iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 6 **Issue:** IX **Month of publication:** September 2018

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 6 Issue IX, Sep 2018- Available at www.ijraset.com

Improving Performance of Wireless Ad Hoc Network Using Routing Protocol

Dr. S.A. Arunmozhi[1], Vinobharathi. V[2]
[1, 2]*Electronics and Communication Engineering, Saranathan college of Engineering, Trichirapalli, Tamilnadu*

Abstract: ***In wireless adhoc networks, the end-to-end data communication is needed to collect data from source to destination. It suffers from several constraints, like low computation capability, less storage capability, restricted energy resources, liability to physical capture, and therefore the use of insecure wireless communication channels. As the size and the density increases over the network, there are more chances of penetration of security in such network. These constraints build "security" in mobile ad hoc network challenge. Most of the protocols designed for mobile ad hoc networks consider energy efficiency but not security as a goal. In this present work, a trust sensing-based secure routing mechanism (TSSRM) is designed to provide the security over the network. The presented work is a hybrid approach that performs the reliable node identification and provides the communication over the safe node. The presented work is divided in three main layers. In the first layer, the protocol level change is performed over the network. In the second layer, we have defined an authentication mechanism to generate private and shared keys for every node in the network. At the third level of this presented work, a reliable routing approach is suggested. The trust analysis is performed here based on the honesty, reliability and the effective parameters. To demonstrate the utility of the proposed routing protocol, we apply it to a network having blackhole attack. For each node, we identify the best trust composition and formation to maximize application performance. The presented routing mechanism is an effective and reliable communication approach that can take the decision on next hop selection under the trust vector. Only a trustful node is eligible to transmit data over the network. TSSRM is compared with AOMDV routing protocol and the results of our work has shown in ns2 simulation software.***

Index Wireless ad hoc network, optimal route, security, QoS metrics, trust degree.

I. INTRODUTION

The performance of computer and wireless communications technologies has advanced in recent years. As a result, it is expected that the use and application of advanced mobile wireless computing will be increasingly widespread. Much of this future development will involve the utilization of the Internet Protocol (IP) suite. Mobile ad hoc networks (MANETs) are envisioned to support effective and robust mobile wireless network operation through the incorporation of routing functionality into mobile nodes. These networks are foreseen to have topologies that are multi hop, dynamic, random, and sometimes rapidly changing. These topologies will possibly be composed of wireless links that are relatively bandwidth-constrained [1]. In MANETs, the limited battery capacity of a mobile node affects network survivability since links are disconnected when the battery is exhausted. Therefore, a routing protocol considering the mobile nodes energy is essential to guarantee network connectivity and prolong the network lifetime [2]. Power-aware routing protocols deal with the techniques that reduce the energy consumption of the batteries of the mobile nodes. This approach is basically done by forwarding the traffic through nodes that their batteries have higher energy levels. This will increase the network lifetime.

In this paper, nodes instead of forwarding the packets to all the encountered neighboring nodes, select only the appropriate node. The selection of appropriate node is based on the distance and energy level. Firstly, only the neighboring nodes having distance less than neighbor discovery range are considered as neighboring nodes. Then neighboring nodes are filtered by calculating the distance to destination. Nodes which have distance less than average distance are selected as neighboring nodes. Then the appropriate node is selected which has comparatively higher energy. The node with higher energy is selected because it has high chances of surviving in the network compared to other nodes. This prevents from packets being dropped due to low energy at the nodes. Approximate distance to destination is measured in order to reduce the number of hops. Decision of selecting an appropriate node is done at every hop. So with this solution life time of the network can be increased by consuming energy in the network by reducing the number of transmissions. This process presents a routing mechanism which aims at reducing energy consumption in the network. This is done by avoiding broadcasting of messages to all the neighboring nodes thus reducing the number of transmissions in the network.

This paper is structured as follows: Section II describe about literature survey, section III describes methodology, lastly conclusion are draw in section IV.

II. LITERATURE SURVEY

Opportunistic Network consists of 100 numbers of nodes which are mobile. When source node comes in contact with other nodes which are within its communication range, it filters the nodes based on their distance and residual energy levels. Only an appropriate node with high energy compared to all other nodes and whose distance to destination is comparatively less is selected as the next hop. The same procedure is applied for the next hop and is repeated until the destination node is found. Once destination is found message is delivered. In the proposed solution it is assumed that nodes have some regularity in their movements [3]. In FFAOMDV algorithm, nodes instead of forwarding the packets to all the encountered neighboring nodes, select only the appropriate node. The selection of appropriate node is based on the distance and energy level[4]. Firstly, only the neighboring nodes having distance less than neighbor discovery range are considered as neighboring nodes. Then neighboring nodes are filtered by calculating the distance to destination. Nodes which have distance less than average distance are selected as neighboring nodes. Then the appropriate node is selected which has comparatively higher energy. The node with higher energy is selected because it has high chances of surviving in the network compared to other nodes. This prevents from packets being dropped due to low energy at the nodes. Approximate distance to destination is measured in order to reduce the number of hops. Decision of selecting an appropriate node is done at every hop. So with this solution life time of the network can be increased by consuming energy in the network by reducing the number of transmissions[5]. This process presents a routing mechanism which aims at reducing energy consumption in the network. This is done by avoiding broadcasting of messages to all the neighboring nodes thus reducing the number of transmissions in the network[6].

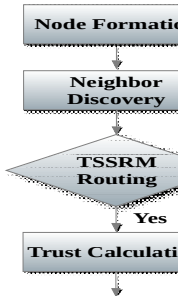
III. METHOTOLOGY

A novel routing algorithm which used for reducing the routing overhead of network is proposed in this section. Proposed a Trust Sensing based Secure Routing Protocol (TSSRM) in this process. The Trust Detection protocol algorithm is used to find the neigh bore node of in this network. Calculation of Nodal Trust Algorithm - During data routing and detection routing, every node will perform a nodal trust calculation to aid in black hole avoidance. These modules closely interact to coordinate the functions of misbehavior detection, discovery of trustworthy routes, and evaluation of the reputation of peers.We consider a wireless sensor network consisting of sensor nodes that are uniformly and randomly scattered in a circular network; the network radius is R, with nodal density ρ, and nodes do not move after being deployed. Upon detection of an event, a sensor node will generate messages, and those messages must be sent to the sink node.We consider that link-level security has been established through a common cryptography-based protocol. Thus, we consider a link key to be safe unless the adversary physically compromises either side of the link. The adversaries model: We consider that black holes are formed by the compromised nodes and will unselectively discard all packets passed by to prevent data from being sent to the sink. The adversary has the ability to compromise some of the nodes. However, we consider the adversary to be unable to compromise the sink and its neighboring nodes. The data collection has better security performance and strong capability against black hole attacks. The main goal of our scheme is to ensure that the nodal data safely reach the sink and are not blocked by the black hole. Thus, the scheme design goal is to maximize the ratio of packets successfully reaching the sink. Consider that the number of packets that are required to reach the sink is M and that the number of packets that ultimately succeed in reaching the sink is m; the success ratio is q = m/M. Active detection routing protocol: A detection route refers to a route without data packets whose goal is to convince the adversary to launch an attack so the system can identify the attack behavior and then mark the black hole location. Thus, the system can lower the trust of suspicious nodes and increment the trust of nodes in successful routing routes. Through active detection routing, nodal trust can be quickly obtained, and it can effectively guide the data route in choosing nodes with high trust to avoid black holes. The active detection routing protocol is the scheme, the source node randomly selects an undetected neighbor node to create an active detection route. Considering that the longest detection route length, the detection route decreases its length by 1 for every hop until the length is decreased to 0, and then the detection route ends. Data routing protocol. The data routing refers to the process of nodal data routing to the sink. The routing protocol is similar to common routing protocols in WSNs; the difference is that the route will select a node with high trust for the next hop to avoid black holes and thus improve the success ratio of reaching the sink. The routing protocol can adopt an existing routing protocol, and we take the shortest route protocol as an example. Node a in the route will choose the neighbor that is nearer the sink and has high trust as the next hop. If there is not a node among all neighbors nearer the sink that has trust above the default threshold, it will report to the upper node that there is no path from a to the sink. The upper node, working in the same manner, will

re-select a different node from among its neighbors nearer the sink until the data are routed to the sink or there is conclusively no path to the sink. In the ActiveTrust scheme, the trust calculation should meet the following condition. If the node is found to be malicious in the latest detection, then its trust should be below the threshold, and the node will not be chosen for later routing. If the malicious node returns to the normal node, it needs several detections to take it into routing consideration; The core idea of data routing is that when any node receives a data packet, it selects one node from the set of candidates nearer the sink whose trust is greater than the preset threshold as the next hop.

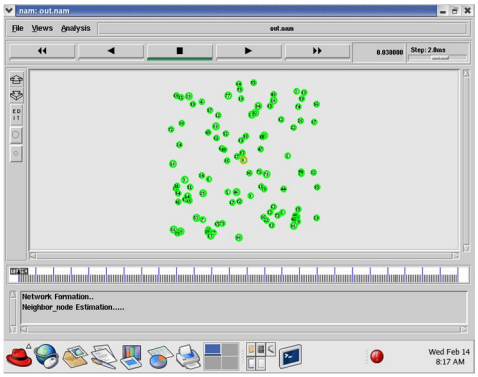
A. System Design

Block Diagram



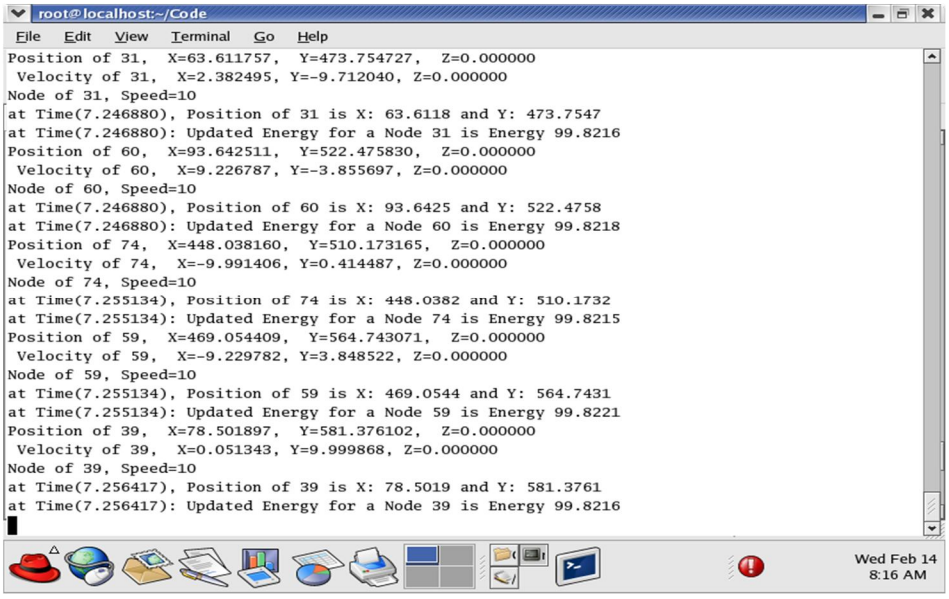
B. Modules Description

1) Network Formation: Network formation is illustrated as shown in Figure 4.1 an aspect of creating nodes of network and transmits data. The decentralized nature of wireless sensor networks makes them suitable for a variety of applications where central nodes can't be relied on, and may improve the scalability of wireless ad hoc networks compared to wireless managed networks, though theoretical and practical limits to the overall capacity of such networks have been identified. Minimal configuration and quick deployment make ad hoc networks suitable for emergency situations like natural disasters or military conflicts. The presence of a dynamic and adaptive routing protocol will enable ad hoc networks to be formed quickly. Network of 100 nodes is created using network simulator for wireless sensor network.

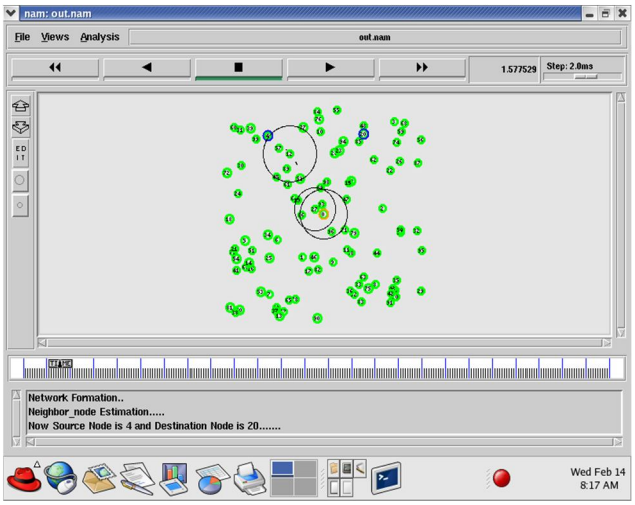


*2) Neighbor Node Discovery***:** On-demand reactive routing protocol that uses routing tables with one entry per destination. When a source node needs to find a route to a destination, it starts a route discovery process, based on flooding, to locate the destination node. Upon receiving a route request (RREQ) packet, intermediate nodes update their routing tables for a reverse route to the source. Similarly, the forward route to the destination is updated upon reception of a route reply (RREP) packet originated either by the destination itself or any other intermediate node that has a current route to the destination. The detection of neighbors for packet relay is an important factor for wireless network. Better identification of next hop in routing provides a

collision free packet forwarding even under a high traffic scenario. The proposed neighbor discovery process allows mobile nodes to broadcast the discovery packets using probability measurement. It can execute the discovery process immediately, when it detect the termination of the neighbor discovery phase. To select optimal routers for routing using an efficient neighbor discovery process. To reduce the routing overhead using probability based route discovery approach. Contribution to further reduce the routing overhead, the proposed work improves the accuracy of probability measurement by removing common neighbors between two nodes.



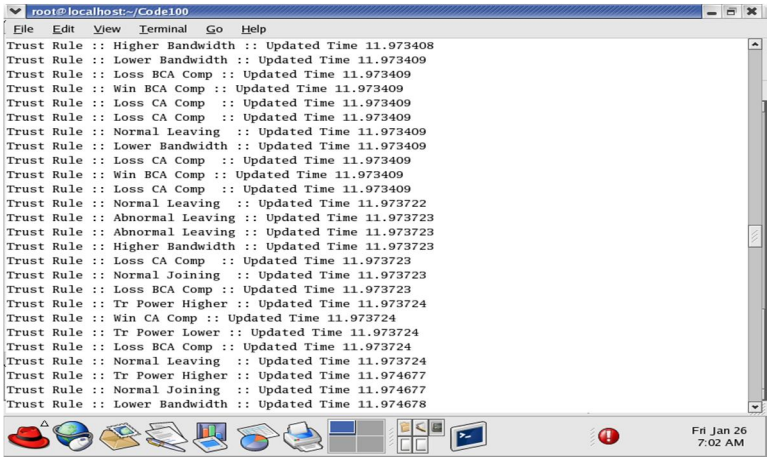
3) Tssrm Routing Process: Source node initializes the process of trust derivation and transmits the trust request packet TR to its neighbors. When it is ready to transmit message to node destination node. The trust request packet is expressed as TR. It consists of identity of assessing node and assessed node, threshold and times- tamp. hl represents the hop counter of TR,hl is positive integrand decreases with the increasing of the number of forwarding. hl should not be set too large in order to reduce the flooding overhead caused by the trust transmission. Neighbor needs to check the freshness firstly after receiving the trust request packet, and the request will be abandoned if it is duplicate, otherwise the request will be broadcast identity of assessing to all the neighbor nodes. The neighbor nodes will send the trust reply to node source node through the reverse route after receiving the trust request packet. However, all the neighbor nodes that received the request will discard the request and no longer forward it if the value of hop count in the trust request packet is decremented to zero. After obtaining the parameters provided by the neighbor nodes then source node will evaluate the trust status of neighbor node by combining direct trust, indirect trust and incentive factor. Then source node determines whether nodes can be relay node according to the constraint condition of trust route. Source node can obtain a credible forwarding and send routing requests of the nodes according to the constructed trust calculation model. If there is an optimal route to destination node in the credible node routing table, any intermediate credible node that receives routing requests will send a reply to source node so that the optimal route from source node to destination node can be obtained. In this case, go to initial stage will be repeated to find the next credible node if there is no optimal route to destination node in the credible node routing table that received the routing requests. Destination node will send a reply to source node via the reverse route according to the routing algorithm. The source node will send a packet to the destination node via the constructed optimal route. Considering that the direct trust derivation model mainly depends on its own detection system, which produces a little communication overhead. However, the indirect trust model is inseparable from the communication overhead since it involves the information interaction between recommended nodes. The TSSRM constructed in this paper only selects the suggestions provided by neighbor nodes of the evaluated node, which control the recommended range and reduce the communication overhead in the process of information transmission. In addition, the combination of direct trust, indirect trust and incentive factor can effectively detect the nodes which give up relay forwarding to save energy, so as to expel attack nodes from the credible route quickly.



4) *Trust Value Calculation*: The proposed Trust based Management Framework gives an overview about trust in wsn. It works on the concept of trust factor in (initialization phase), for selecting the most efficient route and a routing path is evaluated using the concept of trust value that is updated during the route exchange process. To find the shortest path from source to destination. To choose the best path by using the appropriate route selection mechanism. The contribution is Trust and Highly stable greedy forwarding. In wsn if forwarding nodes have high mobility, may chances to make local topology inaccuracy. If the node involved in the forwarding path node moves frequently then there is the situation of link failure which leads to packet loss. Hence it is required to select the nodes with low mobility which means selection of stable node as forwarder based on its mobility. Mobility based forwarding node selection scheme improves the routing performance. This module calculates the Trust value on the basis of three parameters

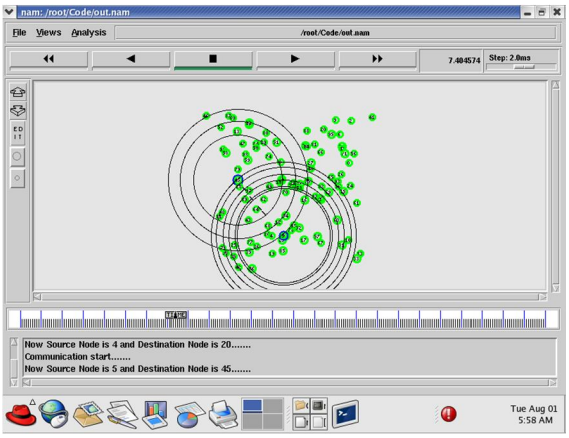
a) Energy
b) Packet Count
c) Queue Size

When current trust value is greater than 0.7, there may be a selfish node in the network. If the selfish nodes are identified then it is added to block list. Otherwise the data send to destination.



5) *Attacker Detection*: The common trust mechanisms and detection algorithms are difficult to handle on-off attack and bad mouthing attack effectively. Since TSSRM combines behavior with energy and introduces SEDTF in the process of constructing com- prehensile trust degree, it can effectively identify the above attack behaviors of the trust degree (TD) usually increases with time if there is no abnormal phenomenon (from 20s to 70s). But the trust degree will decline when the malicious nodes activate on-off attack (from 70s to 100s). When the SEDTF is utilized for TSSRM to handle on-off attacks, as time goes on, the more accurate the judgment for the trust of malicious node is, the higher accuracy of trust evaluation is, because the SEDTF makes that bad behavior will be memorized for a longer time than good behavior

6) *Data Transmission*: Route request send to all intermediate nodes between source and destination. Route discovery for shortest and freshest path. When a source node needs to find a route to a destination, it starts a route discovery process, based on flooding, to locate the destination node. Upon receiving a route request (RREQ) packet, intermediate nodes update their routing tables for a reverse route to the source. After reaches the destination node- Sends Route reply packets to source node. Transmit the data from source node to destination node through energy efficient intermediate nodes, If any path failure occurs again starts route discovery. Route request send to all intermediate nodes between source S and destination Route discovery for shortest and freshest path using ADDRP.Check the Neighbor list. Detection of misbehavior nodes using Security Packet. Then send communication between sources to destination node.



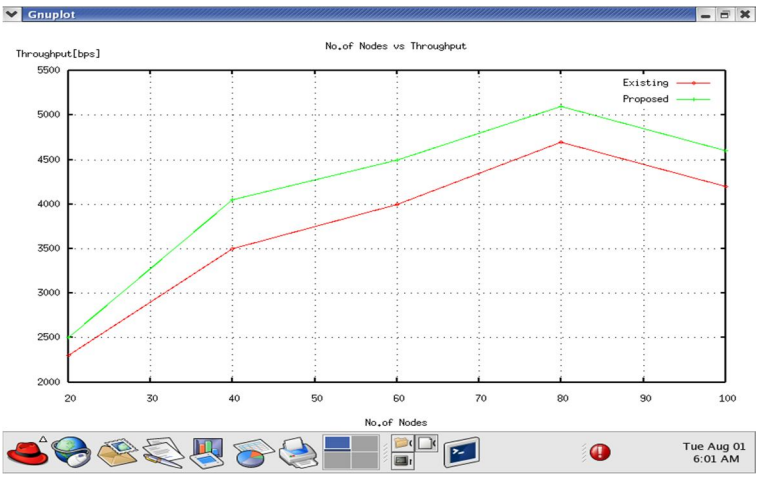
7) *Performance Analysis*: To have detailed energy-related information over a simulation, the ns-2 code was modified to obtain the amount of energy consumed over time. The system used these data to evaluate the protocols from the energetic point of view of Packet Delivery Ratio, Energy consumption, Delay and throughp

IV. EXPERIMENTAL RESULT

A. *Throughput*

Throughput is the number of useful bits per unit of time forwarded by the network from a certain source address to a certain destination, excluding protocol overhead, and excluding transmitted data packets.

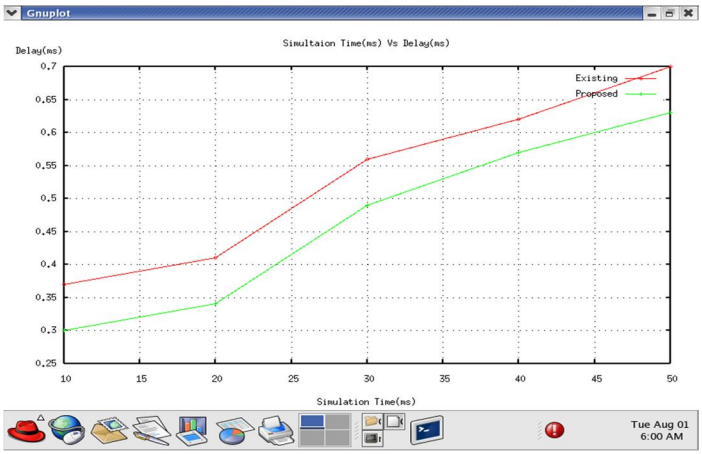
$$\text{Throughput} = \frac{\text{No of Packets Received}}{\text{Simulation time}}$$



B. Delay

It is defined as the average time taken by the packet to reach the server node from the client node.

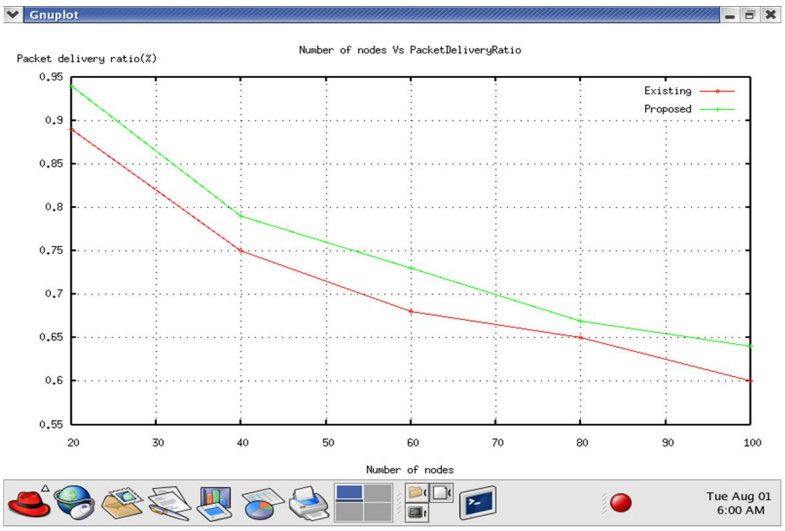
$$\text{Delay} = \frac{\text{No of Packets Sent}}{\text{Simulation time}}$$



C. Packet Delivery Ratio

Packet Delivery Ratio is defined as the average of the ratio of the number of data packets received by each receiver over the number of data packets sent by the source.

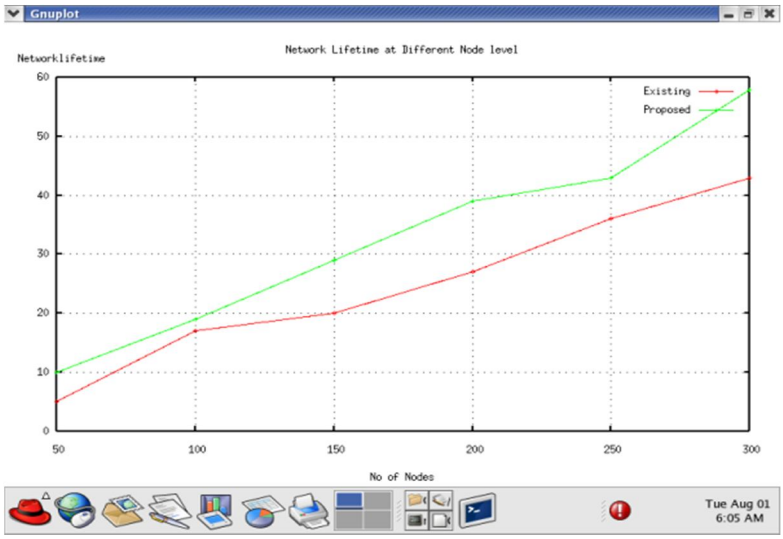
$$\text{Delivery ratio} = \frac{\text{No of Packets receved}}{\text{No of packets Sent}}$$



D. Transmission time

The **transmission time**, is the amount of time from the beginning until the end of a message transmission.

$$\text{Packet transmission time} = \frac{\text{Packet size}}{\text{Bit rate}}$$



E. Energy consumption

Energy consumption is nothing but overall energy consumed for transmission. CE denotes the consumed energy for all nodes. Final energy is taken after sending and receiving of each node. Final energy is also called remaining energy. The energy model represents the energy level of nodes in the network. The energy model defined in a node has an initial value that is the level of energy the node has at the beginning of the simulation. This energy is termed as initial Energy. In simulation, the variable "energy" represents the energy level in a node at any specified time. The value of initial Energy is passed as an input argument. A node loses a particular amount of energy for every packet transmitted and every packet received. As a result, the value of initial Energy in a node gets decreased. The energy consumption level of a node at any time of the simulation can be determined by finding the difference between the current energy value and initial Energy value. If an energy level of a node reaches zero, it cannot receive or transmit anymore packets.

$$CE = \left(\sum_{i}^{n} \text{Initial Energy} - \text{Final Energy}[i] \right)^{n}$$

Where,

CE - Consumed Energy
i - Initially i is 0
n - Number of nodes

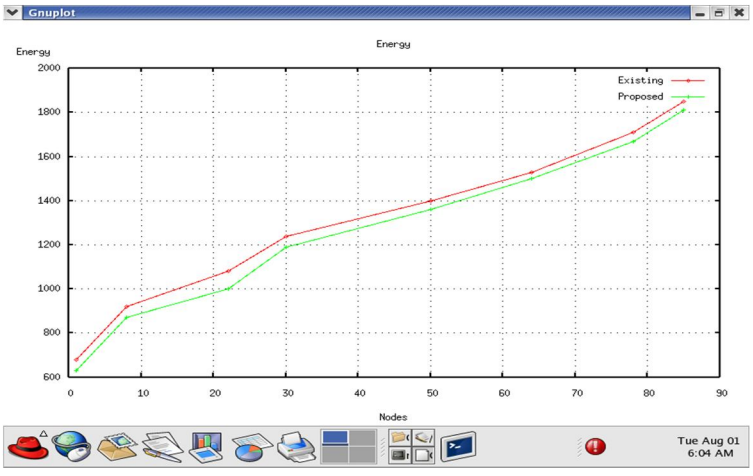
1) Total Energy

TE + = CE[i]

Total energy is calculated by overall Consumed Energy (CE)

2) Average Energy

AE = TE / n

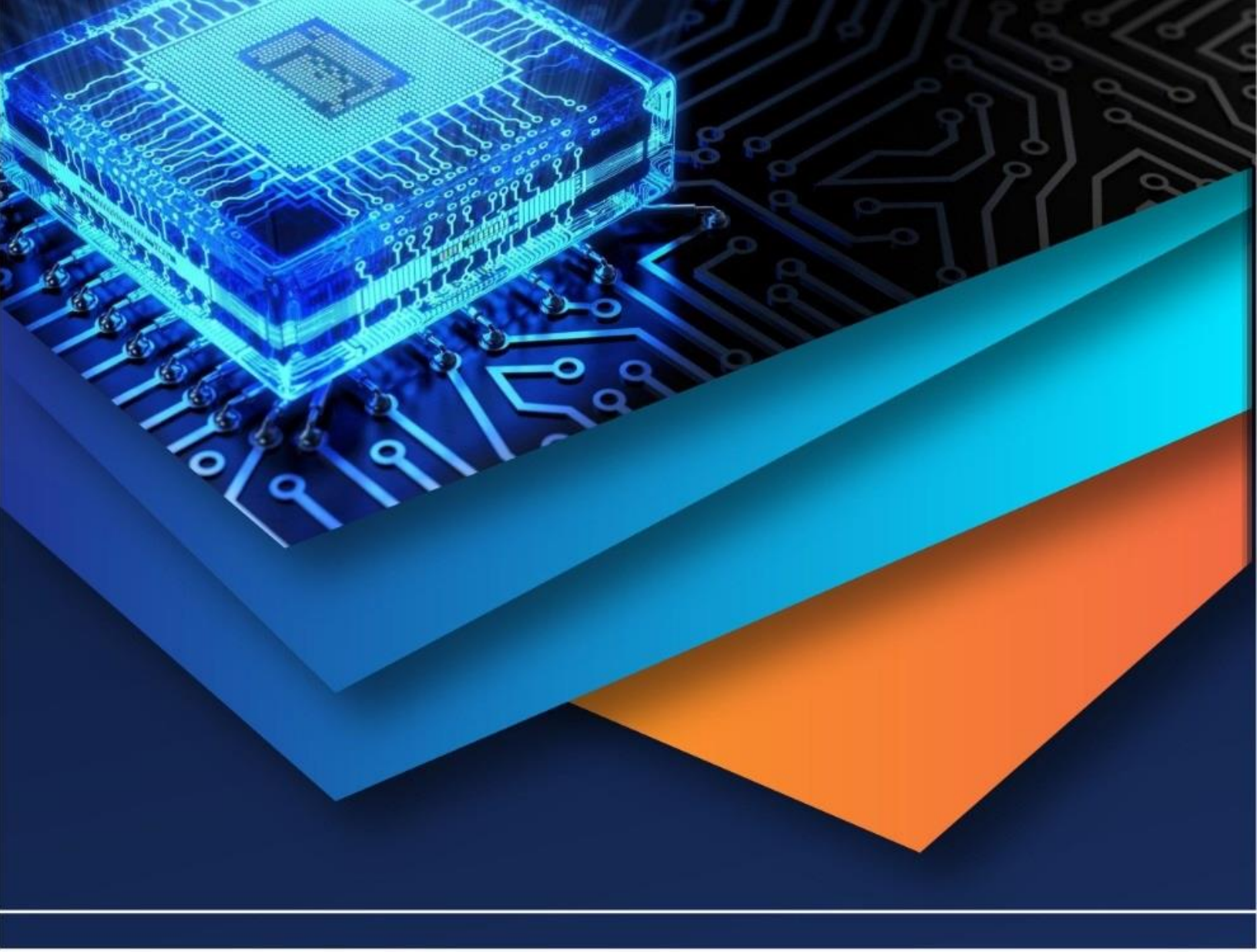


V. CONCLUSION

WSN is an important part of mode communication systems, and trust sensing routing protocol for WSN is an effective way to improve security, therefore, the study of trust sensing routing protocol is very important This paper presents a trust sensing based secure routing mechanism to handle common network attacks .An optimized routing algorithm is proposed by using semiring theory, which considers the trust degree and other QoS metrics. Simulation results show that TSSRM can reduce the routing over head and improve the reliability of data transmission compared with the traditional trust mechanism. Future research will design a distributed intrusion detection system for WSN, which may provide a new way for the research of trust degree and ubiquitous routing.

REFERENCES

[1] S. Corson and J. Masker, Mobile Ad Hoc Networking (MANET): Routing Protocol Performance Issues andEvaluation Considerations.RFCEditor, 1999.
[2] Q.A.ZengandD.P.Agrawal,HandbookofWirelessNetworksandMobile Computing. New York, NY, USA: Wiley, 2002.
[3] C. E. Perkins, ‘‘Ad hoc networking: An introduction,’’ in Proc. Ad Hoc Netw., 2001, pp. 20–22.
[4] S. Zheng, W. U. Weiqiang, and Q. Zhang, ‘‘Energy and link-state based routing protocol for MANET,’’ IEICE Trans. Inf. Syst., vol. 94, no. 5, pp. 1026–1034, 2011.
[5] M.K.MarinaandS.R.Das,‘‘Adhocon-demandmultipathdistancevector routing,’’ Wireless Commun. Mobile Comput., vol. 6, no. 7, pp. 969–988, 2006.
[6] M. Tekaya, N. Tabbane, and S. Tabbane, ‘‘Multipath routing mechanism with load balancing in ad hoc network,’’ in Proc. Int. Conf. Comput. Eng. Syst. (ICCES), Nov. 2010, pp. 67–72
[7] L. Gatani, G. L. Re, and S. Gaglio, ‘‘Notice of violation of IEEE pub- lication principles an adaptive routing protocol for ad hoc peer-to-peer networks,’’inProc.6thIEEEInt.Symp.WorldWirelessMobileMultimedia Netw., Jun. 2005, pp. 44–50.
[8] Y. Chaba, R. B. Patel, and R. Gargi, ‘‘Issues and challenges involved in multipath routing with DYMO protocol,’’ Int. J. Inf. Technol. Knowl. Manage., vol. 5, no. 1, pp. 21–25, Jan./Jun. 2012.
[9] S. Mueller, R. P. Tsang, and D. Ghosal, ‘‘Multipath routing in mobile ad hoc networks: Issues and challenges,’’ in Performance Tools and Applications to Networked Systems. Berlin, Germany: Springer, 2004, pp. 209–234.
[10] V. Balaji and V. Duraisamy, ‘‘Varying overhead ad hoc on demand vector routing in highly mobile ad hoc network,’’ J. Comput. Sci., vol. 7, no. 5, pp. 678–682, 2011.
[11] M. Poonam and D. Preeti, ‘‘Packet forwarding using AOMDV algorithm in WSN,’’ Int. J. Appl. Innov. Eng. Manage. (IJAIEM), vol. 3, no. 5, pp. 456–459, May 2014.
[12] G. Cervera, M. Barbeau, J. Garcia-Alfaro, and E. Kranakis, ‘‘A multi- path routing strategy to prevent flooding disruption attacks in link state routing protocols for MANETs,’’ J. Netw. Comput. Appl., vol. 36, no. 2, pp. 744–755, Mar. 2013.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY