for organizingoriginal data and use trusty nodes from the routing path, and consequently distinguish the amount of received data with the limit.

$$T(s)=\max_{s} C*t-(5)$$

Intruder node as a real attacker node, whetheramount of wrong datareaches thelimits in particular communication. In certain time period, thenresultmaintain the equivalentattacker node as a rightful node so as to reject it from the routing path as well as re-establish its process as the usual node. If its, whetheramount of blamenot succeed to reach limit, the linkedintruder nodesneed toarrest in the routing path. Specifically in aindividualcondition, whether the time slot is fixed to unlimited, this method is same to the non-voting-based methodbecause the trusty node in the routing path should notconvince the rejection rule. As Significance, influential the amount of limit is necessary for trustworthiness and correctness of this method. $R(n)$resource utilization for each node.

$$t=R(n)-(6)$$

Whether the limit is fix to maximum level, it use a more time slot to detectattacker node is a not a trusty node since this schemehas to wait for more loss of data to reach the decision; amisbehaving for no reason detectedsince of require of sufficientmaintain from intermediate nodes. Uniformly, whenthe predefined limit is fixedminimum level, revokemisbehavingnodes shouldremovefrom the routing path by remainingmisbehaving nodesamongagreement. To diminish these tremendous conditions, present to establish the optimallimit value dependson the amountof intermediate nodes with the engagedprotection strategy.

$$T(s)=\max_{s} C*R(n)-(7)$$

The amounts of intermediate nodes are available in routing path. In specific time slot, the specifiednode crossesamong an area and meet anamount of next relay nodes. Becausewireless nodes are believed uniformly in the network environment, node behavior is changed into good to bad condition, they are identified and removed in routing path, so packet latency is reduced and the lifespan of network nodes are improved.

Algorithm for Improved provoking trustworthy Routing

Step1: For each analyze routing path.
Step 2:Frequent transmitting packets along path.
Step3:Monitor time allocation for particular transmission.
Step 4: If{node= good}
Step 5: node perform communication
Step 6: search next neighbor node
Step 7: else
Step 8: if {node==bad}
Step 9: fake node are detected
Step 10: not perform communication
Step 11: reject that node from connection
Step 12: end if
Step 13: end for

3.3 Warning Packet Arising

Node characteristics are clearly monitored and it arise warning packets when node suddenly changes its behavior to bad. The mode of operation is altered every time good to bad, so using improved provoking trustworthy Routing applied to filter out the misbehaving node currently present in routing path.Intermediate relay nodes can perfectly blame the intruder which it is not a trusty node so that areefficiently removed from the routing path.$W(P)$weight of packet

$$C(P)=\max_{s} C*R(n)+A-(8)$$

$$A=W(P)-(9)$$

The possibility of a node that is contributes in correct blame. Sequence to obtain a highpossibility of effectively rejecting trusty nodes fromthe routing path, the amount of packet transmission succeedas maximum. To select ansuitable range of limit to obtain the higher correctness ofadding nodes in routing path that can improves correct dischargepossibility whenconcurrentlypreservesmall fake dischargepossibility. A connection considers to areasonablepath allocation for two intermediate relay nodes operating probablyin best of the communication modes. Effective kind of communications with the efficient intermediate node are measured according
to the current pathsituation. To consideronly dual-hop communicationbecauseseparating arelay node connection into more hops shouldlaunches more duplicate of packetsin the network environment.

$$C(P) = \max_{s} C * R(n) + W(P) - (10)$$

$$Fre_{pack} = \max_{s} C * R(n) + W(P) - (11)$$

Protection rate of packet transmission in particular routing path is increased. Warning message packet is arise when bad node performing an communication. It drops or misuses those data they are initially detected and rejected from routing path.Because it use only higher efficient nodes from starting point to ending point, so time delay is minimized and network lifetime is prolonged.

Warning Packet Arising Algorithm

Step 1: Routing path is established.
Step 2: for each discover efficient connection based routing path
Step 3: if {node==trusty}
Step 4: Protection based communication is performed.
Step 5: increase lifespan of network
Step 6: else
Step 7: if {node==fake}.
Step 8: create warning packet that are broadcasted to neighbor nodes
Step 9: reduce time delay
Step 10: End if
Step 11: End for.

This scheme improves the security, so all packet are delivered successfully from source node to destination node. There is no need to rebroadcast the data packets so packet latency is minimized, intruder nodes are earlier to detect and reject from routing path in network.

Packet ID: Packet ID containsall wireless ad hoc nodeinformation. This indicates the individual node characteristics and routing table maintenance of nodes.

Source ID	Destination ID	Frequent Data packet broadcasting through path	Improved provoking trustworthy Routing	Warning Packet Arising	Improving network lifetime
4	4	4	6	3	5

Figure 2: Proposed IPTRPacket format

In figure 2: the proposed IPTRpacket format is shown. Here the source and destination node ID field takes 4 bytes. Third one is Frequent Data packet broadcasting through pathcarries 4 bytes. Sender transmits data continuously in allocated routing path. In fourth field occupies 6 bytes. Improved provoking trustworthy Routing, it provides the trigger for choosing trusty node in routing, also separate true and bad node in network.In fifth occupies 3 bytes,Warning Packet Arising, whether there is any intruder or fake node available gives warning message packet to neighbor or sender node in routing path. The Improving network lifetime, it occupies 5bytes; to selects trusty node to achieve efficient connection based routing.

IV. PERFORMANCE EVALUATION

A. Simulation Model and Parameters

The proposed IPTR is simulated with Network Simulator tool (NS 2.34). In our simulation, 100 wireless ad hoc nodes are placed in a 1010 meter x 980 meter square region for 18 milliseconds simulation time. Each Mobile node goes random manner among the network in different speed. All nodes have the same transmission range of 250 meters. CBR Constant Bit Rate provides a constant speed of packet transmission in network to limit the traffic rate. DSDVDestination sequence distance vector routing protocol is used to protection based communication with best connection path. Table 1 shows Simulation setup is Estimation.

Table 1: Simulation Setup

No. of Nodes	100
Area Size	1010 X980
Mac	802.11g
Radio Range	250m
Simulation Time	18ms
Traffic Source	CBR
Packet Size	512 bytes
Mobility Model	Random Way Point
Protocol	DSDV

Simulation Result: Figure 3 show that the proposed IPTRmethod obtainsprotection and connection based efficient routingcompared with existing ERLC [15] and TLMR[16]. IPTRcheck and detect the fake node behavior in routing path, while any fake node available, it generates the warning message given to neighbor node in routing path. Itincrease network lifetime and reduce time delay.

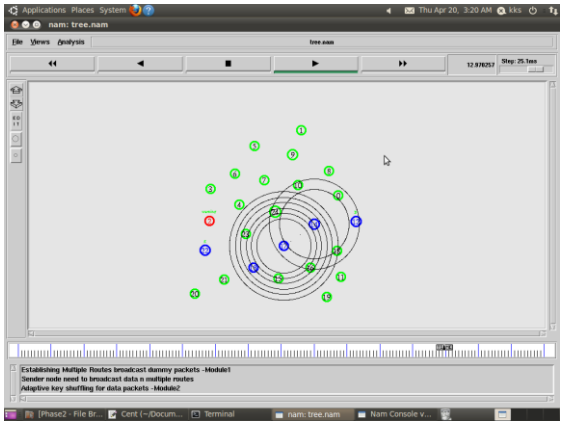


Figure 3: Proposed IPTR Result

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 used for packet transmission from source node to destination node, fake node available in network, it provides the warning message alert to protect the communication. In proposed IPTR method end to end delay was reduced compared to existing method ERLC, AKS, and TLMR.$\boldsymbol{EndtoEndDelay = EndTime - StartTime}$

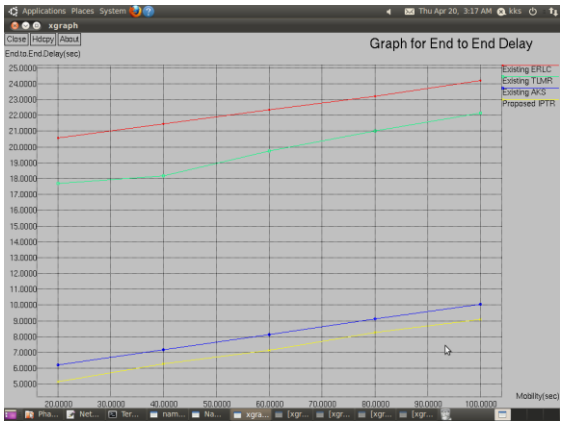


Figure 4: Graph for Mobility vs. End to End Delay

Communication overhead: Figure 5 shows communication overhead is minimizedin whichsender transmit packet to receiver node, it detect and remove the fake node which available in routing path, protected communication is performed. In proposed IPTR method Network overhead is minimized compared to existing method ERLC, AKS, and TLMR.

$$\boldsymbol{Communicationoverhead = (NumberofPacketLosses/Received) * 100}$$

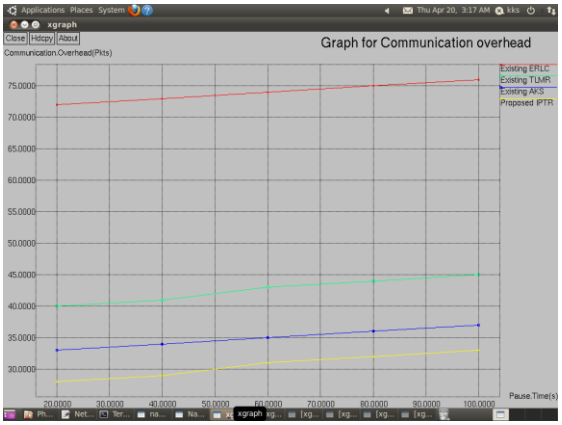


Figure 5: Graph for Pause time vs. Communication overhead

Packet Delivery Ratio: Figure 6 shows Packet delivery ratio is measured by no of received from no of packet sent in particular speed. Node velocity is not a constant, simulation mobility is fixed at 100(bps). In proposed IPTR method Packet delivery ratio is improved compared to existing method ERLC, AKS, and TLMR.

$$\boldsymbol{PacketDeliveryRatio = (Numberofpacketreceived/Sent) * speed}$$

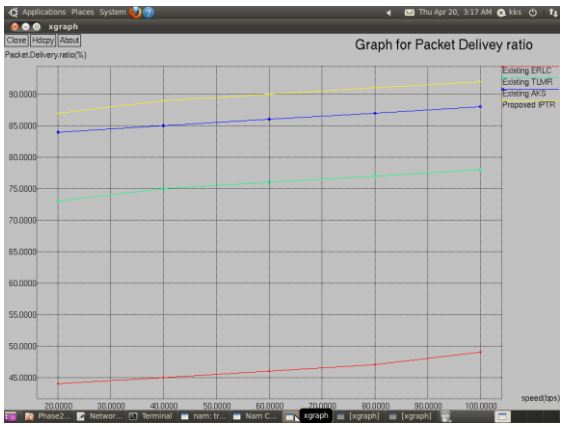


Figure 6: Graph for Nodesvs. Packet Delivery ratio

Detection efficiency: Figure 7 shows detection efficiency, attacks are occurred packet transmission is repeated from source node to destination node. The frequent transmission is continues since IPTR identify intruders present in network. In proposed IPTR method detection efficiency is improved compared to existing method ERLC, AKS, and TLMR.

$$\boldsymbol{Detectionefficiency = attackdetectionrate/overalltime}$$

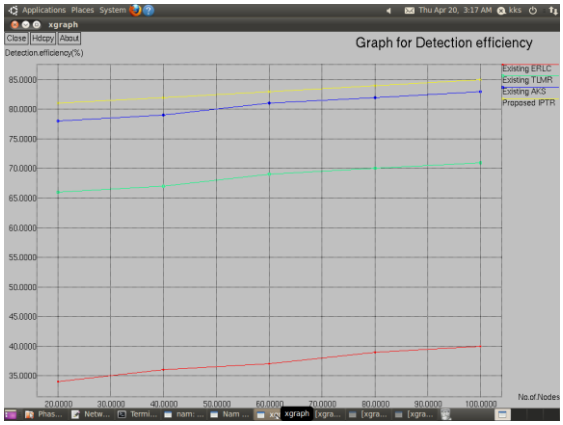


Figure 7: Graph for Nodes vs. Detection efficiency

Network Lifetime: Figure 8 show thatLifetime of the network is measured by nodes process time taken to utilize network from overall network ability, no keys are used, since warning alerts are provided to neighbor nodes. In proposed IPTR method, the network Lifetime is increased compared to existing method ERLC, AKS, and TLMR.

$$NetworkLifetime = timetakentoutilizenetwork/overallability$$

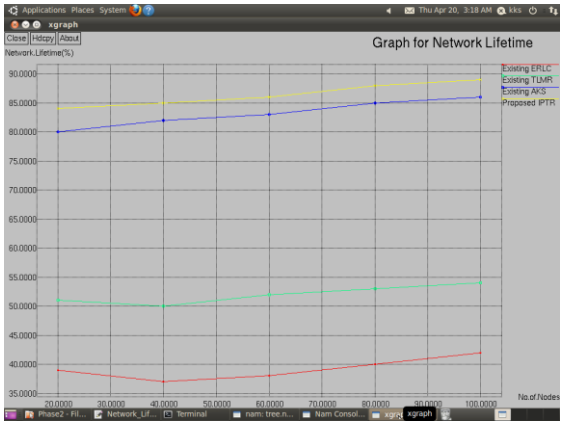


Figure 8: Graph for Nodes vs. Network Lifetime

Connectivity ratio: Figure 9 shows thatconnectivity ratiobetween two nodes is estimated very timein network, time taken to complete particular communication with particular transmission speed use warning alert generation. In proposed IPTR method, thePacket Integrity rate is improved compared to existing method ERLC, AKS, and TLMR.

$$Connectivityratio = \left(\frac{Packet\ transmission\ rate}{timetaken}\right) * 100$$

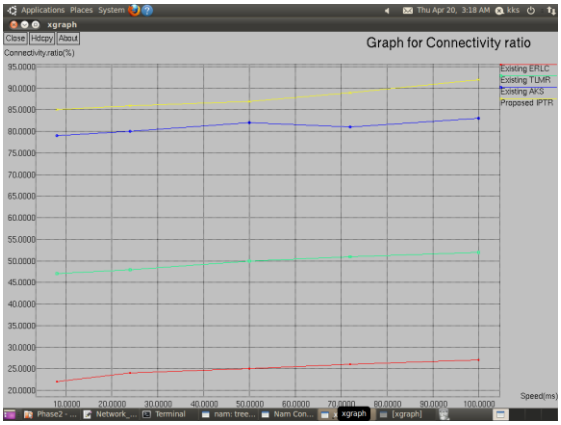


Figure 9: Graph for Speed vs. Connectivity ratio

V. CONCLUSION

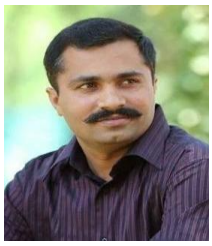
In wireless nodes, which should perform communication with poor connection among nodes, so nodes alter its behavior in any time, such as it perform trusty communication they changed to fake communication, it also cause more time delay and minimum network lifetime, and more resource is utilized. ProposedIPTRmethod to obtain a protection based efficient communication, this analyze routing node in path also detect the bad node behavior to remove that node from entire network. If any fake node performs communication they give warning message packet to remaining neighbor node in network environment. In future presentsUpdatable link with cross layer optimization to measure various parameters.

REFERENCES:

1. H. Yang, H. Luo, F. Ye, S. Lu, and L. Zhang, “Security in Mobile Ad Hoc Networks: Challenges and Solutions,” IEEE Wireless Comm., vol. 11, no. 1, pp. 38-47, Feb. 2004.
2. P. Sakarindr and N. Ansari, “Security Services in Group Communications Over Wireless Infrastructure, Mobile Ad Hoc, and Wireless Sensor Networks,” IEEE Wireless Comm., vol. 14, no. 5, pp. 8-20, Oct. 2007.
3. A.M. Hegland, E. Winjum, C. Rong, and P. Spilling, “A Survey of Key Management in Ad Hoc Networks,” IEEE Comm. Surveys and Tutorials, vol. 8, no. 3, pp. 48-66, Third Quarter 2006.
4. L. Zhou and Z.J. Haas, “Securing Ad Hoc Networks,” IEEE Network Magazine, vol. 13, no. 6, pp. 24-30, Nov./Dec. 1999.
5. L. Zhou, B. Cchneider, and R. Van Renesse, “COCA: A Secure Distributed Online Certification Authority,” ACM Trans. Computer Systems, vol. 20, no. 4, pp. 329-368, Nov. 2002.
6. H. Chan, V. Gligor, A. Perrig, and G. Muralidharan, “On the Distribution and Revocation of Cryptographic Keys in Sensor Networks,” IEEE Trans. Dependable and Secure Computing, vol. 2, no. 3, pp. 233-247, July 2005.
7. P. Yi, Z. Dai, Y. Zhong, and S. Zhang, “Resisting Flooding Attacks in Ad Hoc Networks,” Proc. Int’l Conf. Information Technology: Coding and Computing, vol. 2, pp. 657-662, Apr. 2005.
8. B. Kannhavong, H. Nakayama, A. Jamalipour, Y. Nemoto, and N.Kato, “A Survey of Routing Attacks in MANET,” IEEE WirelessComm. Magazine, vol. 14, no. 5, pp. 85-91, Oct. 2007.
9. H. Nakayama, S. Kurosawa, A. Jamalipour, Y. Nemoto, and N.Kato, “A Dynamic Anomaly Detection Scheme for Aodv-BasedMobile Ad Hoc Networks,” IEEE Trans. Vehicular Technology,vol. 58, no. 5, pp. 2471-2481, June 2009.
10. J. Newsome, E. Shi, D. Song, and A. Perrig, “The Sybil Attackin Sensor Network: Analysis & Defenses,” Proc. Third Int’lSymp. Information Processing in Sensor Networks, pp. 259-268,2004.

11. 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.
12. 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.
13. Priyadharshini, M. Ramya, S. Prasanna, and N. Balaji. "Energy and mobility based group key management in mobile ad hoc networks." Recent Trends in Information Technology (ICRTIT), 2014 International Conference on. IEEE, 2014.
14. Thandavarayan, Gokulnath, K. Sangeetha, and Selvaraj Seerangan. "ORZEF: An optimized routing using zone to establish security in MANET using multipath and friend-based ad hoc routing." Pattern Recognition, Informatics and Medical Engineering (PRIME), 2012 International Conference on. IEEE, 2012.
15. Pavlatos, Nikolaos, et al. "A multipath mobile ad-hoc routing protocol for enhanced reliability in lossy communications." Telecommunications and Multimedia (TEMU), 2016 International Conference on. IEEE, 2016.
16. Le, Tuan, Haik Kalantarian, and Mario Gerla. "A two-level multicast routing strategy for delay tolerant networks." Ad Hoc Networking Workshop (MED-HOC-NET), 2015 14th Annual Mediterranean. IEEE, 2015.
17. Nishanthini, C., and G. Rajkumar. "Congestion avoidance through cooperative routing in MANETs." Information Communication and Embedded Systems (ICICES), 2013 International Conference on. IEEE, 2013.
18. Obaidat, Mohammad S., et al. "Preventing packet dropping and message tampering attacks on AODV-based mobile ad hoc networks." Computer, Information and Telecommunication Systems (CITS), 2012 International Conference on. IEEE, 2012.
19. Zhang, Xin Ming, et al. "A neighbor coverage-based probabilistic rebroadcast for reducing routing overhead in mobile ad hoc networks." IEEE transactions on mobile computing 12.3 (2013): 424-433.
20. Meghanathan, Natarajan. "A unicast MANET routing protocol to simultaneously minimize the stability-hop count tradeoff and end-to-end Delay." Information Technology: New Generations (ITNG), 2012 Ninth International Conference on. IEEE, 2012.

AUTHORS PROFILE



Lt. Dr. K. P. SRIDHAR received the B.E. Electronics and Communication Engineering from Mahalingam College of Engineering and Technology, Pollachi, in 2008, and the M.E. and Ph.D. degrees in Electronics and Communication Engineering from the Anna University, Coimbatore and Karpagam University, Coimbatore in 2011 and 2016, respectively. Since July 2010, he has been with the Department of Electronics and Communication Engineering, Karpagam University, where he is an Associate Professor. His current research interests include Sensor Fusion Device, PSO Neural Network, Wireless Sensor Fusion System, Biometric Voting System, and Humanoid Robot for Mines & Disaster

Febin Sheron P S received the B.E. Electronics andCommunication Engineering from Jayaram College of Engineering and Technology, Tiruchirappalli, in 2004, and M.Tech in Embedded systems from University of Calicut. Pursuing Ph.D in Karpagam Academy of Higher Education since July2013.Currently working as a Project Manager at Robert Bosch Engineering and business solution Limited since 2008. Current research interests include Communication and Networking.