TRUST SENSING BASED SECURE ROUTING FOR WIRELESS SENSOR NETWORKS

D.Meghana[1],K. Ramalinga Reddy[2]

1. Student, Branch of WMC, G.Narayanamma institute of technology and science, Hyderabad, India

2.Head of the Department, Dept. of ETM, G.Narayanamma institute of technology and science, Hyderabad, India.

ABSTRACT:A trust sensing based mostly secure routing mechanism (TSSRM) with the light-weight characteristics and also the ability to resist several common attacks at the same time is planned because of the intense result of the typical network attacks which are caused by the limited energy and the poor deployment environment of wireless sensor network (WSN) on data transmission. On the other hand, route selection algorithm of security is also optimized by taking the trust degree and QoS metrics into account. TSSRM can progress the security and effectiveness of Wireless sensor network. The behavior of the sensor nodes is by analyzed including the movement and energy consumption of sensor nodes. The trust sensing based secure routing mechanism for wireless sensor network is proposed to solve the network overhead and the security of multi-hop information transmission. When network entities do not have much awareness how to trust one other, they either naïvely believe in the good intentions of other entities. Without trust, a network entity has to delegate a task, such as sending data to a destination, to someone who may not be trustworthy. This could cause failures of important network functions like routing. The proposed routing algorithm is applied to secure routing mechanism to achieve the efficient and reliable transmission of data and to further ensure the security of data transmission.The Extension of the trust sensing based secure routing is that whenever the malicious nodes gets identified depending on the trust degree it sets a multipath routing by which the network overhead can be reduced and there will be an increase in the packet delivery ratio.

KEYWORDS:Malicious nodes, QOS requirements, reliable data transmission, wireless sensor network, multihop communication, network overhead.

1. INTRODUCTION

Internet of Things (IOT) supports cloud computing ,social network frequently and construction of smart city[1,2].The characteristics of Wireless sensor networks such as low cost, self-organization and rapid deployment plays an important role in simplifying the services of smart city. Smart cities that depend on different types of distributed intelligent devices can provide urban residents with a wide range of applications such as environmental monitoring, traffic management, and social entertainment. The wide ranging sensor nodes can both collect the physical information of urban environment and control the public and private facilities in the situation of smart urban environment .

There is a serious effect on data and information security as the multi-hop routing is unprotected to various types of attacks due to the open, distributed and dynamic characteristic of WSN[3-4].The existing secure routing algorithms at present are not suitable for the multi-hop distributed and energy-constrained WSN as usually they are directed against specific harmful or selfish behavior attacks, since they mainly depend on encryption algorithms and authentication mechanisms. Trust management (TM) is an helpful way to solve the security problems of WSN as defined [5-6], however, the common routing protocol based on trust is difficult to ensure the security of multi-hop information transmission, for which the reasons are given as follows. Primarily, new risks may also be prompted even though the method depending on trust can manage the natural attacks in WSN. On the other hand , the trust is

automatically different from other normal route indicators, such as the number of hops, delay or other QoS requirements, but the special property of trust degree in the design of routing protocols is not considered by credible nodes. Further more ,if the network routing protocol is changed the existing routing protocol depending on trust has certain limitations, such as dependence on specific route scheme, the security mechanism may be invalid.

To solve the network overhead and multi hop information transmission security the trust sensing based secure routing mechanism for WSN is proposed. Simulation results show that TSSRM not only improves the routing overhead in WSN effectively, but also security of information for multi-hop communication network. The main contributions of this paper is summarized as follows:

1) Behavior of sensor nodes, including the movement and energy consumption of sensor nodes is analyzed. Evaluation of the trust degree of the sensor node is done according to these characters, and then the trust degree of route is calculated and to get the optimal route from the source node to the destination node the trust calculation model of network is established. The routing metrics is an combination of the trust degree and QOS metrics to give an optimized routing algorithm by using the semiring theory.

2) The routing algorithms proposed are applied to the secure routing mechanism to attain the efficient and reliable transmission of data. At the same time, the maintenance process of TSSRM is also presented to further ensure the security of data transmission. Trust worthy system is introduced to provide the secured data delivery. Trust is the assuredness of honesty between two entities which are involved in the process of communication.

2. LITERATURE SURVEY

When network entities do not know how to trust each other, they either simply believe in good intentions of other entities or are unreasonable. The simple users can suffer badly from malicious attacks, whereas the unreasonable users can cause the network to suffer from low availability and efficiency. Without trust, a network entity has to replace a task, such as sending data to a destination, to someone that may not be trustworthy[7]. This would cause failures of important network functions, like routing**.**

The distributed networks such as MANETs and sensor networks gives the trust evaluation system that targets the protection of the system against malicious attacks. The arranging of trust in distributed networks is that for the bad mouthing attack the most effective defense is to organize the trust in the malicious node detection. The conflicting behavior attack use the recommendation trust in malicious node detection which reduces the detection rate[8].

The trust management system suffers from a Sybil attack if the malicious node generates several fake IDs. These fake IDs can be shared to the malicious nodes.

The trust management suffers from the new attack if a malicious node easily register as new user[9].As a new user registers the malicious node can remove away the bad history. The registering of a new or a fake ID becomes difficult as the defense against the sybil attack depends on the authentication and access control but not on the design of trust management.

The trust is defined as a dynamic event. The in-appropriate entity may become the appropriate entity because of the environmental changes, a good entity may be adjusted and turned into a malicious node. A mobile node may explore a bad channel situation at a certain location and the trust value may be low with forwarding the packets. When the channel situation is good some process should be taken to replace its trust value after it moves to a new location.

The radio links are commonly uncertain in sensor nodes as the wireless communication will take place. The confidentiality, integrity, authenticity, and availability of all the messages will be the major security parameter[10]. The data compression or the duplicate elimination is major aspect for the sensor networks for the effective and efficient energy in the data processing. Message authenticity, integrity, and confidentiality are commonly achieved by an end-to-end security mechanism.

The essential process of the wireless sensor networks is to feel the environment and transmit the acquired information to base station for the immediate processing. The network routing is

mainly focused on efficiency and effectiveness of the data propagation. Thus routing is an important process in the sensor networks. The security and routing of the node should be taken carefully to avoid any attacks.

The target tracking and monitoring of the environment are very critical in many of the sensor locations of the network applications. Many routing protocols such as the geographical routing protocol and location aided routing protocol make routing decisions on the on the information based on the node locations. The beacon nodes which are known for their main importance of knowing their own location through receivers are been used for the sensor networks. This protocol works in two stages as the first one being referred as the reference messages and the second stage as non beacon messages which depends on the receiving of the signal strength accordingly.

The various cryptographic operations such as encryption, authentication is necessary for achieving the security in wireless sensor networks[11].The exchanging of the information has to be done safely and secure by communicating with the nodes properly. Key management[12] schemes are mechanisms used to establish and distribute various kinds of cryptographic keys in the network, such as individual keys, pairwise keys, and group keys. The Key management is an important cryptographic method for the issues of security. A secure key management scheme is essential for the security of these primitives, and thus important to achieve secure infrastructure in sensor networks.

The radio links are commonly insecure as the sensor networks use wireless communications. Eavesdropping, injection, replay, and other attacks can be placed on the network[13]. The compromising on some normal nodes and deployment of the malicious nodes is considered on the side of the opponent attacks indeed. A typical expectation is to assume that base stations are well protected and trusted. Since a base station is the gateway for sensor nodes to communicate with the outside world, compromising the base station could provide the entire sensor network useless.

The development of the large scale wireless sensor networks in wireless communication have enabled the sensor networks that majorly consists of the low-power, low-cost small-size sensor networks. Sensor networks facilitates the large scale and real time data in complex environments. Security is critical for many sensor network applications, such as military target tracking and security monitoring[14]. To provide security and privacy to little detector node is difficult, due to the limited capabilities of sensor nodes in terms of computation, communication, memory/storage, and energy supply.

A large-scale sensor network consists of thousands of sensor nodes and will be spread over a good space. Typical sensor nodes are small with restricted communication and computing capabilities, and are powered by batteries. These small sensor nodes are affected to many kinds of attacks. For a large-scale sensor network, it is impractical to monitor and protect each individual sensor from physical or logical attack. Attacks on sensor networks can be classified into attacks on physical, link (medium access control), network, transportation, and application layers[15]. Attacks can also be classified based on the capability of the attacker, such as sensor level and laptop-level. A powerful laptop-level rival will so way more damage to a network than a malicious sensor node, since it has much better power supply, as well as larger computation and communication capabilities than a sensor node.

A primary region-based neighbor discovery protocol[16] is defined which relies on sending notification messages when nodes enter and exit regions to set up the communication links. The main challenge is figuring out when messages need to be sent to guarantee they reach their intended destination despite the continuous motion of the nodes. However , this basic neighbor discovery protocol doesn't guarantee communication links once nodes are moving quickly across region boundaries.

- The basic neighbor discovery protocol, is that at a high-level, the protocol relies on nodes sending notification messages tagged with their ids ,whenever nodes are about to change regions.
- When a node i is about to exit a region, it broadcasts a leave message some time before leaving. This leave message includes the region i will be moving into, or null if it

will not be in the next region sufficiently long to establish a link. Using the information received in the leave message, i's neighbors determine if they should begin tearing down the corresponding link with i

- When a node i enters a new region and determines that it is going to remain there for sufficiently long, it broadcasts a join message. The recipients of the join message may start setting up the corresponding link to i . The timing of these messages ensures that the proper definition of the corresponding links are maintained.

3. EXISTING SCHEME

Wireless sensor networks are composed of many sensor nodes. Some of the specific controlling tasks are done by these nodes. The transmission of the data to the control centers is done for the further analysis and also the controlling of the data in an area is obtained. The open environment of the WSNs makes the nodes to get easily exposed to a variety of attacks, such as eavesdropping, node compromising, and physical disruption. These attacks are likely to lead to unreliable data. Therefore, it is important to take measures to ensure data reliability and reduce energy consumption.

Trust models of WSNs should be as simple as possible, i.e. without constraints on software, hardware, memory usage, computing, processing speed, communication bandwidth, and detect the different attacks easily, and update trust relations accordingly[17]. The energy efficiency should be considered mainly. In trust models, trust and trustworthiness should be evaluated at the same time, since trustworthiness is a node's opinion of other nodes in the network.

Trust can be defined as the mathematical representation of trustworthiness. Trust is a derivation of the reputation of an entity[18].The direct trust and indirect trust are calculated separately. Direct trust is calculated based on First-Hand Information, while the indirect trust is calculated based on Second-Hand Information or recommendations from neighbor nodes[19]. Only calculating direct or indirect trust in not sufficient enough for trust evaluation. Trust models based on only one type of feedback are insufficient. The trust models based on previous positive feedbacks only can be cheated in a way that, colluded sensors send good reports for each other. Thus, positive and negative feedbacks should be taken into account at the same time. In WSNs, sensor nodes are always responsible for several tasks. Therefore, trust models should consider designing different trust computation methods for different tasks. Trust models are designed to improve network security.

3.1 Trust Model Evaluation:

The model is principally utilized in the perception layer of WSNs. The perception layer of Wireless sensor networks can be subdivided into the sensor node, relay node, and sink node. The different types of nodes have different behaviors and data. The sink node directly communicates with the gateway, so its security is relatively easy to guarantee. In the data transmission phase, the sensor nodes collect data and transmit it to the relay nodes (the cluster head). Relay nodes do information fusion and transfer information to the sink. The trust value of the sensor nodes is calculated in the cluster heads[20]. The trust value of the cluster head is calculated in the sink head. The trust calculation model of the whole multi-hop route is established by the trust model between two nodes including direct trust degree, indirect trust degree and incentive factor to decide the secure route of data transmission.

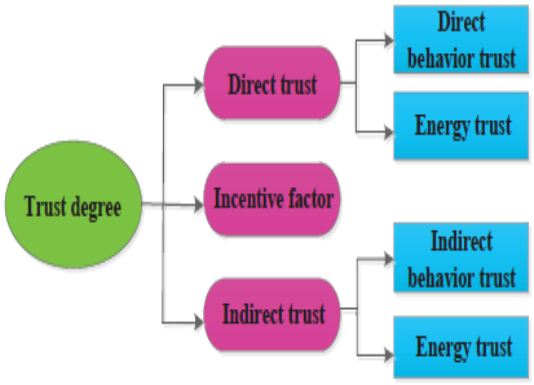

Fig 1: Trust model

3.1.1 Direct trust calculation of nodes:

The behavior of sensor nodes can be monitored by neighbor nodes in WSN. Since sensor nodes are highly constrained in computing power, energy, memory and bandwidth, it is not enough to judge the trust degree of nodes only by controlling the behavior of nodes.

3.1.1 a) Direct behavior trust:

Direct behavior trust is the direct observation of every node involved in communication

$dtd(x,y)l = \omega_1 \times dtd_{P(y)}(x,y)^{l-1} + \omega_2 \times dtd_{N(y)}(x,y)^{l-1} + ift(x,y)^l$ (1)

where $dtd_{P(y)}(x,y)^{l-1}$ denotes the direct trust degree of y for x according to the good behavior of node y in the past, $dtd_{N(y)}(x,y)^{l-1}$ denotes the direct trust degree of y for x according to the bad behavior of node y in the past. n stands for the number of neighbor nodes and l denotes the serial number of estimated records. ω_1, ω_2 denotes the decay factor of positive and negative evaluation, $ift(x,y)^l$ denotes the current behavior of the evaluation of the nodes.

3.1.1 b) Direct energy trust:

The nodes in the network will choose nodes with high trust degree as relay for forwarding information, which aggravates the energy consumption of nodes with high trust degree, thus resulting in uneven network load or even network segmentation. The energy consumption of node *y* during receiving and sending message is

$Receiving\_cost(k,d) = E_{elec} \times k$ (2)

$Sending\_cost(k,d) = E_{elec} \times k + E_{amp} \times k \times d^2$ (3)

The total energy consumption is

$EC = 2 \times E_{elec} \times k + E_{amp} \times k \times d^2$ (4)

where K:number of message bits , d: distance between node x &y, E_{elec}: unit energy consumption E_{amp}: energy consumption for achieving transmission

3.1.2 Indirect trust calculation of nodes:

Indirect trust is the trust relationship provided by other neighbors in the target node connected domain. Similar to the direct trust calculation model, the indirect trust degree is composed of the indirect behavior trust degree and the indirect energy trust degree. Since energy is an objective parameter, the indirect energy trust degree is the same as the direct energy trust degree. Only the indirect behavior trust degree of node is taken into consideration. If the direct connected domain of target node y in the network is C_y,

$$itd(x,y)^l = \sum_{z \in C_y, z \neq x} \left(dtd(x,z)^l \times dtd(z,y)^l \right) \quad (5)$$

The malicious nodes in the set of credible nodes can be detected, and false suggestions provided will be excluded from the network.

3.1.3 Incentive factor:

Incentive mechanism is established to punish the malicious node while restoring the nodes to cooperate by considering the limited energy of wireless sensor network and vulnerability of malicious nodes. Incentive is that the node will increase the number of participating in the network cooperation to improve the trust degree of node actively when the trust degree of node is reduced. Punishment is mainly defined in two aspects: (1) if the node does not participate in network cooperation, then the trust degree of node will be reduced. The node is considered as a failure node or a malicious node and will be removed out of the network when its trust degree is below a certain level. (2) If the node already has higher trust degree, the node is still very involved in the cooperation between the networks, and then the network will consider the node as a malicious node and remove it out of WSN directly. Therefore, in the case of that the number of node participating in the network cooperation is more, the incentive factor value has much positive impact on the trust degree, on the contrary, the trust degree of node which hasmuch more malicious behaviors must be reduced to encourageeffective cooperation between nodes.The maximum historical effectivetime τ is defined since the information interactionhas timeliness firstly, and then the incentive factor is alsodefined according to the interaction between nodes in τ. Incentive factor e_{xy} is given as

$$e_{xy} = 1 - \frac{F_{xy}^{\tau}}{F_{xy}^{\tau} + S_{xy}^{\tau}} \quad (6)$$

3.2 The TSSRM Scheme:

The network attacks area unit caused by the restricted energy and also the poor preparation surroundings of wireless sensor network (WSN) on information transmission, a trust sensing based

secure routing mechanism (TSSRM) is defined with the ability to resist the common attacks i.e grey hole attack, on-off attack The security route selection is also optimized by taking trust degree and QoS metrics into account. The trust sensing based secure routing is done in three stages: Network initialization process , Route construction, Route maintenance.

- Network initialization process: The network initialization is done by selecting a node with higher initial trust degree as the cluster head. The higher the node's trust degree is, the higher its energy is, and the longer the node lifetime is, which is more favorable for the stability of cluster structure. The possible geographical overlap between clusters in the process of distribution, is possible to select nodes with the highest TD_s in adjacent nodes as cluster head.

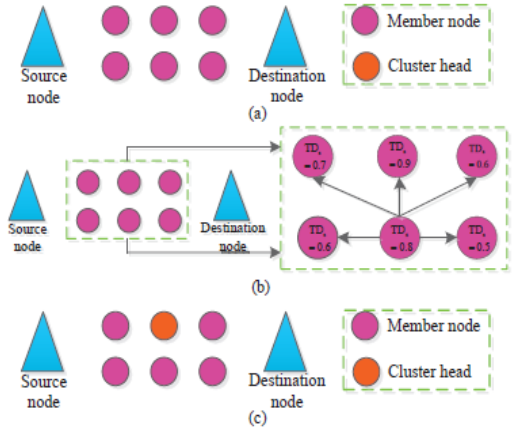

Fig 2: Process of cluster head

The trust calculation method based on the constrained resource of WSN, the trust degree $td(x,y)^l$ of target node y for node x is:

$$td(x,y)^l = \alpha \times s\_dtd(x,y)^l + \beta \times \frac{s\_itd(x,y)_l}{n-1} + \gamma \times e_{xy}$$

td: trust degree, s_dtd: direct trust degree,α,β,γ are weighted factors,s_itd: indirect trust degree, e_{xy}: incentive factor.

- Route construction: The establishment steps of TSSRM are as follows:
- Step1:Node n_0 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 n_{11}. The trust request packet is expressed as TR =⟨ei_{id}; ed_{id}; $td(r)_{th}$; ts; s; hl⟩. Node n_2 needs to check the freshness firstly after receiving the trust request packet, and the request will be removed if it is duplicate, otherwise, the request will be broadcasted to all the neighbor nodes of n_2.
- Step 2: The neighbor nodes (n_1, n_3 and n_6) of node n_2 will send the trust reply to node n_0 through the reverse route after receiving the trust request packet. The neighbor nodes that received the request will discard the request and no longer forward it if the value of hl in the trust request packet is reduced to zero.
- Step 3: After obtaining the parameters provided by the neighbor nodes of node n_2, node n_0 will evaluate the trust status of node n_2 by combining direct trust, indirect trust and incentive factor. Node n_0 determines whether node n_2 can be as a relay node according to the condition of trust route.
- Step 4:If there is an optimal route to node n_{11} in the credible node routing, any intermediate credible node that receives routing requests will send a reply to node n_0 so that the optimal route from n_0 to n_{11} can be obtained.
- Step 5: Node n_{11} will send a reply to node n_0 via the reverse route if it receives routing requests.
- Step 6: The source node n_0 will send a packet to the destination node n_{11} via the constructed optimal route. The direct trust derivation model mainly depends on its own detection system, which produces a little communication overhead. The indirect trust model is inseparable from the communication overhead since it involves the information interaction between recommended nodes. The TSSRM constructed only selects the suggestions provided by neighbor nodes of the evaluated node, which control the recommended range in the process of information transmission.

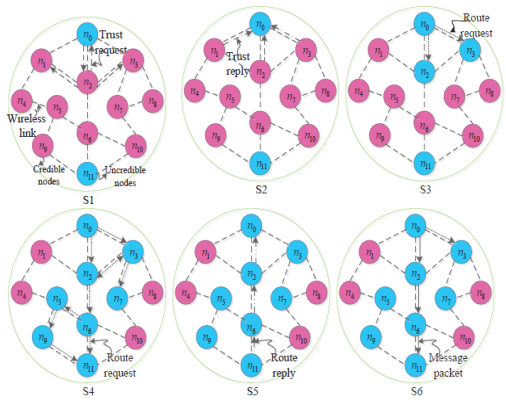

Fig 3 : Routing Process

- Route maintenance: Route maintenance is used to handle the credible route repair caused by node movement or failure in WSN and the credible route updates when new nodes are joined. Node n_2 will send routing update packets to source node n_0 via reverse route if it cannot find an alternative route to node n_6 or the trust degree of alternative route cannot meet the trust constraint conditions, and the optimal credible route will be reconstructed.

3.3 Evaluation of trust status:

The relay node is answerable for the trust analysis of device nodes, data forwarding. The sink node executes the trust analysis of the relay node, and it also includes data trust, behavior trust, and historical trust. The value of the trust is also obtained by the weighted calculation of data trust, behavior trust, and historical trust. The trust list is introduced in order to guarantee the reliability of the data involved in collection. Each sensor node needs to be verified within the access network, that the initial value of the trust list contains all the device nodes.

3.4 Proposed Work: In proposed work the energy consumption is maintained thereby the performance improves and the throughput also improves. The data is being sent through the multiple paths i.e the nodes are taking the alternate path for the transmission in the network. The throughput is increased as less number of packet drops takes place in the transmission. The trust status is taken into consideration for the process of optimal routing. If there exists any malicious node in the existing system it is not considered in the process of routing whereas in the proposed system the routing takes place by taking the alternate paths when there are any malicious node attacks.

4.EVALUATION RESULTS

The performance of the TSSRM mechanism is evaluated by using NS2 simulation. The variables which are evaluated in this routing mechanism are Packet Transfer Rate (PDR), Packet delay, Energy consumption, Throughput. From Fig 4: When compared to the existing, proposed TSSRM, extension the energy consumed is less in extension as it is taking multiple paths while in the process of routing. The major limitation of the wireless sensor networks is maintaining the energy consumption and limited battery power.

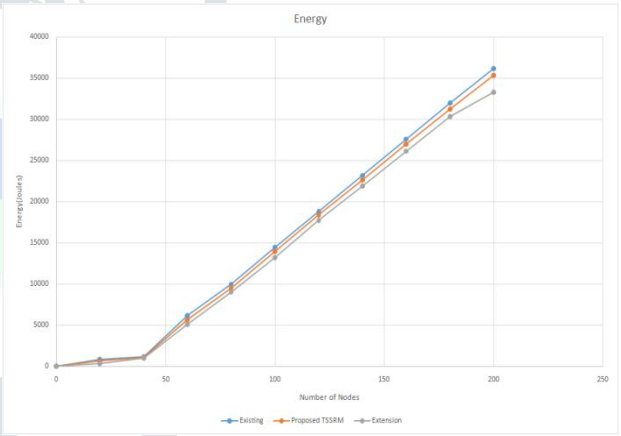

Fig 4: Energy Consumed

From Fig 5: When compared to the throughput of existing, proposed TSSRM, extension the throughput of the extension is better. Throughput is given in kbps(kilo bytes per second) as it is defined as the successful delivery of the data in the network.

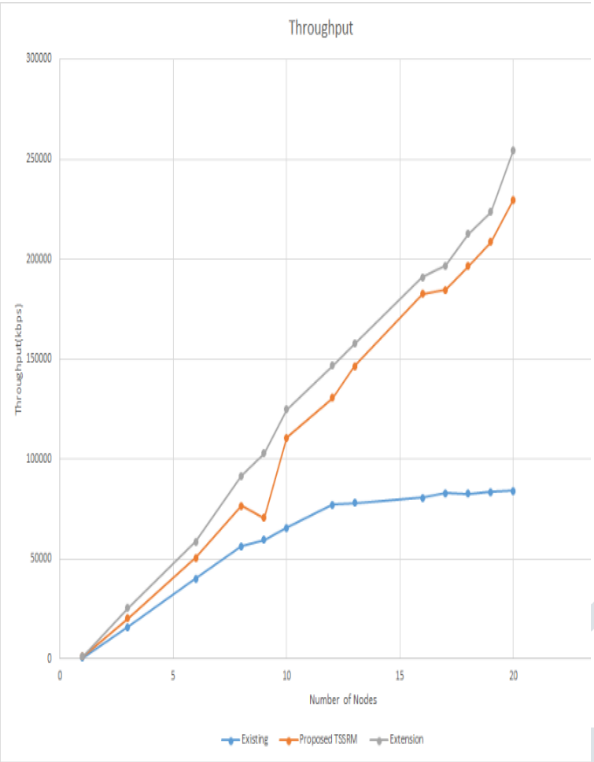

Fig 5: Throughput

From Fig 6: When compared to the packet delay of the existing, proposed TSSRM, extension, the packet delay of the extension is less as if any malicious node exists the routing takes place by the optimal path so that collision is avoided and hence the packet delay reduces thereby the effective transmission of the packet takes place. Thus, delay is less in extension as less number of hopes are involved in data transmission. The packet delay is reduced by taking the alternate paths in the process of routing and also the throughput is increased when compared with the existing system due to the malicious nodes.

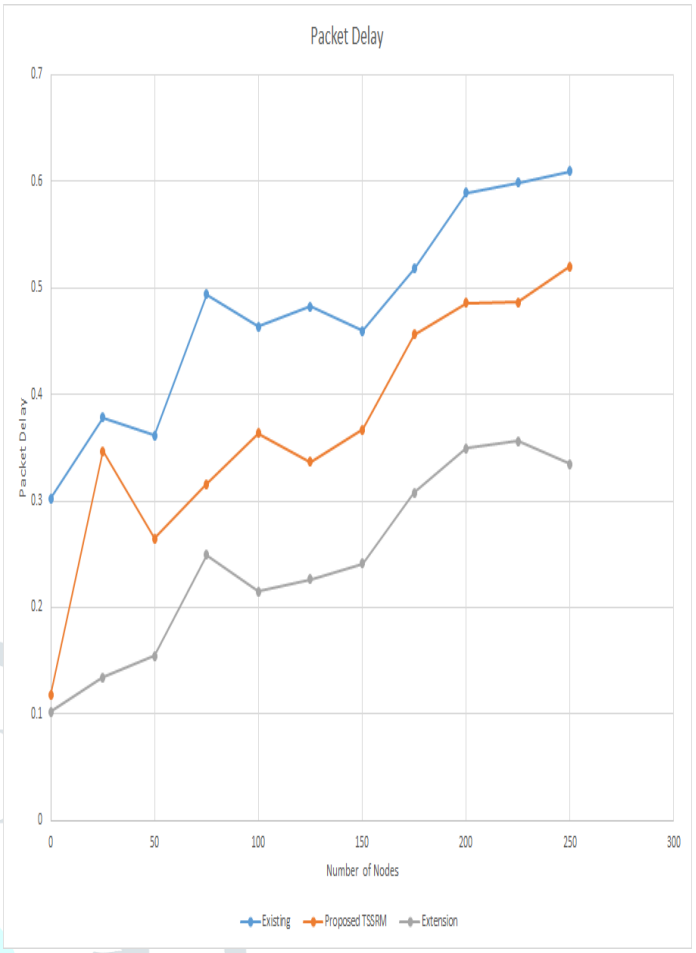

Fig 6: Packet Delay

From Fig 7: When compared to the packet delivery ratio of the existing, proposed TSSRM, extension, the packet delivery ratio of the extension is more. Packet delivery ratio is defined as the ratio of the number of packets sent by the source node and the number of packets received by the destination node. The packet delivery ratio of the extension has achieved high packet delivery ratio and less possibility of attacker selection.

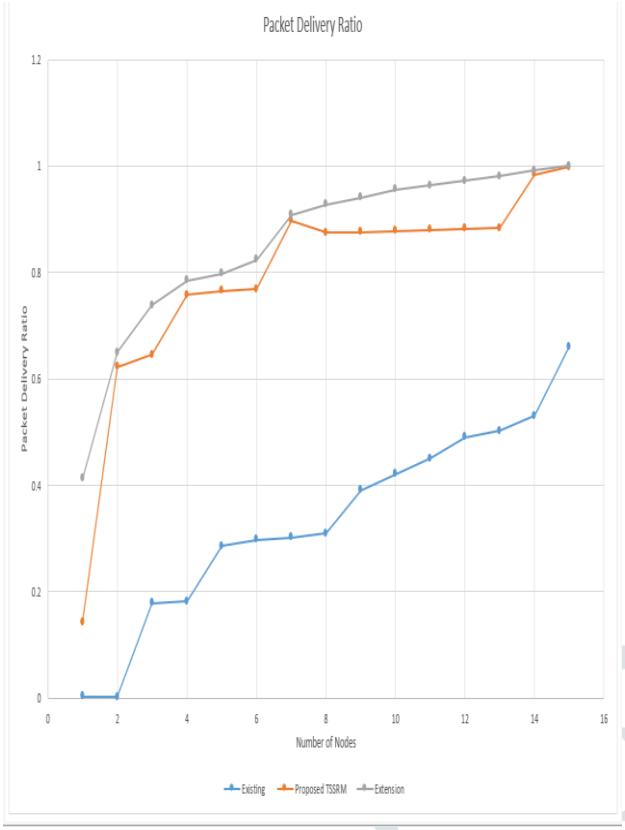

Fig 7: Packet Delivery Ratio

5. CONCLUSION

Trust management scheme consist a powerful tool for the detection of unexpected node behaviors (either faulty or malicious). Once misbehaving nodes area unit detected, their neighbors can use trust information to avoid cooperating with them either for data forwarding, data aggregation or any other cooperative function. In above trust management mechanisms, evaluation of node trust is based on the past behavior evidence or the recommendations from neighbor nodes. In order to improve accuracy of trust value, more trust metrics can be considered, such as, transmission range/radio range, packet loss, latency, path quality, hop count.

REFERENCES

[1] O. Ozel, K. Tutuncuoglu, J. Yang, S. Ulukus, and A. Yener, ”Transmission
with energy harvesting nodes in fading wireless channels: optimal
policies,” IEEE Journal on Selected Areas in Communications, vol. 29,
no. 8, pp. 1732-1743, Sep. 2011.

[2] N. Marlon, C. Jose, A. B. Campelo, O. Rafael, V. C. Juan, and J. S. Juan,
”Active low intrusion hybrid monitor for wireless sensor networks,”
Sensors, vol. 15, no. 3, pp. 23927-23952, 2015.

[3] G. Ottman, A. Bhatt, H. Hofmann, and G. Lesieutre, ”Adaptive piezoelectric
energy harvesting circuit for wireless, remote power supply,” IEEE
Transactions on Power Electronics, vol. 17, no. 5, pp. 669-676, Sep. 2002.

[4] A. K. A. Mohammad, and S. Gadadhar, ”Enhancing cooperation in
MANET using neighborhood compressive sensing model,” Egyptian
Informatics Journal, vol. 6, no. 1, pp. 1-15, 2016.

[5] G. Uttam G, and D. Raja, ”SDRP: secure and dynamic routing protocol
for mobile ad-hoc networks,” IET Networks, vol. 3, no. 2, pp. 235-243,
2014.

[6] W. K. K. Chin, and K. L. AYau, ”Trust and reputation scheme for
clustering in cognitive radio networks,” International Conference on
Frontiers of Communications, Networks and Applications (ICFCNA),
KualaLumpur, Malaysia, Nov. 2014, pp. 1-6.

[7] Y. Gao, H. W. Chris, J. J. Duan, and J. R. Chou, ”A novel energy aware
distributed clustering algorithm for heterogeneous wireless sensor
networks in the mobile environment,” Sensors, vol. 15, no. 10, pp. 31108-
31124, 2015.

[8] J. G. Choi, S. Bahk, ”Cell-throughput analysis of the proportional fair
scheduler in the single-cell environment,” IEEE Transactions on Vehicular
Technology, vol. 56, no. 2, pp. 766-778, 2007.

[9] K. B. Sourav, and M. K. Pabitra, ”SIR: a secure and intelligent routing
protocol for vehicular ad hoc network,” IET Networks, vol. 4, no. 6, pp.
185-194, 2015.

[10] E. Adel, K. Abdellatif, and E. Mohammed, ”A new trust model to
secure routing protocols against DoS attacks in MANETs,” The 10th International

Conference on Intelligent Systems: Theories and Applications
(SITA), Taiwan, Oct. 2015, pp. 1-6.
[11] J. M. Chang, T. Po-Chun, W. G. Isaac, C. C. Han, and C. F. Lai,
"Defending against collaborative attacks by malicious nodes in MANETs:
A cooperative bait detection approach," IEEE Systems Journal, vol. 9, no.
6, pp. 65-75, 2015.
[12] P. G. Fernando, M. C. A. Rossana, T. O. Carina, and J. N. Souza,
"EPMOSt: An energy-efficient passive monitoring system for wireless
sensor networks," Sensors, vol. 14, no. 3, pp. 10804-10828, 2015.
[13] X. Du, and H. Chen, "Security in Wireless Sensor Networks," IEEE
Wireless Communications, vol. 15, no. 4, pp. 60-66, 2008.
[14] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao, "A Survey
on Internet of Things: Architecture, Enabling Technologies, Security and
Privacy, and Applications," IEEE Internet of Things Journal, vol. PP, no.
99, pp. 1-18, 2017.
[15] Z. Liu, X. Yang, P. Zhao, and W. Yu, "On Energy-balanced Backpressure
Routing Mechanisms for Stochastic Energy Harvesting Wireless
Sensor Networks," International Journal of Distributed Sensor Networks
(IJDSN), vol. 12, no. 8, pp. 1-9, 2016.
[16] N. Hidehisa, K. Satoshi, J. Abbas, N. Yoshiaki, and K. Nei, "A dynamic
anomaly detection scheme for AODV-based mobile ad hoc networks,"
IEEE Transactions on Vehicular Technology, vol. 58, no. 13, pp. 2471-
2481, 2009.
[17] Y. X. Liu, M. X. Dong, O. Kaoru, and A. F. Liu, "ActiveTrust: Secure
and trustable routing in wireless sensor networks," IEEE Transactions on
Information Forensics and Security, vol. 11, no. 2, pp. 2013-2027, 2016.
[18] L. H. G. Ferraz, P. B. Velloso, and O. C. M. B. Duarte, "An accurate
and precise malicious node exclusion mechanism for ad hoc networks,"
Ad Hoc Networks, vol. 19, no. 6, pp. 142-155, 2014.
[19] S. Kurosawa, H. Nakayama, N. Kato, A. Jamalipour, and Y Nemoto,
"Detecting blackhole attack on AODV-based mobile ad hoc networks by
dynamic learning method," International Journal of Network Security,
vol. 5, no. 9, pp. 14-21, 2007.
[20] D. Zhu, X. Yang, W. Yu, and X. Fu, "Network Coding vs. Traditional
Routing in Adversarial Wireless Networks," International Journal of Ad
Hoc Network-Elsevier, vol. 20, no. 2, pp. 119-131, 2014.

BIBILIOGRAPHY

D.Meghana Pursuing M.Tech in the department of WMC,G.Narayanamma Institute Of Technology andSciences,under JNTUH,Hyderabad,Telangana,India.

K.RamaLingaReddy working as H.O.D in ETM Department ,G.Narayanamma Institute of Technology and Sciences, Hyderabad.He completed B.Tech from Osmania University,Hyderabad in the year 1989.M.Tech from SV University ,Tirupathi in the year 1991.Ph.D from JNTUH in the year 2011.He presented 50 papers in international conferences and journals, his area of interest is Wireless Communication Networks and Digital Image Processing.