EFFICIENT SECURE ROUTING ALGORITHM FOR WIRELESS SENSOR NETWORKS USING LIGHT WEIGHTED TRUST MANAGEMENT PROTOCOL

R. Mohan Kumar, A. V. Ramprasad and G. N. Priyadharshini
Department of ECE, KLN College of Engineering
E-Mail: psr_mohan2005@yahoo.co.in

ABSTRACT

In wireless sensor networks, secure routing and trusted transmission of data through the nodes is one of the most challenging applications. In this paper, we are implementing the concept of trust management by using QOS metric estimation and the concept of Light weight trust management protocol is also introduced. The trust degree is calculated among the nodes by the method of direct and indirect trust computation with the help of neighbor's recommendation and direct monitoring of packet forwarding process. The packets are transmitted only through the trusted nodes. The trust degree is calculated with the help of threshold value that is set to every nodes and the packet forwarding behavior. The nodes are said to be highly trusted node based on the trust degree value of the nodes. This method is implemented using Trust based QOS routing algorithm (TQR) .From this we can achieve the most efficient transmission among the network. Finally the performance is compared with AODV, Watchdog DSR and QAODV protocol. This will conclude that it can prevent attacks from the malicious nodes and increase the security level among the network Index Terms—Component, formatting, style, styling, insert.

Keywords: metric computation, trust degree, TQR scheme, QOS routing**.**

1. INTRODUCTION

Wireless sensor networks (WSN) is a network which consists of number of autonomous systems that are spatially distributed among the network. The Wireless Sensor Networks is composed of number of miniature components that are capable of computation, communication and Sensing. This forms a bridge between the real physical and the virtual world. It has many applications such as industry, science, transportation, civil infrastructure Seismic monitoring and Security. The components in a wireless node are sensors, memory, processor, GPS, Radio transceiver and Power Source. The challenges of Wireless Sensor Networks are energy efficiency, Robustness, responsiveness, Privacy and Security. The operation of Wireless sensor networks are structured versus Randomized Deployment, Connectivity and Coverage Metrics of Interest. The random Graphtheory is Useful for analyzing such deployments in wireless sensor Networks. Security is one of the most challenging issue in Wireless sensor Networks. So we have to improve the security among the nodes inorder to achieve efficient communication.

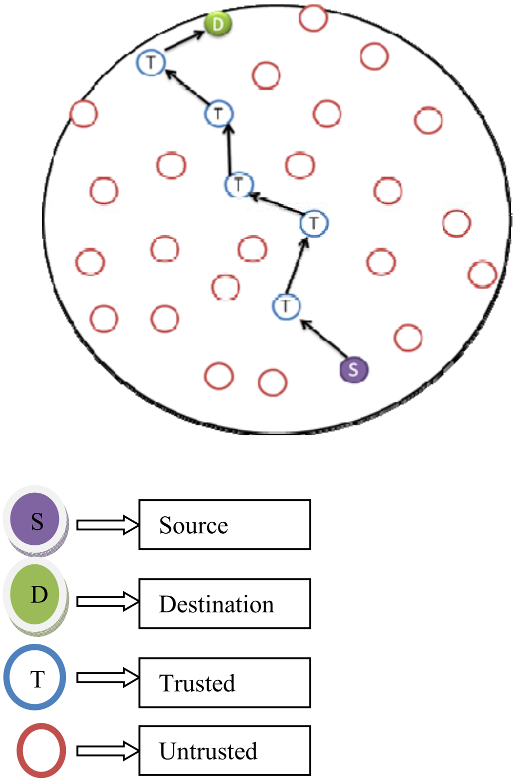

Figure-1. Schematic Representation of Packet Transmission.

In this paper, the security level of the nodes is increased by calculating the trust degree for each nodes. The trust degree is calculated for the nodes by the method of direct and indirect computation among the neighbor nodes. Then the packets are transmitted among the trustnodes. The Trusted nodes are identified based on the trust value of each nodes. The nodes that are having low trust value is assumed as the untrusted nodes. The trusted nodes are the nodes that are having high trust value. In this the TQR (Trust based QOS Routing) scheme is also introduced. The trust is calculated for the nodes based on the quality of service technique that is the packet forwarding behavior and the delivery ratio. The main contribution of this paper are given as follows: (1) A novel based model for the evaluation of trust and satisfying QOS requirement is proposed. (2) To integrate Quality of Service requirements and trust degree into a routing algorithm. Then the simulations performing the effectiveness of the above said routing scheme is provided. This can prevent the nodes from the attacker which degrades the efficiency of the network.

In Figure-1 the Transmission of packets are represented schematically. In this from the source node the packets are transmitted to the destination through the trusted nodes. The trusted nodes are calculated based on the energy model of the nodes. The nodes that satisfy the energy model condition are considered as trusted nodes. Remaining nodes are said to be malicious nodes and the packets will not be transmitted through it. By this way the secured transmission is achieved in the wireless sensor networks.

2. RELATED WORKS

In this section, we briefly revise the previous works that have done on trust establishment and QOS schemes for wireless sensor networks.

A. Trust model

Nowadays there are latest trends about the trust establishment for Wireless sensor networks. In [4] Moazam Bidaki, *et al*. proposed a scheme called Trust based and cryptographic Based Clustering. The author proposed a method to select stability, trustworthy and high energy cluster head's. This aims to detect and isolate the malicious and misbehavior nodes with low communication and processing overheads. The parameters that are considered in this paper are Mobility index and Stability. Though it has many secure clustering schemes presented for MANET but there is a lack of solution to operate in both hostile and secure atmosphere. In [9], Christhu Raj M R, et al proposed a work that investigates some trust techniques and present the effective methodologies to calculate the trust of a sensor node to eliminate the selfish or compromised nodes in the network. Selfish nodes are the one that will attack the nodes affect the parameters such as packet forwarding and the delivery ratio. It will degrade the performance of the network and the efficiency of the network will also get reduced. The author used the trust model such as Bayesian trust model, Game theory trust model, Entropy trust model, Fuzzy trust model. The parameters such as entropy, reputation and trust values. The limitation in this paper is that the quality of service parameters are not considered. In [8] Chris Karlof, et al proposed a work to analyze the secure routing in wireless sensor networks. The algorithm that is used in this work is Tiny OSbeaconing, Directed diffusion, Geographic routing. The secure nodes are analyzed with the help of the beacon signal then the packets are sent only through the secure nodes. The limitations in this paper is that the routing protocols for Wireless Sensor Networks are insecure. In this paper the author have proposed a goal to carryout secure routing in wireless sensor networks and alsothey have explained the attacks against peer-to-peer networks and adhoc networks. In [1] ShailaK, et al., proposed a scheme called an Anonymity Trust Management Scheme (ATMS) which is applied to clustered systems to enhance the security level in wireless sensor networks. The parameters that are considered in this paper are the trust values, Number of clusters, and anonymity factor. In this the cluster heads will communicate with other cluster heads and the node information will be transmitted. A method of creation of dynamic pool ID creation is proposed in this paper. The trust indicates thenode'sability to provide the required service. The nodes with higher trust values are considered as the secure or trust nodes and that are having low trust values are considered as the untrusted nodes. The method of anonymity is used here to hide the ID of the nodes that are compromised. Here the chance of node failure is minimized. The limitation in this paper is that it is not applicable for Dynamic Wireless sensor networks. In [7], Mohammad Sadeghi, *et al.* proposed a method to Extend the secure routing protocols to meet the security requirements and to carry out secured transmission. The algorithm that are used in this work is Directed diffusion, Tiny OS beaconing, Geographic routing and Rumor routing. The tiny OS beaconing is a method that builds a form of spanning tree as a base station that will broadcast a route update to their neighbors periodically. This will continue recursively in every node by marking its parental node as its first node that it will hear a routing update. In this they have also introduced the scheme of Geographic and energy aware routing (GEAR) and Greedy Perimeter Stateless Routing (GPSR) that will give information about the node position and neighbor selection information. Though it guarantees the secured transmission the malicious node disturbs the stability of the system. In [2], Ing-Ray Chen et al., proposed a work that determines and apply the best operational settings at runtime in response to dynamically changing network conditions. The algorithm used in this scheme is Dynamic Trust Management algorithm. The parameters that are considered in this paper are Trust value, Delivery ratio, Message delay, Message overhead. The trust value is calculated for every nodes and the nodes that are having highest trust value are considered as the secure nodes. The secure nodes are also considered based on the Delivery ratio of the nodes. The nodes are continuously monitored and their performance about packet delivery is calculated to identify the secure nodes. But this protocol design limits to quantify the protocol overhead. A. Shaikh, *et al.*

Designed a protocol for Wireless Sensor Networks that reduces the memory, energy consumption and communication overheads. The algorithm used in this work is the Group based Trust Management scheme. The author has considered the parameters such as Trust values, Communication overhead, Memory requirement, Energy consumption. But the GTMS protocol trust value is based on the past interactions and trust formation issue to maximize application is not addressed. Scalability is also a limiting factor in this paper. In [6] Miguel Garcia, et al., proposed a work to Estimate the energy consumption in secure group based architecture for wireless sensor networks. He algorithm used in this work is the Group Based Security algorithm. The parameters that are considered in this work are Network key, Node group key, Relationship of update among the group keys. Here the energy consumption method for all protocol operation is explained along with the method of key creation and their usage. The network that has presented have two types of security zones intergroup security and intragroup security. In this the intergroup security is given with a unique key and the Intra group security is given with a group key. But the deployment of the sensor node optimized to run this protocol is not developed. In [3], Arnab Banerjee, *et al.* have proposed a method of providing a new scheme based on trust and also a method of message confidentiality and integrity is explained. The protocol that is used in this concept is Efficient Secure routing Protocol. Power available for a node, coverage and reliability are the parameters that are considered in this work. But the mitigation of many routing attacks are not simulated. In [11],Junqi Zhang, *et al*. proposed a novel hierarchical trust management scheme that minimizes communication and storage overhead. The algorithm used in this paper is group based trust management scheme. In this the trust value is considered as one of the parameters. The nodes that are having high trust value is considered as the highly trusted node and the one which has low trust value is considered as the insecure nodes. The other parameter that is considered in this paper is the Group trust value. In this scheme a time window and a decay function is incorporated that will capture the changing nature of trust value in various trust calculations. In [5], I.A. Jannathulfirthous, *et al.* have proposed a method to secure the Wireless Sensor Networks against attackers misdirecting the multi-hop routing, TARF, a trust-aware routing framework is designed and implemented for dynamic WSNs. The Trust-aware routing framework algorithm is used by the author to implement the proposed work. The parameters such as Route evaluation time, Time slot size, Packet transmission time are used here. In this the spoofing attacks of wireless nodes are detected by the spatial correlation is received signal strength (RSS).But the problem of Improving the accuracy of determining the number of attackers using Support Vector Machines(SVM) method is not focused in this paper. In [12]X. Anita, *et al.* proposed a new two way acknowledgment-based trust framework with individual and group acknowledgment requirement for trust establishment in Wireless Sensor Networks. To implement this 2 way acknowledgement protocol is used in this paper. The parameters such as Threshold trust level, Simulation time, Packet Delivery Ratio, Control Overhead are considered here. The two way acknowledgement protocol calculates the direct trust among the nodes by a link layer acknowledgment and a two-hop acknowledgment using a downstream neighbor. Buta much wider spectrum of security threats involving collaborative attackers are existing. In [10], Yenumula B. Reddy proposed an agent-based approach that maintains the node's current status. To implement this a Agent based approach is used in this paper. The parameters that are considered in this paper are Number of Iterations, Node Ratings, Reputation of a node, Current Reputation. In this agent based approach the detection is possible through ratings of the node. The rating is calculated by the ratio of packet forwarded by packet received. In this the ratings are updated using the sporas formula or molina's formula or with both the combination. The agent based approach is similar to cluster based approach or watchdog approach. But in this paper the event-based trust calculation is not included. In [13] Mandeep Kaur Gulati and Krishan Kumar proposed a work in which the packets are transmitted by finding the best route by the Quality of Service (QOS) routing method. In this the protocol used is that the DSDV Protocol and Optimum Link State Routing (OLSR).In this the distance vector routing the shortest distance will be calculated and the packets will be transmitted through that shortest path. But this is not applicable for application such as multimedia audio and video and also there will be no guarantee for the delivery of packets.

In [14], Jian Wang, YanhengLiu, Yu Jiao proposed a work in which the packets are transmitted through the trusted nodes and if any misbehavior is sensed by the nodes it will alert the other nodes through an alarm signal. In this the DSDV Protocol is implemented. But this will not be able to detect the attacks such as cryptographic attacks. In [15] by Shinsuke Kajioka, *et.al.* The routing process is carried out between the nodes with respect to topology bandwidth and the source node determines the logical path. It is equipped with number of network interfaces. Though it has end to end delay and packet delivery ratio in this method the nodes will have more load which should be reduced for efficient transmission. In [16] Pedro B.et.al., proposed a method to carry out the transmission through secure nodes. In this the trust nodes are taken as the secure nodes. The trusted nodes are assigned by the recommendation of the neighbouring nodes. The protocol used is Recommendation Exchange Protocol (REP).Though in this method the packets are transmitted through secure nodes it has less security compared to others.

3. TRUST BASED QOS MODEL

In this paper, a trust based Qos model which gives application, Trust derivation and Computation in a multi-Quality of service constraints background. In this

QOS is an agreement to give guaranteed services which includes jitter, bandwidth, loss rate and delay to the users. The method of supporting multi QOS constraint make the QOS routing problem NP- complete[12].Some authors [ ] explained about the trade-off between the delay and bandwidth. In this the end-to-end bandwidth through a route from the source to destination is calculated mostly by the medium access protocols which is used for resource management and channel access. Meeting these constraints simultaneously leads to difficulty in computation. So to make it simple we are considering the link delay alone for supporting QOS routing audio and video transmission. In this we are going to find a feasible way to calculate the link delay by taking the parameters such as link quality, which incorporate a scheme called as trust aware technique to the route discovery procedure to develop the security of the network.

A. Network assumption

In the adhoc networks the applications and protocols are based on the collaboration of the nodes because of the lack of infrastructure. In some cases the collaboration will not be a essential one. In this the nodes should forward the packet to their correct destination by spending their own form energy without any benefit. If a node does not forward its packets to their destination it will be characterized as the selfish behavior and the nodes are characterized as the selfish nodes. This selfish behavior will leads to the drawbacks such as high energy consumption and low efficiency. The attacks are noted such as gray hole attack and black hole attack. In this the nodes are assumed as a bidirectional which means that the node A can be able to transmit the packets at the same time the node B will also be able to transmit and receive the packets.

B. Definition of trust

Trust is the fact that reveals that these nodes will not act as malicious nodes. In the adhoc networks the networks the nodes can be able to communicate with one another based on the mutual trust process. In this the trust concept will be time dependent and asymmetric. In this the trust is classified as the direct trust and indirect trust. The direct trust means that the process of monitoring the nodes directly without any recommendation by other nodes. The indirect trust will be based on the recommendation to the nodes by the other nodes by the recommendation of the neighbors. In this paper the trust is evaluated based on these two methods. In this the indirect trust by the recommendation of other nodes will speed up the convergence rather than the direct trust method.

C. Trust model

In this each node will derive a trust degree value for each neighbors based on the above said methods. This trust degree will be based on the level of trust by its neighbors. Let $T_{i,j}(t)$ denote the degree of trust of the node I by its neighbor j at a time duration of t. This trust value will vary from 0 to 1.The trust degree value 0 represents the distrust of the nodes. The trust degree value 1 represents the complete trust for the node.The definition of weighted average of two parts is given as $T_{i,j}(t)$.

$$T_{i,j}(t) = w_1T_{i,j}^d(t)+w_2T_{i,j}^r(t) \tag{1}$$

In this the $T_{i,j}(t)$ denotes the direct trust degree of node i in node j based on the node i's direct observation of node j's packets forwarding behavior at a time T. $T_{i,j}^r(t)$indicates the indirect trust degree that the neighbors of node I have in node j by the recommendation at a time t. These neighboring nodes of node j will also be the neighboring nodes of node i. By assuming that the node has n neighbors , then$T_{i,j}^r(t)$ can be calculated as

$$T_{i,j}^r(t)=\frac{1}{n}\sum_{k=1}^{n} \quad T_{k,j}^d(t) \tag{2}$$

$T_{i,j}^r(t)$ defines the average of the existing trust degrees of the neighbors at time t.

The indirect trust degree will be calculated based on the neighbors recommendation.This type of recommendation will increase the trust evaluation process for nodes that will not succeed in observing their neighbors because of their source constraints.

When a source node discovers a path to the destination node with the help of the packet forwarding behavior the trust degree of the path should be calculated. The trust degree of the path is the average trust value of each and every nodes. The path is selected based on the average trust value of the path that is the path that has highest average trust value. But this method will not be completely suitable because the path that has highest trust value may not have the shortest path than the other path. So that the path will also have a longest path. To overcome this the trust value for each and every nodes are calculated. Based on the trust value of the individual nodes the path for transmission of packets is considered. This is the process that is carried out in this paper. So the trust degree of theroute is based on the trust degree of all the nodes that are present in that particular route. Let the route be represented as r, which consists of l number of nodes that is represented by a sequence {1, 2,…….l} where node I represents the ithnode. Thus the trust degree of route r is given as R_r

$$R_r=T_{1,2}(t)T_{2,3}(t)\ldots.T_{l-2,l-1}(t)=T_{i,i+1}(t) \tag{3}$$

The trust models that have vulnerabilities can be exploited by the presence of malicious nodes. In this trust model as mentioned above the trust is established based on the direct and indirect computation. This type of trust model will be met with the attacks such as slanderer attack and collusion attacks. A slanderer attack is a process that sends false recommendations to affect the reputation of other nodes. In addition to this malicious nodes can work in collision to strengthen the effectiveness of the attack. These types of attack may cause severe damage to the entire network. So in future we will improve the model to overcome these types of attacks by using the maturity based model [30].

Table-1

Trust	Trust Degree Value	Meaning
1	(γ,1]	Trusted Node
2	(0.3,γ]	Less Trusted Node
3	0.3	Uncertain Node
4	(0,0.3)	Suspect Node

D. Trust Estimation

1. Computation of node trust

The trust degree values that is calculated by monitoring the behavior of the neighbor nodes will form the basic blocks upon the model is built. In this section the method of estimating the node trust is discussed. The node trust is calculated based on the packet forwarding behavior. That is the node should forward the number of packets that have to be transmitted. The correct packet forwarding depends also on the reliable packet forwarding. It is a method of transmitting the packets without any modification which is denoted as a reliable one. At time t,$T_{i,j}^{d}(t)$ is calculated with the forwarding ratio of node j, which is given as

$$T_{i,j}^{d}(t)= \frac{F_{i,j}(t)}{R_{i,j}(t)} \qquad (4)$$

Where $F_{i,j}(t)$ denotes the number of packets that are correctly forwarded by the node j at time t, $R_{i,j}$ signifies the number of packets that are successfully received by the node j at the time of t. All these nodes will operate in a promiscuous mode. When a node listen to its neighbor that it is forwarding a packet first it should check its forwarding behavior. After the node received that packet it increments $R_{i,j}(t)$ by one. And if the node finds that the neighbor nodes have forwarded the packet that has to forward it will increase the valueof $F_{i,j}(t)$ by one.

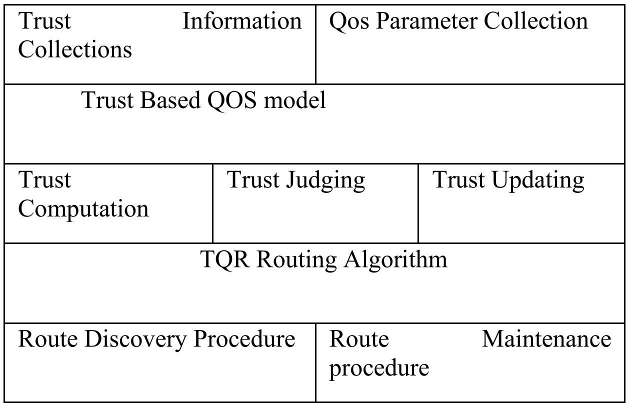

Figure-2. Framework of TQR Routing Algorithm.

After each and every interaction, the node i can be able to monitor its neighbor nodes forwarding behavior by the method of passive acknowledgement. A threshold γ to detect themalicious nodes. The different meanings of trust degree is given in Table-1.

2. Updating of node Trust

After each and every interaction that is carried out between the nodes the direct trust degree is updated by the methodof passive acknowledgement. After the trust update interval Δt,it will be written as

$$T'_{i,j}(t+\Delta t)=\mu * T_{i,j}(t) + (1-\mu) * T_{i,j}(t+\Delta t) \qquad (5)$$

Where $T'_{i,j}(t+\Delta t)$ denotes the updated trust degree at a time t+Δt and $T_{i,j}(t+\Delta t)$ is the trust degree of node j which is measured by the node i at a time t+Δt, $\mu(0<\mu<1)$ is the weighting factorthat is used to balance the current measurement and its previous estimation. In this every node will maintain a trust degree value record for every neighbor to which the particular packets are sent for forwarding purpose. In this trust record table the field will contain the node ID, nodetrust, direct trust degree, indirect trust degree, last updating time and the current time.

4. TQR: TRUST BASED QOS ROUTING ALGORITHM

A. Framework of TQR

To find the optimal solution and to decrease the distance of packet forwarding there are many algorithms that are carried out which includes Distributed Bellman-Ford algorithm [20] and Dijkstraalgorithm. But in this type of algorithm a source node will have to conduct wide communication with other nodes which is significantly extensive because of the use of control packet exchanges. So in this paper the distributed heuristic algorithm is used to design the Trust based QOS routing method. This Trust based QOS Routing consists of two parts they are Routing discovery and routing maintenance. The entire framework of TQR is shown in Figure-2.In this algorithm it involves the following components such as trust judging, trust updating and trust computation. The route discovery consists of two phases.

Table-2. Structure of a QOS Parameter Record Table.

Node ID	QOS(link delay)		Current Time	Last Computing Time	
	ETX	Transmission Delay	Propagation Delay		

The two phases of route discovery are the route request REQ delivery and the route reply REP delivery for the purpose of route establishing.

The TQR algorithm will be based on the following assumptions. (1) In this all the nodes will communicate through a shared wireless channel and all the channels will be bidirectional. (2) All the nodes will operate in the promiscuous node (3) We assume that the reliable link layer protocol to be in place.(4) We assume that all the nodes are identical in their physical characteristics.(5)The trust degree of each node will be obtained from the trust record table while the QOS Parameters can be obtained from the Table-3.

B. The procedure for route discovery

1. The Procedure for REQ Delivery

Step-1. If a source node S wants to send a data packet to the destination node D, the node S should check whether the route is available for further transmission of packets such as trust and QOS constraints. If the routes are available for the transmission then the procedure will be followed as given in step 3. If there is no such a route then the source node S initiates a route discovery procedure. The available path should be referred from the local routing table.

Step-2. The source node s verify with its neighbor nodes trust degree by trying with the trust threshold γ from the local trust record table.

Step-3. After the intermediate node j receives the REQ packet that is sent by the source node S,it will verify whether is has received the REQ Packet, if it is received it drops the REQ packet and the following procedure will end. Otherwise it collects the information such as $R_{s,j}(t)$, $F_{s,j}(t)$ and $\delta_j(t)$ form the local routing table .

Step-4. If the intermediate neighbor node k of node j has an available route to reach the destination D and the if the routing cost metric is least that is greater than γ then the node will generate a route reply packet REP to node S.

Step-5. Otherwise the node k performs the route discovery procedure which is same as the step3.Then the node k will continue to broadcast the REQ until it reaches the point of destination.

Step-6. When this particular destination node receives D receives REQ Packets it will decide to select the optimal route which has the least value of C(t).At that time the node D generates the route reply packet REP.

2. The procedure of REP Delivery

The procedure REP delivery will be reverse process of REQ delivery. With the same procedure if it has the available route to reach the destination D it will generate a REP packet and the packet will be sent back to the source node S along the available route for the establishment of the route. After the source node receives the REP Packet the source node sends data packets beside the trust and QOS constraints route.

3. Algorithm Design

Algorithm 1 Sending REQ()

```
//To the source node;
//whether there is the feasible path to the destination;
if(it exists) then
sendingdata( );
Else
    Broadcasts the REQ packet;
End if
//To the intermediate node or the destination node
        ReceivingREQ ( );
```

Algorithm 2 Receiving REQ() Sub procedure

```
//when a intermediate node receives a REQ packet;
  //checks whether it is the destination of the route
request;
If(is the destination)then
computes the least metric of C(t) from the existing
several REQ packets ;
  //After the node chooses the optimal route ,the
destination starts the REP delivery procedure;
  sendingREP( )
  Else
   if (not duplicate REQ) then
   checks the freshness of the REQ packet;
If(is a fresh packet) then
 get its value of T(t) and δ(t) from the record tables in
its
caches;
If ( T(t) ≥ γ ) then
 computes the $C'(t) \leftarrow \delta(t).(1-T(t))$;
 fetches the c(t) field from the REQ packet as
denoted by c′(t)
and updates the c(t) field by using C′′(t) as:
  $c''(t) \leftarrow c(t) + c'(t)$
  Rebroadcasts the updated REQ packet;
  Else
   Discards the REQ packet;
   waits for another REQ Packet
   End if
   Else
       Discards the REQ packet
   Endif
    Else
        Discards the REQ packet
     End if
     Endif
```

C. The procedure of route maintenance

Route maintenance is the mechanism in which the source node will be able to detect, while using an already established route to the destination node D, but if the network topology has changed such that it cannot be used for its longer use because the link along the route will no longer work. When the maintenance procedure indicates that the source route is broken, S can attempt to use another route based on its convenience if it is not found then it can find a new route. Route maintenance is used if only the node actually sends packet to the node Suppose if a link-broken event happens, the node with its broken link will broadcast RERpackets towards its upstream nodes for choosing the alternate route. The detailed explanation of route maintenance procedure is shown in Figure-3.

Algorithm 3 Sending REP

```
//Each node starts the route reply procedure
If(is the source node ) then
    // The REP delivery procedure finishes:
    Sendingdata( );
Else
    Looks up the local route table for next hop
    Continues to send the REP packet to the destination node by using the reverse optimal route of previous route discovery procedure;
End if
```

Algorithm 4 Receiving REP()

```
//When a intermediate node receives the first REP Packet;
//checks whether it is the source node of the route request;
If( is not the source node) then
    Forwards the REP packets to its next hop along the reverse optimal route;
Else
    Sendingdata( );
Endif
```

Algorithm 5 Maintain Route

```
//Each node monitors the link state of its neighbor nodes in a specified period by sending HELLO probe packets;
If (the current time  does not expire)then
    Updates its trust degree with its neighbor nodes by sending hello packets;
    The node notifies all the surrounding nodes about the link broken state by sending the RER packets about the abnormal nodes ;
Else
    Waits for a certain time interval(TTL) to check the link state of neighbors nodes;
End if
//To the other normal nodes
If(receives the REr packet)then
    Updates the routes to the destination node by passing the broken link and its neighbor table;
    If(is the source node)then
        Rebroadcasts the REQ packets to establish a new route by passing the broken link;
    Else
        Executes the local repairing procedureby choosing the alternative routes;
    Endif
Else
    Waits for the next RER packet;
Endif
```

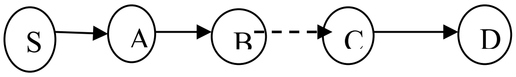

Figure-3. Route Maintenance Procedure.

D. Correctness analysis of TQR Algorithm

Theorem 1. The algorithm ensures that it is loop – free

Proof.
In this we assume that the network is having atleast one loop. Let {B,…..,c}be the loop which is shown in Figure 3.When the node D receives the REQ packet sent by its upstream neighbor node,it chooses the {S,A,B,….,C} as the shortest convenient route by comparing the routing cost metric.The route cost metric of {S,A,B,….C} will be C(t).IN this it is proved by contradiction method.We assume that node D chooses route {S,A,B,…..,C,B,….,C} as the optimal route.The route cost metric of route will be C′ (t).Due to this C′(t)=C(t)+w, where w is the route cost metric of loop{B,…….C},it is obvious that c′(t)>C(t). This leads to a contradiction with the assumption that the C′(t) is the optimal cost.Therefore the conclusion will be true.

E. Complexity analysis of TQR Algorithm

Theorem 2. The overhead complexity of the algorithm is $O(|M|^2d)$.M is the subset of all intermediate nodes in the network graph,such that their trust degree is greater than the trust threshold γ,d is the maximum node degree in the directed graph.

Table-3. Simulation Parameters.

Parameter	Meaning	Value
Area	Rectangular Field	1500X1500m
N	Number of nodes	100
S	Max Mobile speed	30m/s
R	Transmission Radius	300m
P	Data payload Size	500bytes/pac
w1	Weighting factor $T_{i,j}^{d}(t)$	0.8
w2	Weighting Factor $T_{i,j}^{r}(t)$	0.6
μ	Weighting factor of node trust	0.6
Δt	Time interval of Trust update	0.3s
T	Simulation Time	700s
M	Number Of Malicious Nodes	1-20
γ	Threshold of Trust DegreeValue	0.8

Table-4.

Scene Node	Malicious Node speed interval	Maximum	Trust update
1	10	0-40	0.03
2	0-20	20	0.03
3	7	12	0.03-0.1

These are the simulation parameters of Trust Based Qos Routing algorithm.

5. SIMULATION RESULTS

A. Varying Node Speeds

In this scene the performance comparison between TQR and AODV is calculated. As shown in Figure-4(b) the delivery ratios of TQR-0.5 and TQR-0.6 will decrease remarkably as the node maximum speed speedup when the delivery ratio of AODV decreases gently. As shown in Figure-4(a) the average end to end delay and routing packet overhead rise with increase of maximum speed. In this the detection ratio of TQR increases as increase in node speed. It is shown that when the nodes move faster the number of interaction between the nodes increases gradually. This leads to higher detection ratio of TQR-0.5 is little better than TQR-0.6.IT is shown that as the number of malicious node increases the nodes will met with heavy damage.

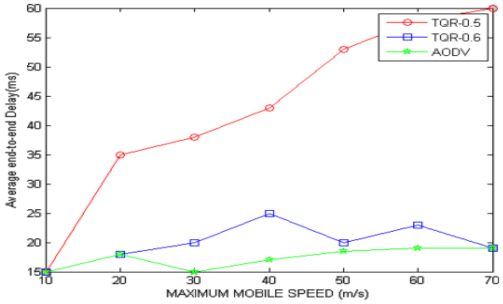

Figure-4(a)

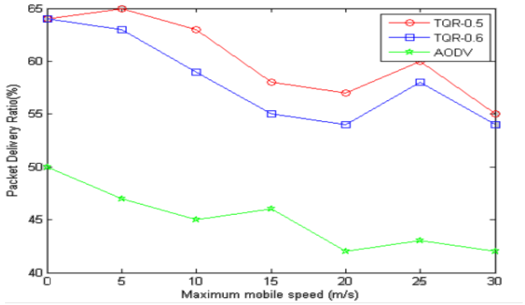

Figure-4(b)

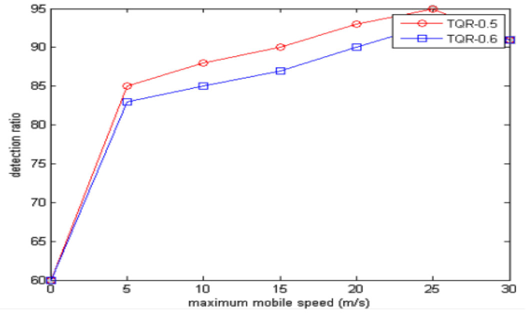

Figure-4(c)

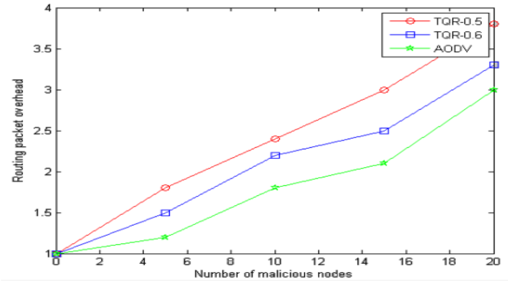

Figure-4(d)

In Figure-4(d) the routing packet overhead of all the protocol increases gradually by varying the number of malicious nodes.They decline gradually with increase in the number of nodes.

6. CONCLUSIONS

In this the trust based QOS routing algorithm is proposed which enhances the security level of the network in the presence of malicious nodes. This algorithm ensures that the forwarding of packets through the trusted node and least delay nodes by monitoring the behavior of the QOS constraints. Once a malicious node is detected it is isolated from the networks that no packet will be forwarded through it. This algorithm was proposed and implemented with NS2 based on AODV classic protocol. Its performance was evaluated through intensive simulations. A comparison is showed that TQR shows better performance in most of the simulation scenarios.

In our future work an extensive simulation will be conducted to verify the performance of TQR algorithm and compare it with existing protocols to evaluate the performance such as intrusion detection, secure routing and key management.

REFERENCES

[1] Shaila K., Sivasankari H., S H Manjula., Venugopal K. R. and L M Patnaik. Anonymity ant Trust Management Scheme. an ACEEE International Journal on Network Security. Vol. 03, No. 04, Oct 2012.

[2] Ing-Ray Chen. FenyeBao., MoonJeong Chang. and Jin-Hee Cho. Dynamic Trust Management for Delay Tolerant Networks and Its Application to Secure Routing. 6th IFIP WG 11.11 International Conference on Trust Management (IFIPTM 2012)

[3] Arnab Banerjee., Aniruddha Bhattacharyya, Dipayan Bose. Power and Trust based Secured routing approach in MANET an International Journal of Security, Privacy and Trust Management (IJSPTM), Vol. 1, No 3/4, August 2012.

[4] Moazam Bidaki. and Mohammad Masdari. Reputation-Based Clustering Algorithms in Mobile Ad Hoc Networks. an International Journal of Advanced Science and Technology Vol. 54, May, 2013.

[5] I. A. Jannathul Firthous. D. SuganthiAnandhavalli. Resource Management Based on Trust-Aware Routing And Detection of Multiple Spoofing Attackers in WSNS. an International Research Journal of Mobile and Wireless Communications – IRJMWC.

[6] Miguel Garcia., Jaime Lloret., Sandra Sendra. and Raquel Lacuesta. Secure Communications in Group-based Wireless Sensor Networks. International Journal of Communication Networks and Information Security (IJCNIS). Vol. 2, No. 1, April 2010.

[7] Mohammad Sadeghi., Farshad Khosravi., Kayvan Atefi., Mehdi Barati. Security Analysis of Routing Protocols in Wireless Sensor Networks. IJCSI International Journal of Computer Science Issues. Vol. 9, Issue 1, No 3, January 2012.

[8] Chris Karlofand David Wagner. Secure Routing in Wireless Sensor Networks:Attacks and Countermeasures.

[9] Christhu Raj M R., Edwin Prem Kumar G., Kartheek Kusampudi. A Survey on Detecting Selfish Nodes in Wireless Sensor Networks Using Different Trust Methodologies. International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958. Volume-2, Issue-3, February 2013.

[10] Yenumula B. Reddy. Trust-Based Approach in Wireless SensorNetworks Using an Agent to Each Cluster” International Journal of Security, Privacy and Trust Management (IJSPTM). Vol.1, No.1, February 2012

[11] Junqi Zhang., Rajan Shankaran., Mehmet A. Orgun., Vijay Varadharajan. and Abdul Sattar. A Trust Management Architecture for Hierarchical Wireless Sensor Networks.

[12] X. Anita., J. Martin LeoManickam. and M. A. Bhagyaveni. Two-Way Acknowledgment-Based Trust Framework for Wireless Sensor Networks” International Journal of Distributed Sensor Networks Volume 2013.

[13] Mandeep Kaur Gulati. and Krishan Kumar. Survey of Multipath QOS Routing Protocols for Mobile Ad hoc Networks. International Journal of Advances in Engineering & Technology. May 2012

[14] Jian Wang., Yanheng Liu., Yu Jiao. Building a trusted route in a mobile ad hoc network considering communication reliability and path length. Journal of Network and Computer Applications 34 (2011) 1138–1149

[15] Shinsuke Kajioka., Naoki Wakamiyaa., Hiroki Satohb., Kazuya Mondenb., Masato Hayashic., Susumu Matsuib., Masayuki Murataa. A QoS-aware

Routing Mechanism for Multi-Channel Multi-Interface Ad-Hoc Networks.

[16]Pedro B. Velloso., Rafael P. Laufer., Daniel de O. Cunha. Otto Carlos M. B. Duarte. and Guy Pujolle. Trust Management in Mobile Ad Hoc Networks Using a Scalable Maturity-Based Model" IEEE transactions on network and service management, vol. 7, no. 3, september 2010.