TAEER: Trust Aware Energy Efficient Routing Frame Work for Wireless Sensor Networks

Prabha R, Krishnaveni M, Manjula S. H, K. R. Venugopal, L. M. Patnaik

Abstract: Wireless Sensor Networks are basically employed for critical tasks whose operation is of prime importance.The sensor nodes are deployed in an environment where human intervention is not possible most of the times. The deployment of sensor nodes in habitat monitoring, health care, military fields demands that security to be in place because the data being handled is highly confidential. Wireless sensor networks are vulnerableto a wide set of attacks which threaten the network operation. The routing procedure employed inwireless sensor networks must becapable of preventing the data integrity loss that results out of the both active and passive attacks. In addition to the network being secure, trust establishment atvarious points at which the data is transmitted and energy awareness is essential tohave high network lifetime. Networks are highly constrained in resources such as memory, processing capabilities and energy. This resourceconstraint is a rigid obstacle against applying traditional security mechanism like cryptographic solutions which need too much processing power and thus leading to heavy energy consumption. The limited energy resources on sensor nodes makethem an attractive target for the attackers. Our proposed protocol caters to include trustworthiness and energy awareness by including a trust model thatincludesboth directand indirecttrusts.The proposed protocol safeguards a wireless sensor network from intruders by considering the trustworthiness of the forwarder node at every stage of multi-hop routing. Increasesnetwork lifetime by considering the energy level of the node, preventstheadversaryfrom tracing the route from source to destination by providing path variation. The protocolis built on NS2 Simulator. Experimental results show that the protocol provides energy balance through establishment of trustworthy paths from the sourceto thedestination.

Keywords: Energy Awareness,Routing, Security, Trust Model, Wireless Sensor Network.

I. INTRODUCTION

Wireless Sensor Network (WSN) is one type of ad hoc networks that consists of a very large number of tiny devices equipped with signal processing circuits, microcontrollers, sensors and actuators and wireless transmitters or receivers. Nodes are deployed either randomly or in a grid-like structure according to the sensing and environmental conditions and requirements[1].

Manuscript Received on January 2015.

Prabha R, Department of Computer Science and Engineering, University Visvesvaraya College of Engineering, Bangalore, India.

Krishnaveni M, Department of Computer Science and Engineering, University Visvesvaraya College of Engineering, Bangalore, India.

Dr. S. H. Manjula, Department of Computer Science and Engineering, University Visvesvaraya College of Engineering, Bangalore, India.

Dr. K. R. Venugopal, Department of Computer Science and Engineering, University Visvesvaraya College of Engineering, Bangalore, India.

Dr. L. M. Patnaik, Honorary Professor, Indian Institute of Science, Bangalore, India.

Networking and security technologies are in an advanced stage, wirelesssensor networks present complexities which dictate the design of new protocols. First, these networks operate in an infrastructure-less ad hoc manner, which implies that the communication relies on the cooperation amongnodes for the accomplishment of basic networkingtaskssuchasrouting. Each timeasensorneeds tosend the sensed value to the data sink, it looks for an available neighbor. As these are ad hoc networks designed to operate in a self-organized manner, a malicious node may enter the network. Due to the wireless operation, eavesdropping can be easily performed in this environment whichmakes the network vulnerable privacy attacks and traffic analysis attacks which threaten the whole network operation. Cryptography and authentication can help but do not suffice due to the constraints described above. To this end, security (although vital for most application cases) is seriously threatened in wireless sensor networks and the routing procedure is at the focus of adversaries due to its importance for the proper network operation and its vulnerability introduced by the required cooperation. The routing attacks as reported refuse to forward all or part of its neighbor's traffic issuing black-hole (or grey-hole) attack. A malicious node may also modify any packet it forwards (modification/ integrity attack), which affects the communication. More sophisticated attacks (like the replay attacks) try to deceive the routing protocol advertising wrong information. To combat malicious behaviors, an approach has been proposed in the literature: nodes monitor the behavior of their neighbors in order to establish trust relationships among each other and base their routing decisions not only on pure routing information, but also on their expectation (trust) that their neighbors will sincerely cooperate. In other words, a trust management system is implemented. To complete the routing protocol design, once the trustworthiness of each neighbor is evaluated, its exploitation to decide the routing path has to be defined. The selection of the most trusted neighbor, although straightforward, may result in the exhaustion of its energy, which contradicts the principle that energy consumption should be considered in all layer protocol design in order to realize the vision of "autonomous, long-lived" sensor networks. While routing protocols taking into account the remaining neighbors' energy levels have been proposed, its combination with the realization of a trust management system has attracted little attention. In the proposed routing protocol that features improved security, targets the extension of the network lifetime. This is achieved at the expense of calculating the sensing area of each neighbor.

To achieve higher security even when the sensor nodes aremovingand robustness in the trust calculation, the exchange of trust information is proposed which further increases the node energy consumption.

Motivation:Trust management system for wireless sensor networks is a mechanism that can be used to support the decision-making processes of the network [2].It aidsthe members of WSN (trustors) to deal with uncertainty about the future actions of other participants (trustees). The WSN is established without any existing infrastructure, which is a major feature exploited in most application. They rely on the mutual cooperation among nodes to route traffic towards sink or base station. Hence, trust establishment among the nodes is a must to evaluate the trustworthiness of other nodes and is one of the most critical issues in WSN. Survival of a WSN is dependent upon the cooperative and trusting nature of its nodes. Hence, the trust establishment between nodes is must. Trust is dependent on time; it can increase or decrease with time based on the available evidence through direct interactions with the same entity or recommendations from other trusted entities [3].

Contribution: The main contribution of this paper is design and implementation of Trust Aware Energy Efficient Routing (TAEER) Algorithm to achieve network level security. TAEER algorithm secures the WSNform any intruders trying to access information form the network. TAEER algorithm implements identity, route, location and data privacy to safeguard the WSN from an adversary misdirecting the multi-hop routing and security attacks.A new Identity, Route and Location privacy algorithm is proposed that ensures the source,identity,location and route privacy. The algorithm forwards thepackets to destination through trustedintermediate nodes.

II. ORGANIZATION

Section III deals with the RELATED WORK, Section IV gives the NETWORK MODEL, Section V deals withASSUMPTIONS, Section VI presents ADVERSARY MODEL. Section VII represents MATHEMATICAL MODELING. Section VIII presents RESULT ANALYSIS followed by Section IX CONCLUSION andREFERENCES.

III. RELATED WORK

Nitin*et al.,* [4] proposed a Trust Aware Routing Frame work (TRAF) solution**.**.TARF proves very effective against those harmful attack developed out of identity deception by providing the trustworthiness and energy efficient route in the communication of WSN. TARF achieved this by using two main components which are Trust-Manager and Energy-Watcher**.**Zhan *et al.*,[5]focused on TrustAware Routing Frame work, which significantly reduced the negative impacts from the attackers.It incorporates thetrustworthiness of nodes into routing decisions and allows a node to circumvent an adversary misdirecting considerable traffic witha forged identity attained through replaying. Guanghua*et al.,* [6] addressed a trust-based defending model againstmultiple attacks. The characteristics of resource-constrained sensor nodes, trust values ofneighboring nodes on the routing path is calculated through the Dirichlet distribution function, which is based on data packets acknowledgements in a certain period instead of energy-consuming monitoring. Trust is combined with the cost ofgeographic and energy aware routing for selecting the next hop of routing. Tayal*et al.*,[7] surveys the design and implementation of a trust aware routing protocol, which works efficiently and securely over wireless sensor networks. This frameworkhas been proposed to secure multi-hop routing in WSN against intruders exploiting the replay of routing information by an adversary to misdirect significant network traffic, resulting in disastrous consequences.Leena*et al.*,[8] designed a trust-aware routing framework for dynamic WSN, against those harmful attacks out of identity deception. Suneyna*et al.*,[9] proposed a mechanism for detecting suspicious transmission and consequent. Identification of malicious nodes for disseminating information in the network and a comparison will be done with existing approaches regarding packet loss, packetdelivery ratio, latency and throughput through simulation. Theodore *et al.,* [10] focusedontrust-aware,location-basedroutingprotocol which protects the WSN against routing attacks and supportsLarge-scale WSN deployments. The solutionhas been shown to be efficient in detection andavoiding malicious nodes and has been implemented in state-of-the-art sensor nodes for a real-life test-bed. Dikondwar*et al.,* [11] implemented the energy module for wireless sensor network which will calculate the transmission cost in terms of energy and accordingly find the route with least energy consumption after each transmission the energy module implemented on each sensor node will record the used energy value and send the energy recorded to the neighboring nodes. Manogna*et al.*,[12] developed a robust trust-aware routing framework for dynamic WSN. Without prolonged time synchronization or known geographic information. Offered dependable and energy-efficient route. The work demonstrates effective against those harmful attacks developedout of identity deception. Devanagavi*et al.*,[13] designed Agent based Secured Routing using Trusted neighbors (ASERT) in WSN. ASERT selects trustworthy neighbors and establishes secured routes using software agents.it operates in defining Safeguard Agency (SA) and Routing Agency (RA), both consisting of static and mobile agents and a knowledge base.Parimala*et al.,* [14]focused on the kind of attacks in which adversaries misdirect network traffic by identity deception through replaying routing information. Based on identity deception, the adversary is capable of launching harmful and hard-to-detect attacks against routing, such as selective forwarding, wormhole attacks, sinkholeattacks andSybil attacks.

IV. NETWORKMODEL

A typical wireless sensor network scenario is shown in Figure 1. Links are bidirectional. Sensor nodes use IEEE 802.11 standard link layer protocol, which keeps packets in its cache until the sender receives an acknowledgment (ACK).

Whenever a receiver (next hop) node successfully receives the packet it will send back an ACK packet to the sender. If the sender node does not receive an ACK packet during predefined threshold time, then the sender node will retransmit that packet.

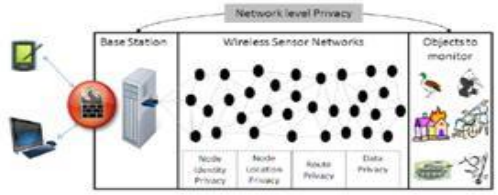

Figure 1: A Typical WSN Scenario

V. ASSUMPTIONS

For reasonof scalability, it is assumed that no sensor node needs to know the global network topology,except that it must know the geographical location of its own, its neighboring nodes and the base station. It is assumed that each sensor node in the network can share a unique secret key with the base station. These keys are periodically updated. The public key of the base station is also assumedknown to all the nodes in the network. Sensor nodes do not require their own public and private keys;because computation cost of public and private keys is generally high. It is also assumed that sensor nodes are capable of performing encryption and decryptionof the data by using any cipher algorithm such as DES, AES etc. This provides anadditional layerof security.

VI. ADVERSARY MODEL

Assumption:An adversary can perform passive attacks, since such attacks helps to conceal the adversary's presence in the network. The adversary is alsocapable of performing some active attacks like fabrication and packetdrop attacks. Other assumption is that the adversary is both device-rich and resource-rich.

Device-rich: The adversary is equipped with devices like antenna and spectrum analyzers, so thatthe adversary can measure the angle of arrival of the packet and received signal strength. Thesedevices will help the adversary to find out the immediate sender ofthepacketand move to thatnode. This kind of hop-by-hop trace back mechanism will be carried out by the adversary until theactual sender node is reached.

Resource-rich: The adversary has no resource constraint in computation power, memory or energy.It is assumed that the adversary has some basic domain knowledge like the range of identitiesassigned to the sensor nodes, the public key of the base station and information about the cipheralgorithms used inthe network. Adversary has no knowledge of whichidentity is physicallyassociated withwhich node. The trust management methodology that is adopted in this paper is useful to detect and prevent some non-privacy disclosure threats such as black hole attack, sink hole attack, and selective forwarding or gray hole attack.

Table 1: Types of Attacks

Black hole Attack	A malicious node denies performing routing anddrops part or the entire received packet.
Sink hole Attack	A malicious node tries to attract traffic advertising fakerouting information, and thenit refuses to forward it.
Modification Attack	An adversary modifies the data and/or routing packets andforwards it.
Replay Attack	The original routing messages are repeated at a later time,thus deceiving the routingfunctionality.
Traffic Analysis Attack	A malicious node monitors the traffic flows in order toidentify, locate and attack the critical nodes.

VII. MATHEMATICAL MODELING

TAEER protocol uses the concept of Direction and Trust and Energy Consumption as the metrics for forwarding packets in the network.Directionensuresreach ability of the packet, trust ensures reliability of the transmission, Energy consumption analysis ensures longevityof the network.

*Direction:*The physical location of the base station is the reference point for each sensor node. Based on this reference point, each nodeclassifies its neighboring nodes intofour categories:

(ii) Forward Neighbor Nodes Sets (*SF)*:A node *m* having a neighbor *n* is said to belong to Forward Neighboring Node Set (SF) if that node *n* lies in the area covered by $\frac{-\pi}{2}$ to $\frac{\pi}{2}$ with respect to the line joining the base station and the node*m*.

$$Cm, n=SF, \text{ if } \frac{-\pi}{2} \leq \theta \leq \frac{\pi}{2} \qquad (1)$$

(ii) Right Side Backward Neighboring Nodes Set (*SRb*) : A node *m* having a neighbor *n* is said to belong to Right Side Backward Neighboring Node Set (*SRb*) if that node *n* lies in the area covered by$\frac{\pi}{2}$*to*$\frac{5\pi}{6}$ with respect to the line joining the base station and the node*m*.

$$Cm,n=SRb, \text{ if } \frac{\pi}{2} \leq \theta \leq \frac{5\pi}{6} \qquad (2)$$

(iii) Left Side Backward Neighboring Nodes (*SLb)*:A node *m* having a neighbor *n* is said to belong to Left Side Backward Neighboring Node Set (*SLb*) if that node *n* lies in the area covered by $\frac{7\pi}{6}$ to $\frac{3\pi}{2}$ with respect to the line joining the base station and the node *m*.

$$Cm,n= SLb, \text{ if } \frac{7\pi}{6} \leq \theta \leq \frac{3\pi}{2} \qquad (3)$$

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

(iv)Middle Backward NeighboringNodes (*SMb):*A node *m* having a neighbor *n* is said to belong to Middle Side Backward Neighboring Node Set (*SMb*) if that node *n* lies in the area covered by$\frac{5\pi}{6}$ to $\frac{7\pi}{6}$ with respect to the line joining the base station and the node *m*.

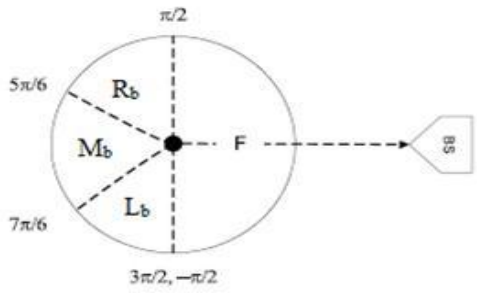

Figure 2: Negihbour Node Classification

Cm,n= *SMb*, if $\frac{5\pi}{6} \leq \theta \leq \frac{7\pi}{6}$ (4)

Theobjective of this categorization is to provide More path diversity.

Trust:Trustworthiness of a node is of prime importance as the data transmitted via these nodes is highly confidential at most of the times. Based onthis property of trust each node classifies its neighboring nodes into trustworthy nodes and untrustworthynodes.A trustworthynode is a one that interacts successfully most of the time with the othernodes. An untrustworthynode performs unsuccessful interactions with the neighboring nodes. An untrustworthy node could be a faulty or malicious node.A successful interaction involves the sender receiving a confirmation that the packet has reached the receiving neighbor. The first requirement of successful reception is achieved on the reception of the link layeracknowledgment (ACK). The second requirement of forwarding towards the destination is achievedwith the help of enhanced passive acknowledgment (PACK) by overhearing the transmission of a nexthop on the route, since they are within the radio range. If the sender node does not overhear theretransmission of the packet within a threshold time from its neighboring node or if the overheard packetis found to be illegally fabricated- (by comparing the payload that is attached to the packet), then thesender node will consider that interaction asunsuccessful.

Table 2: Notationsused in the Algorithm

N	Number of Nodes in the Network
T	Number of Trusted Nodes in the Network
M(t)	Set of Trusted Nodes in the Network
M(tF)	Forward Neighbor set of a Node
M(tRb)	Right Backward Neighbor set of a Node
M(tLb)	Left Backward Neighbor set of a Node
M(tMb)	Middle Backward Neighbor set of a Node
Nexthop(*k*)	Chosen Next Hop of a Node *k*
Contention(*x*)	Random Node Selection from the Set *x*
$Energy_{critical}$	Threshold Energy of a Node to participate in Communication
Energy(*k*)	Energy of a Node *k*
Energy(nexthop(*k*)	Energy of Selected Next Hop of Node k
$Energy_{transmission}$	Energy Required for One-hop Transmission
$Energy_{reception}$	Energy Required for One-hop Reception
Prevhop	Identity of Previous Hop
Nexthop	Identity of Next Hop
SeqID	Sequence Id of a Packet
Payload	Data in the Packet

Table 3: Neighbor Node Classification Algorithm for Static Network

Initialization Phase:
In a well- established static network
Step 1:for all N nodes in the network
Step 2: Broadcast HELLO packets
Step 3:endfor
Step 4: for every node receiving the HELLO packet
Step 5: if sending node is not included inrouting table of receivernode
Step 6: Update the neighbor set of the receiving node appropriately based on the trust value and direction property (include the node in any of the sets appropriately *(M(tF)* or M (tRb) or *M(tLb*) or *M (tMb))*
Step 7: else drop the packet
Step 8: endif
Step 9: endfor

Consider anode*i*, having *m* neighboring nodes in which *t* nodes are trusted. So, $0 \leq t \leq m$ and $M(t) = M(tF) \cup M(tRb) \cup M(tLb) \cup M(tMb)$. Here *M(tF),M(tRb), M(tLb), M(tMb)* represent the set of trusted nodes that are in the forward, right backward, left backward, and middle backward directions, respectively. These neighbor sets *(M(tF), M(tRb),M(tLb), M(tMb))* are initialized and updated whenever a change occurs in the neighborhood. In the routing phaseTAEER algorithm given in Table 5 is called. Source node firstchecksthe availabilityof the trusted neighboring nodes in its forward direction set *M(tF)*. If trusted nodes exist then it will randomly select one node as a next hop from the set *M(tF)* and check if the sending and receiving nodes have sufficient energy for transmission and reception respectively. Then the packet is forwardedtowards it. If there is no trustednode in its forward directionthen the source nodewill check the availability of a trusted node in the

Table 4: Neighbor Node Classification Algorithm for a dynamic Network

Step 1: If a new node enters the network or a node changes its trust value
Step 2: Broadcast HELLO packets from this node (new node or the one that has changed the trust value)
Step 3: end if
Step 4: for every node receiving the HELLO packet
Step 5: if sending node is not included in routing table of receiver node

Step 6: Update the neighbor set of the receiving node appropriately based on the trust value and direction property (include the sender node in any of the sets appropriately*(M(tF)* or *M(tRb)* or *M(tLb)* or *M(tMb)* of receiver node)
Step 7: else drop the packet
Step 8: end if
Step 9: end for

in its forward directionthen the source nodewill check the availability of a trusted node in theright *(M(tRb))* and left *(M(tLb))* backward sets. If the trusted nodes are available with satisfying energy constraints, then the source node will randomly select one node as a next hop from these sets and forward the packet towards it. If such a node does not exist in these sets either, then the source node will randomly select one trusted node from the backward middle set *(M(tBm))* and forwards the packet towards it withenergy criterion taken into consideration. In allthese cases if a random node selected does not meet the energy constraints, the chosen set is iterated until it exhausts. If thereare no trusted nodes available in all of the sets then the packet will be dropped.

Table 5: Trust Aware Energy Efficient Routing Algorithm (TAEER).

INPUT: **Neighbor node sets**
OUTPUT: Trustworthy node
Routing at Source Node/Intermediate Node.

Step 1: prevhop← null; nexthop←null;
Step 2: if *M(tF)* is not null then
Step 3: nexthop(*k*) = Contention*(M(tF)*);
Step4:ifEnergycritical<(Energy(*k*)Energytransmission) andEnergycritical< (Energy(nexthop(*k*)) – Energyreception) then
Step 5: Selected next hop is used to transmit the packet to the destination
Energy (*k*) = Energy (*k*) – *Energytransmission*
Energy (nexthop (*k*)) = Energy (nexthop (*k*)) – Energyreception)
Step 6: elsego to step 2 with *M (tF) = M (tF)* – nexthop(*k*)
Step 8: end if
Step 9: else if*M (tRb)∪M(tLb)*is notnullthen
Step 10: nexthop(*k*) =Contention(*M(tRb)∪M(tLb));*
Step11: if Energy critical<(Energy(*k*)-Energytransmission) and Energycritical< (Energy(nexthop(*k*)) – Energyreception) then
Step 12: Selected next hop is used to transmit the packet to the destination
Energy (*k*) = Energy (*k*) – Energytransmission
Energy (nexthop (*k*)) = Energy (nexthop(*k*)) – Energyreception)
Step 13: else
Step 14: goto step 11 with *M(tRb) ∪ M(tLb) = (M(tRb) ∪M(tLb))* – nexthop(*k*)
Step 15: end if
Step 16: else if *M (tMb)*is not nullthen
Step 17: nexthop(*k*) = Contention(*M(tMb));*
Step 18: ifEnergycritical< (Energy (*k*) – Energytransmission) andEnergycritical< (Energy (nexthop (*k*)) – Energyreception) then
Step 19: Selected next hop is used to transmit the packet to the destination
Energy (*k*) = Energy (*k*) – Energy transmission
Energy(next hop(*k*)) = Energy(next hop(*k*)) – Energy reception)
Step 20: else
Step 21: go to step 17 with *M(tMb) = M(tMb)* – next hop(*k*)
Step 22: end if
Step 23: else
Step 24: Drop packet and Exit;
Step 25: end if
Step 26: end if
Step 27: Set prevhop= myid;
Step 28: Form packet *p* = {prevhop; nexthop; seqID; payload};
Step 29: Create Signature and save in buffer;
Step30: Forward packet to nexthop;
Step 31: Set timer Δt= Ddnexthop× pt;
Step 32: while *Δt*= true do
Step 33: Signature remains in buffer;
Step 34: end while
Step 35: Signature removed from buffer;

VIII. RESULT ANALYSIS

A. Simulation Setup:NS2 (Network Simulator 2) is used for simulating the TAEER algorithm.. The simulation set up is in accordance with the Table 6 and Table7. The parameters considered for analysis are Energy Consumption, Packet delivery Ratio (PDR), Delay, Jitter, Network Lifetime.

Table 6: Deployment Parameters

Value	Parameters
Network Architecture	Homogenous, Flat
Area Size	500m X 500m
Number of Nodes	20, 40, 50,100
Deployment Type	Random
Transmission Range	250m
Initial Energy	1000 mJ

Table 7: Network Parameters

Value	Parameters
Channel Type	Channel/WirelessChannel
Radio Propagation Model	Propagation/TwoRayGround
Network Interface Type	Phy/WirelessPhy
MAC Layer	Mac/802_11
Interface Queue Type	Queue/DropTail/PriQueue

Link Layer Type	LL
Antenna Model	Antenna/OmniAntenna
Least Utilization Time	0.1 seconds
Maximum Utilization Time	10 seconds
Application Type	Event-Driven
Data Packet size	1000 Bytes
Acknowledgement Packet size	40 Bytes
Transmission Energy per Packet	0.026 Joules
Reception Energy per Packet	0.021 Joules
Idle Energy per second	0.001 Joules

B. Performance Analysis: The QoS performance metrics considered for analysis of TAEER algorithm are average energy consumed, jitter,delay,packet delivery ratio and network lifetime.

(i) Average Energy Consumed: The energy consumption for the transmission of a packet from source to destination is basically dependent on the number ofthe intermediate hops taken in that route. Figure 3 shows the energy consumption.

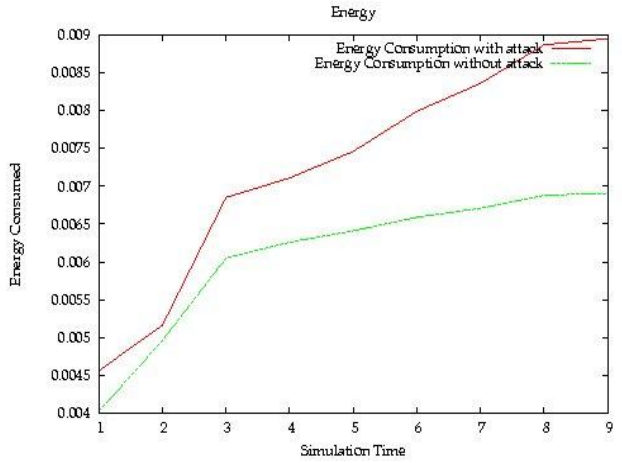

Figure 3: Simulation Time versus Energy Consumed

As the number of hops increase in that route, proportionally energy consumption increases. When there is normal transmission (attack- free), the total energy consumed is equal to the sum of the energy consumed for single hop transmissions for the intermediate hops. When there is attack-prone transmission there is retransmissioninvolved because of lack of acknowledgement in time. Retransmissions add up energy consumption, thus it can be seen from the graph that with attack the consumption is more as compared to its counterpart- without attack.From theapproach that we have used, the communication is not attack prone since all the nodes involved in the communication are trust worthy hence energy consumption is less comparatively.

(ii). Jitter:Jitter is the extraneous noise in the network produced mainly due to a number of packets using the same channel for their transit. In the normalflow, the number of packets in transit that is taking up a channel is low as compared to the abnormal flow (attack prone transmission).

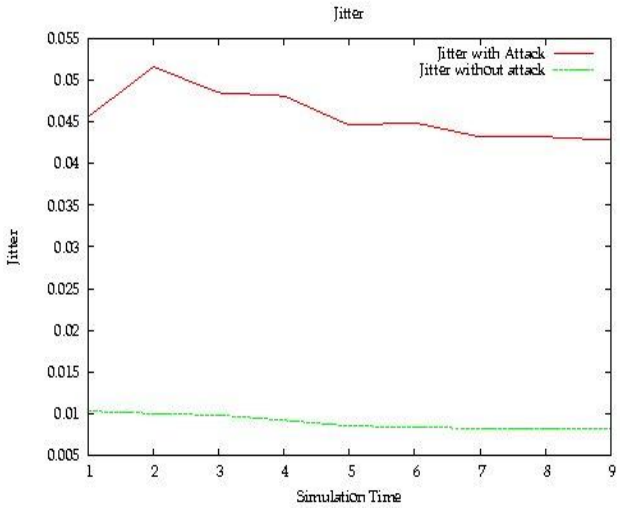

Figure 4: Simulation Time versus Jitter

In case of malicious nodes capable of inducing various types of attacks there will be packet drop because ofwhich there will be retransmissions of the dropped packets. This creates more and more traffic toflow through a single channel which creates jitter to be high.

(iii) Packet Delivery Ratio: Packet Delivery Ratio(PDR) refers to number of packets reaching the destination to the number of packets seeded at the source. The ratio will always be less than 1(unity) as there will be packet drop due to congestion or due to attacks.The algorithm that we have proposed proves to give a better PDR since there are no attacks involved. All the packets sent from the source reach the destination without any hindrance making the PDR very near to unity as illustrated from figure 5.

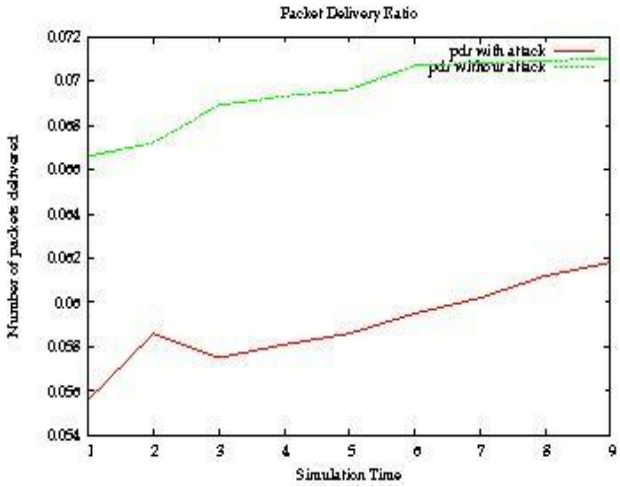

Figure 5: Simulation Time versus Packet Delivery Ratio

(iv) Delay:The End- to-End Delay is the transit time difference for the packet to reach the destination from the source. This delay depends on the number of intermediate nodes that are taken up in the chosen route. Thus if shortest path is chosen, the delay will be minimized. In case of attack, the retransmissions involved give rise to more number of one- hop transmissions repeatedly. Thus the overall end to end delay is increased as compared to its counterpart (transmissions notinvolving attacks).

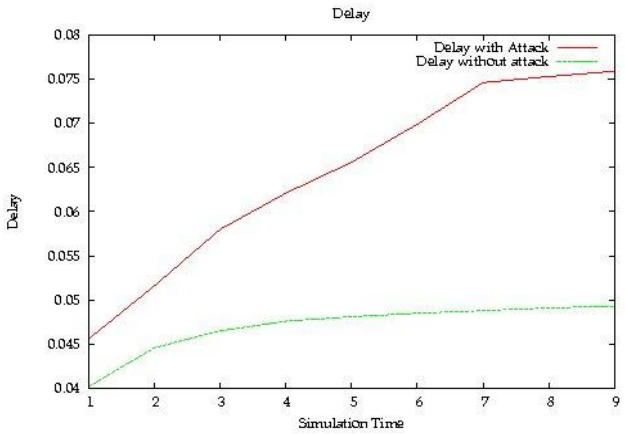

Figure 6: Simulation Time versus Delay

(v) NetworkLifetime:The lifetime of the node is influenced mainly by the energy the node possesses. In the proposed algorithm, a node can participate in a communication only if it has energy more than $E_{critical}$(Threshold Energy) that is after participating in the communication the node must not be in a position of being dearthin energy. Thus check of including a node in the communication or not based on its residual energy is of prime importance since it prevents anode from dying off the network. Thus the TAEER algorithm increases thelongevity of the network as given in figure 7.

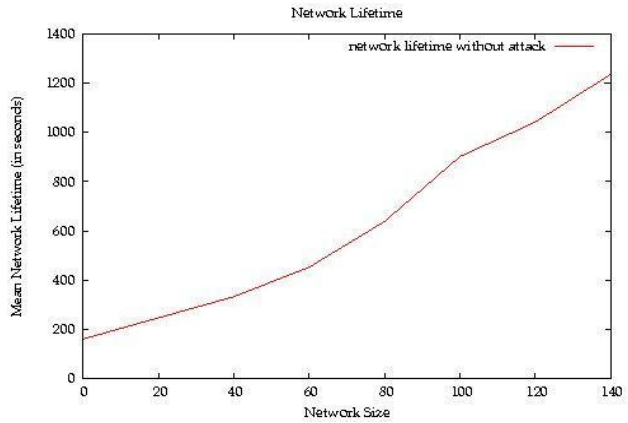

Figure 7: Network Size versus Network Lifetime

IX. CONCLUSION

This paperproposed the TAEER algorithm that is trustworthy thereby providing full network level privacy against security attacks. The TAEER algorithm functionson the concept of randomness in direction. The neighbors are classified based on their direction property andrandomness is involved in selecting the next hop node in transmission. Direction property andrandomness in node selection implements path variation and path length variation for the same set of source and destination.The Performance analysis of TAEER algorithmshows that the network lifetime is increased substantially and improves the throughput and packet delivery ratio when compared to existing Trust Aware Routing frameworkalgorithms. The jitter and delay haveshown substantial improvement..

REFRENCES

1. Djenouri, D, Khelladi, L.,Badache, A.N. "A Survey of Security Issuesin Mobile ad hoc and Sensor Networks", *Communications Surveysand Tutorials, IEEE,* vol. 7, no. 4, pages 2 – 28, 2005.
2. J. Lopez, R. Roman, I. Agudo and C. F. Gago, "Trust Management Systems for Wireless Sensor Networks: Best Practices," *Computer Communications*, vol. 33, no.9, pp. 1086-1093, 2010.
3. ShaikSahilBabu, ArnabRaha, MrinalKantiNaskar,"A Direct Trust Dependent Link State Routing ProtocolUsing Route Trusts for WSNs (DTLSRP)", Scientific Research Journal, vol 3,2011.
4. Nitinwankhade andSandipKadam, "Securing Wireless Sensor Network: Trust Aware Routing Framework (TARF)", *International Journal of Computer and Organization Trends*,vol. 14, no. 1,November 2014.
5. Guoxing Zhan, Weisong Shi, and Julia Deng ,"Design and Implementation of TARF: A Trust-Aware Routing Framework for WSNs, vol. 9, no. 2,2009.
6. Guanghua Zhang, Yuqing Zhang and ZhenguoChen"Using Trust to Secure Geographic and Energy Aware Routing against Multiple Attacks" *Chen National Natural Science Foundation of China*, 2014.
7. SurbhiTayal, ShaliniTiwariand and M. Mohan "Implementationof An Energy Efficient Routing Protocol: TARF (Trust-Aware Routing Framework),*International Journal of Engineering Research and Technology (IJERT)*,vol. 2, no. 5, May – 2013.
8. Leena and ArunKumar,"Designand Accomplishment of TARF:A Trust-Aware Routing Framework for WSNs",*International Journal of P2P Network Trends and Technology (IJPTT)*", vol. 2, 2014.
9. Suneyna and Bhavneesh Malik," Security Enhancement Based on Trust Aware Routing in Wireless Sensor Networks",*InternationalJournal of Advanced Research in Computer Science and Software Engineering* , vol. 3, no.9, September 2013.
10. Theodore Zahariadis, IoannisPapaefstathiou and Lionel Besson "Design and Implementation of a Trust-Aware Routing Protocol For LargeWSNs" *International Journal of Network Security & Its Applications (IJNSA*), vol.2, no.3, July 2010.
11. DipaliDikondwar,and R. K. Krishna "Implementation of Energy Efficient and TtrustAwareRouting for WSNs – Energy Consideration" ,*International Journal of Scientific and Engineering Research*, Volume 4, no. 7, July2013.
12. SaPragna, Shakeel Ahmed and .SaiManogna "Performance Analysis of Trust-Aware Routing Framework for Wireless Mesh Networks",*International Journal of Modern Engineering Research (IJMER)*,vol. 3, no. 5, 2013.
13. Geetha D Devanagavi, N Nalini, Rajashekar C Biradar.,"Trusted Neighbors Based Secured Routing Scheme in Wireless Sensor Networks Using Agents", *International Journal of Wireless Personal Communication*, vol 78, no 1,2014.
14. G. Priyadharshini andM.Parimala "Trust Aware Routing Framework for WSN", *Journal of Innovative Research in Computer and Communication Engineering*, vol.2, no 11, November 2014.

AUTHORS PROFILE

Prabha R, is currently working as an Associate Professor in the Department of Information Science and Engineering, Dr. Ambedkar Institute of Technology, Bangalore, India. She obtained her Bachelor of Engineering degree in Computer Science and Engineering branch.M.E in ComputerScience and Engineering from Computer Science Department, UVCE, Bangalore University in the year 2003. She has 22 years of teaching experience. Currently she is pursuing Ph.D in the Department of Computer Science and Engineering, University Visvesvaraya College of Engineering, Bangalore University, Bangalore. Her research interest is in the areaof Wireless Sensor Networks.

Krishnaveni M, completed her Bachelor of Engineering in Computer science and Engineering from BMS college of Engineering Bangaloreinthe year 2011. Masters of Engineering from in ComputerNetworking and Engineering from Computer Science Department, UVCE, Bangalore University in the year 2014.

Her research interest is in thearea ofWireless Sensor Networks.

Dr. S. H. Manjula, is currently working as an Associate Professor in the Department of Computer Science and Engineering, University Visvesvaraya College of Engineering Bangalore University, Bangalore, India. She obtained her Bachelor of Engineering degree in Computer Science and Engineering branch, Masters of Engineering and Ph D. in Computer Science and Engineering. She has published a book on Wireless Sensor Networks. She has published more than 30 papers in refereed international journals and conferences. Her research interests are in the field of Wireless Sensor Networks, Semantic web and Data Mining.

Dr. Venugopal K R is currently Special Officer, DVG Bangalore University and Principal, University Visveswaraya College of Engineering, Bangalore University Bangalore. He obtained his Bachelor of Engineering from University Visvesvaraya College of Engineering. He received his Master's degree in Computer Science and Automation from Indian Institute of Science Bangalore. He was awarded Ph. D in Economics from Bangalore University and Ph. D in Computer Science from Indian Institute of Technology, Madras. He has a distinguished academic career and has degrees in Electronics, Economics, Law, Business Finance, Public Relations, Communications, Industrial Relations, Computer Science and Journalism. He has authored and edited 39 books on Computer Science and Economics, which include Petrodollar and the World Economy, C Aptitude, Mastering C, Microprocessor Programming, Mastering C++ and Digital Circuits and Systems. During his three decades of service at UVCE he has over 400 research papers to his credit. He was a Post-Doctoral Research Scholar at University of Southern California, USA. His research interests include Computer Networks, Wireless Sensor Networks, Parallel and Distributed Systems, Digital Signal Processing and Data Mining.

Dr. L. M. Patnaik, is honorary professor in Department of Computer Science and Automation, Indian institute of Science, Bangalore. During the past 35 years of his service at the Institute he has over 700 research publications in refereed International Conference Proceedings. He is a Fellow of all the four leading Science and Engineering Academies in India. Fellow of the IEEE and the Academy of Science for the developing world. He has received twenty national and international awards. Notable among them is the IEEE Technical Achievement Award for his significant contributions to High performance Computing and Soft Computing. He is an Ex-Vice Chancellor Defense institute of Advanced Technology, Pune India. His area of research interest has been Parallel and Distributed Computing, Mobile Computing, CAD for VLSI circuits, Soft computing and Computational Neuroscience.