International Journal of Future Innovative Science and Engineering Research (IJFISER)
Volume - 2, Issue - II ISSN (Online): 2454- 1966

Research Manuscript Title

Trust Value Estimation for Secure Data Forwarding In Wireless Sensor Network

[1]Ms.B.Rajarajeswari, M.E.., [2]Ms. S.Sundari,

Assistant Professor, P.G.Scholar,
Department of CSE
Arulmigu Meenakshi Amman College of Engg., Thiruvannamalai District, Tamilnadu, India.

E-Mail: s.sundari91@gmail.com

JUNE – 2016

www.istpublications.com

Trust Value Estimation for Secure Data Forwarding In Wireless Sensor Network

[1]Ms.B.Rajarajeswari, M.E.., [2]Ms. S.Sundari
Assistant Professor, P.G.Scholar,
Department of CSE
Arulmigu Meenakshi Amman College of Engg., Thiruvannamalai District, Tamilnadu, India.
E-Mail: s.sundari91@gmail.com

ABSTRACT

It is important to secure the data while transition in wireless sensor network. Because the information passed from source to destination may contains valuable information. In large area network the attackers may have the way to steal the valuable data which is sent by source. Many security techniques are used for protecting the data. Now a days, Trust is used for secure the data as well as identify the malicious node and block list them. Trust value calculated depending upon the energy parameters. It achieves efficient and secure transmission compared to other techniques. To support scalability, nodes are often grouped into disjoint clusters. Each cluster would have a leader, often referred as cluster head (CH).A CH is responsible for not only the general request but also assisting the general nodes to route the sensed data to the target nodes. The power-consumption of a CH is higher than of a general (non-CH) node. Trust management that models the trust on the behavior of elements of the network, can be especially useful for a sensor network environment to enhance security.

Keywords- trust value calculation, wireless sensor network, cluster head, energy harvesting.

I. INTRODUCTION

A wireless sensor network consists of spatially distributed autonomous sensors to monitor and react to environmental conditions and send the collected data to a command center using wireless channels. The hardware components of a sensor node include a radio transceiver, an embedded processor, internal and external memories, a power source and one or more sensors. A sensor node can sense and forward the information through multi hop routing. The primary security goals for sensor networks are confidentiality, integrity, availability and authentication of data. It is possible that the emerging importance of sensor networks could be hindered by their inherent security problems. It is then imperative to provide a set of security primitives and services that can protect those networks and improve their robustness and reliability.

Due to limited resources of WSNs, it is challenging to incorporate basic security functions such as authentication and privacy. As a result, wireless sensor networks are prone to different types of malicious attacks, such as denial of service, routing protocol attacks etc. Traditional crypto schemes are incapable of preventing such types of malicious attacks. Trust management, which models the trust on the behavior of the elements of the network, can be especially useful for a sensor network environment.

However traditional trust management schemes developed for wired and wireless networks may not be suitable for networks with small sensor nodes due to limited bandwidth and memory constraints. Trust management can help improving the security of WSN. For example, for the routing process, sensor nodes might need to know which other nodes to trust for forwarding a packet. For sensing purposes a node might need to trust other neighboring nodes for checking anomalous measurements.

However, as sensor nodes are usually constrained devices, the trust management systems must be lightweight enough to provide a good performance without hindering the functionality of the system. This survey deals with various trust management schemes proposed for WSNs.

The data collection technique is being employed to store and collect data items and parameters on a database server [3][4]. All the related data items are stored in accessible data form. The problem encountered in the recent past was of the battery power consumption more efficient data collection and collection techniques with right decision making capabilities, Therefore, this paper proposed the efficient and effective architecture and mechanism for mentioned

problem using principles like global weight calculation of nodes , data collection for cluster head and data collection techniques using data cube collection.

Wireless Sensor Network generates a large amount of data that has to be aggregated at various levels. A multidimensional collection approach is considered for exhibiting the node parameters for each network. Bandwidth, memory, signal strength, time, battery power etc. have been utilized to examine the performance of a sensor network, its efficiency can be enhanced by reducing the cost of cluster development. Sensor nodes are becoming popular in mobile communication technology due to their fast communication speed and better result generation in information systems.

Sensor nodes are useful in disaster, war zone and several modern technology like mobile technology, laser technology etc where the data has to be transferred accurately and in a fraction of time where each node is responsible for the extraction and transfer of data such that the data to be exchanged cannot be lost on its way to the receiver. Data Collection uses the parameters of nodes joining the cluster so that the data attributes are selected and stored in an aggregated format for further evaluation and usage.

Data Collection refers to the technique that models the data and information in a dimensional construct that is easy to store and retrieve. The data collection technique is being employed to store and collect data items and parameters on a database server. All the related data items are stored in accessible data form. The problem encountered in the recent past was of the battery power consumption more efficient data collection and collection techniques with right decision making capabilities, Therefore, efficient and effective architecture and mechanism for mentioned problem using principles like global weight calculation of nodes , data collection for cluster head and data collection techniques using data cube collection.

II. RELATED WORK

The concept of trust management in Adhoc sensor network is an efficient tool to handle node misbehavior attacks in network. Trust is integrated component in everyday life, in the context of computer science there are many defamations used and differ with application areas. In a broad manner trust is an essential component for semantic web. According to previous work the trust is the degree of belief about the future behavior of other entities [8, 9]. The first time Blaze, Feigenbaum and Lacy [10] used the term trust management and introduced as a separate security component. There are many trusts based routing approaches have been proposed to detect malicious nodes in network. In 2013 [11] author proposed a trust model and combine each node direct and indirect trust information to define the trustworthiness of all its one hop distance neighbors. Shaikh et al. [11] proposed a group-based trust management scheme for clustered WSNs in which each SN performs peer evaluation based on direct observations or recommendations, and each cluster head (CH) evaluates other CHs as well as SNs under its own cluster. This work is similar to ours in that a hierarchical structure is employed for scalability. However, trust in their case is assessed only based on past interaction experiences in message delivery, which in our case is just one possible trust component along with other social and QoS trust components comprising the overall trust metric. Furthermore, we address the trust formation issue (i.e., how a peer-to-peer trust value is formed) to maximize application performance. The proposed trust based approaches find their trusted nodes in the wireless sensor network based upon the energy, packet count and queue size. Trust achieves better route anonymity protection with lower cost.

III. PROPOSED WORK

The traditional cryptography schemes that provide authentication and data privacy do not detect when an internal node provides false routing information, or where a node does not cooperate with the other nodes to save its resources. Propose Trust based secure routing technique gather the neighbor node information such as energy, packet count, queue size for identifying whether the node is trust or not.C_TV (Computed trust value) value is calculated[11] .If the value is greater than the targeted value then the nodes is consider as a malicious node and add it to the block list. A trust based routing provides a secure transmission between source and destination. Sensor network have the trusted routing algorithm for secure transmission.

The AODV protocol uses sequence numbers to determine the timeliness of each packet and to prevent the creation of loops. Expiry timers are used to keep the route entries updated. Link failures are propagated by a route error (RERR) message from a broken link to the source node of the corresponding route. When the next hop link breaks, RERR packets are sent by the starting node of the link to a set of neighboring nodes that communicate over the broken link with the destination. This recursive process erases all broken entries from the routing table at each node. Since nodes reply to the first arriving RREQ packet, AODV protocol favors the least congested route instead of the shortest route. Note that the fact that

the on-demand approach of the AODV protocol minimizes routing table information potentially leads to a large number of route requests being generated.

The proposed trust routing help in deciding the secure route from source to destination [8][9]. The algorithm namely record and trust based management. We provide the criteria for the source node could be able to find more route rather than one trust route for transmission. Data is sent between nodes in a WSN by hopping through intermediate nodes, which must make decisions about where and how to route the data. WSN faces several problems because of node mobility, network traffic, network size, and the possibility of node faults. The efficiency and behavior of a WSN depends on how well information can be passed around and delivered.

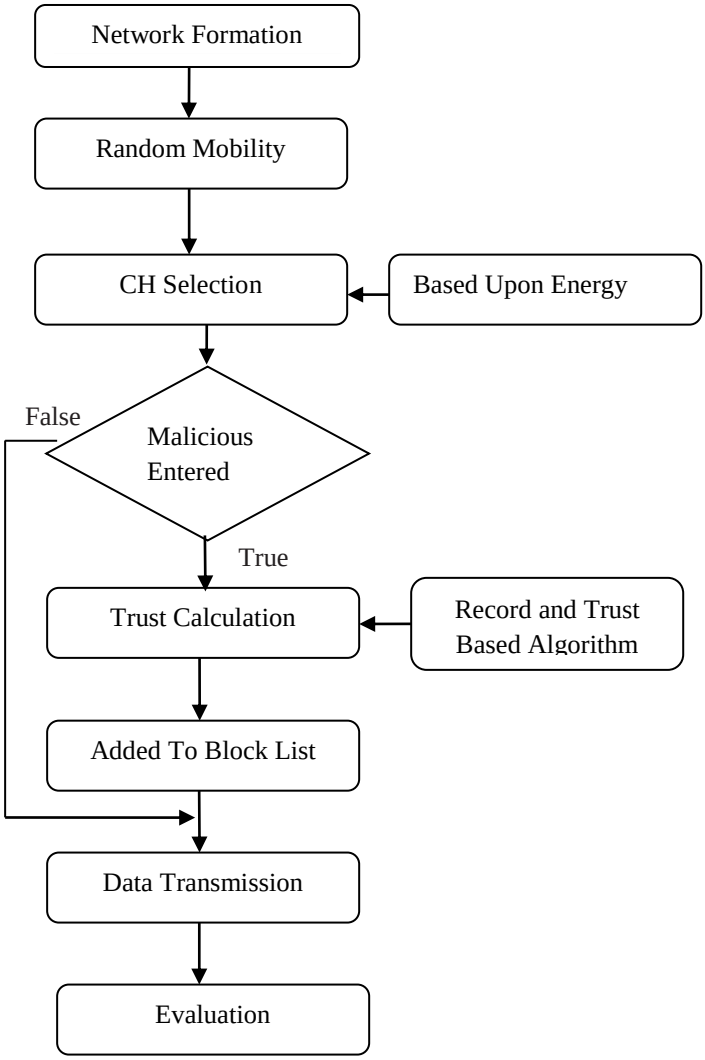

Figure 1.Trust Based Approach

IV. ENERGY CONSERVATION IN WSN

Energy is a factor of outmost importance in WSNs. To increase network lifetime, energy must be saved in every hardware and software solution composing the network architecture. According to the radio model, data communication is responsible for the greatest weight in the energy budget when compared with data sensing and processing. Therefore, it is desirable to use short range instead of long-range communication between sensor nodes because of the transmission power required. In most WSN scenarios, events can be sensed by many source nodes near the phenomenon of interest and far away

from the sink nodes. Then, the use of short-range communication leads obligatorily to data packets being forwarded through intermediate nodes along a multi-hop path.

Minimizing the energy consumption of a wireless sensor network application is crucial for effective realization of the intended application in terms of cost, lifetime, and functionality [4]. However, the minimizing task is hardly possible as no overall energy cost function is available for optimization. Energy consumption is easily one of the most fundamental but crucial factor determining the success of the deployment of sensors and wireless sensor networks (WSNs) due to many severe constraints such as the size of sensors, the unavailability of a power source, and inaccessibility of the location and hence no further handling of sensor devices once they are deployed.

Efforts have been made to minimize the energy consumption of wireless sensor networks and lengthen their useful lifetime at different levels and approaches. Some approaches aim to minimize the energy consumption of sensor itself at its operating level, some aim at minimizing the energy spent in the input/output operations at data transmission level and others target the formulation of sensor networks in terms of their topology and related routing mechanisms[5][6].

V. NETWORK MODEL

Nodes are created for sending and receiving the data packets.AODV (Adhoc On-Demand Distance Vector) routing protocol is used for routing the information which was sent by source [11].TCP is used for establishing the connection between the source and destination. File transfer protocol (FTP) and randomly choose different source-destination connections. Nodes are created for sending and receiving the data packets. AODV(Adhoc On-Demand Distance Vector) routing protocol is used for routing the information which was sent by source. TCP is used for establishing the connection between the source and destination. File transfer protocol(FTP) and randomly choose different source-destination connections.

TCP/IP is a two-layer program. The higher layer, Transmission Control Protocol, manages the assembling of a message or file into smaller packet that are transmitted over the Internet and received by a TCP layer that reassembles the packets into the original message. The lower layer, Internet Protocol, handles the address part of each packet so that it gets to the right destination. Each gateway computer on the network checks this address to see where to forward the message. Even though some packets from the same message are routed differently than others, they'll be reassembled at the destination.

TCP/IP uses the client/server model of communication in which a computer user (a client) requests and is provided a service (such as sending a Web page) by another computer (a server) in the network. TCP/IP communication is primarily point-to-point, meaning each communication is from one point (or host computer) in the network to another point or host computer. TCP/IP and the higher-level applications that use it are collectively said to be "stateless" because each client request is considered a new request unrelated to any previous one (unlike ordinary phone conversations that require a dedicated connection for the call duration). Being stateless frees network paths so that everyone can use them continuously. (Note that the TCP layer itself is not stateless as far as any one message is concerned. Its connection remains in place until all packets in a message have been received.)

VI. CH SELECTION

Cluster head is selected based upon the energy. The nodes which have the highest energy are taken as CH. Clustering plays an important role for energy saving in WSNs. With clustering in WSNs, energy consumption, lifetime of the network and scalability can be improved. Because only cluster head node per cluster is required to perform routing task and the other sensor nodes just forward their data to cluster head. Clustering has important applications in high-density sensor networks, because it is much easier to manage a set of cluster representatives (cluster head) from each cluster than to manage whole sensor nodes [1][2].

CH nodes aggregate the data (thus decreasing the total number of relayed packets) and transmit them to the base station (BS) either directly or through the intermediate communication with other CH nodes. However, because the CH nodes send all the time data to higher distances than the common (member) nodes, they naturally spend energy at higher rates. A common solution in order balance the energy consumption among all the network nodes is to periodically re-elect new CHs (thus rotating the CH role among all the nodes over time) in each cluster. A typical example of the implied hierarchical data communication within a clustered network (assuming single- hop intra cluster communication and multi-hop inter cluster communication) The BS is the data processing point for the data received from the sensor nodes, and where the data is accessed by the end user. It is generally considered fixed and at a far distance from the sensor nodes.

Hierarchical clustering in WSNs can greatly contribute to overall system scalability, lifetime, and energy efficiency [5][6]. Hierarchical routing is an efficient way to lower energy consumption within a cluster, performing data aggregation and fusion in order decrease the number of transmitted messages to the BS. On the contrary, a single-tier network can cause the gateway to overload with the increase in sensors density. Such overload might cause latency in communication and inadequate tracking of events. In addition, the single-tier architecture is not scalable for a larger set of sensors covering a wider area of interest because the sensors are typically not capable of long-haul communication. Hierarchical clustering is particularly useful for applications that require scalability to hundreds or thousands of nodes. Scalability in this context implies the need for load balancing and efficient resource utilization. Applications requiring efficient data aggregation are also natural candidates for clustering. Routing protocols can also employ clustering.

VII. TRUST CALCULATION

The Trust value on the basis of three parameters

- Energy
- Packet Count
- Queue Size

When current trust value is greater than 0.7, there may be a selfish node in the network. If the selfish nodes are identified then it is added to block list. Otherwise the data send to destination [10][11].

Record based trust calculation

Begin
Route discovery process start
Neighbor node information gathered
i) Energy
ii) Packet count
iii) Queue Size
Trust calculation
$T_c = t_s + P / 2$
Where,
T_c - Trust calculation
t_s - Time success
P - Positive real number
t - Time transaction
The current trust value is retrieved.
if (T_CV > 0.7)
Begin
Malicious node is detected
Add to block list
Else
Data transmitted
End
End

VIII. PERFORMANCE ANALYSIS

Packet Delivery ratio: Many protocols in wireless sensor networks use packet delivery ratio (PDR) as a metric to select the best route, transmission rate or power.

Packet overhead: It takes to transmit data on a packet-switched network. Each packet requires extra bytes of format information that is stored in the packet header, which, combined with the assembly and disassembly of packets, reduces the overall transmission.

Routing cost: In packet switching networks, routing directs packet forwarding (the transit of logically addressed packets

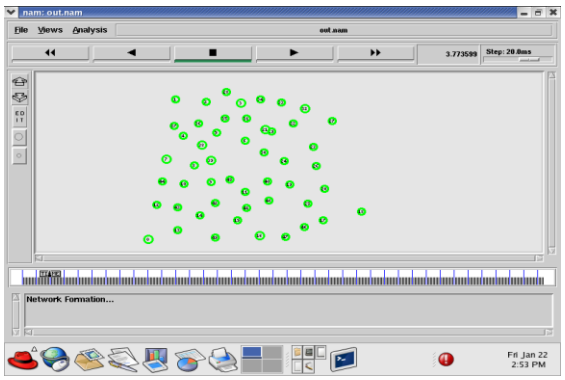

Figure 2. Network Formation

Figure 2 shows the nodes in the network are equipped with a transceiver that can operate in one of two modes: transmission or reception. The receiver node is able to detect the presence of a carrier signal and measure its power even for messages that cannot be decoded into a valid packet. AODV (Adhoc On-Demand Distance Vector) routing protocol is used for routing the information which was sent by source.

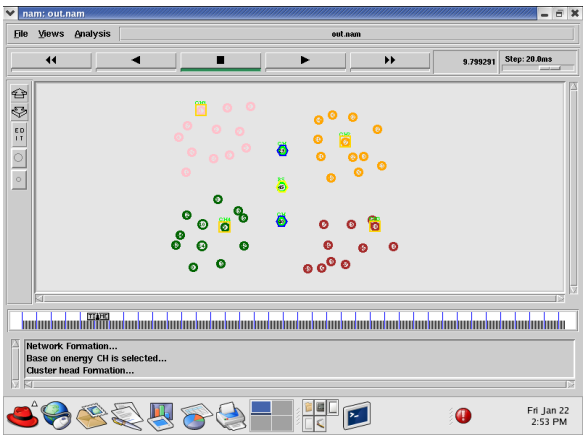

Figure 3. Cluster Selection

Figure 3 describes the four groups of clusters. Every group has 10 nodes. Each and every node has a cluster head to send a data. Two groups send their data to one common cluster head. The cluster head collect the all nodes information and send their data to destination.

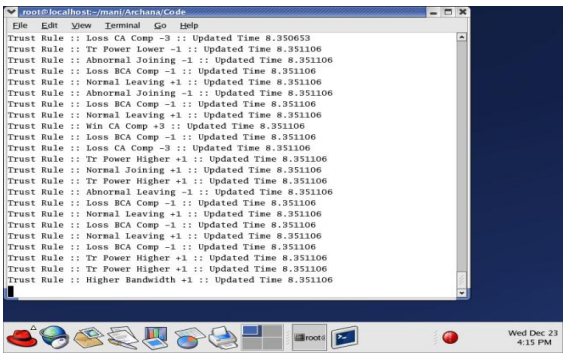

Figure 4.Energy Consumption Of Nodes

Figure 4 shows the consumption of energy by sending and receiving packets. Initially the energy level is 500J.the energy taken by the node 1 is 23.0.the clustering method consumes the very low energy compared to single node transmission.

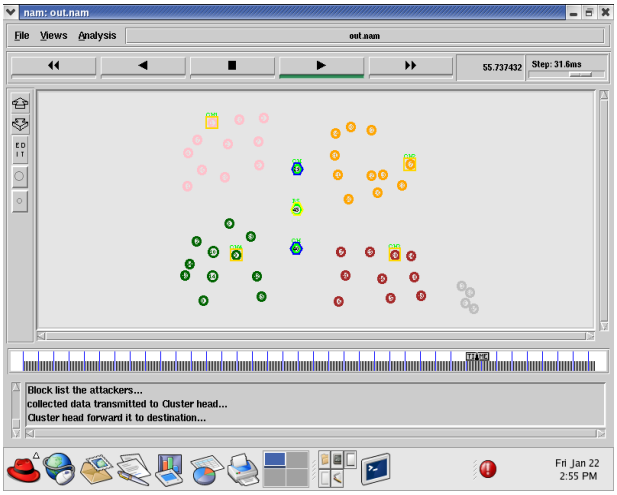

Figure 5.Malicious Node Detection

Figure 5 describes that the data forward using trust node secure the transmission. If the node is malicious then the node does not transmit their packet to cluster head. The malicious node is identified by the trust value calculation. The nodes which have the value of more than 0.7 is malicious node. This kind of node can be identified and blocked before the data transmission.

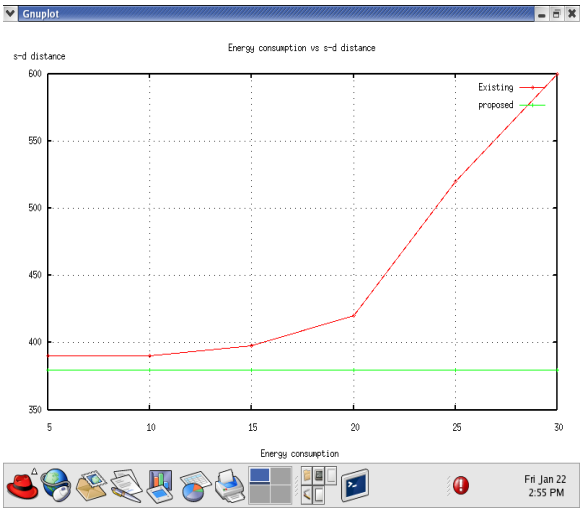

Figure 6.Energy Harvesting

Figure 6 shows the graph, the system uses less energy consumption. The system initial energy was set to 500J.Compared to existing system our system reduces the time taken to detect selfish nodes and consumes less energy

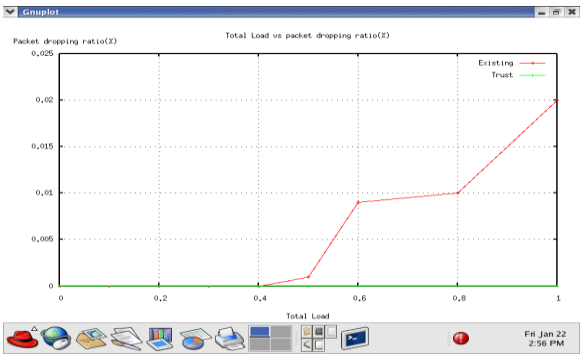

Figure 7.Packet Delivery Ratio

Figure 7 shows the graph, packet delivery ratio is transmit their data to best route with low energy consumption.

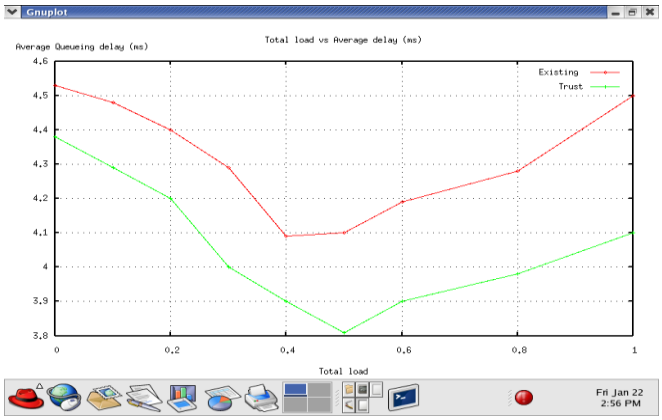

Figure 8.End to End Delay

Figure 8.shows the graph; the proposed system reduces the delay and energy.

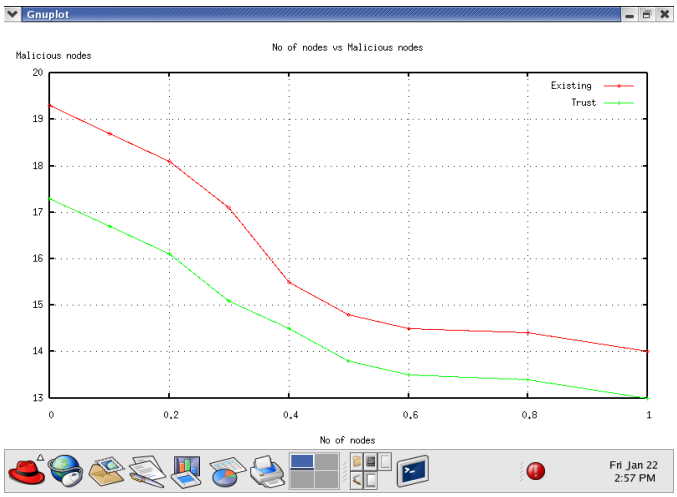

Figure 9.Reduction of Malicious Nodes

Figure 9 shows the graph, the system reduces the malicious nodes based upon the trust calculation. The node below 0.7 is considered as trust node.

XI. CONCLUSION

The proposed approach reduces maximum packet delay ratio than existing system. We achieve better secure transmission. Our trust based routing provides maximum energy efficiency and achieves good performance than existing system. It also reduces packet delay while transmitting. With this minimum overhead, we can easily eliminate the malicious node as well as we can establish a best trusted route between source and destination. Also it creates a secure communication in this environment without any internal attackers. Using simulation results, the performance of this novel protocol is justified. In the future, it will be incorporate with other WSN routing protocols. Current threshold value which can defend against potential active anonymous attacks without unveiling the node identities. Malicious nodes don't have any way to access the information from the nodes. And it provides reliable data transmission.

REFERENCES

[I] Alayev.Y, ChenF,HouY., JohnsonM. P., Bar-NoyA., "Throughput maximization in mobileWSN scheduling with power control and rate selection," in Proc.IEEE 8th Int. Conf. Distrib.Comput. Sensor Syst., 2012, pp. 33–40.

[II] Bar-Yehuda. R and EvenS., "A local-ratio theorem for approximating the weighted vertex cover problem," Annu. Discrete Math.,vol. 25, pp. 27–45, 1985.

[III] Basagni.S, Bol€ oniL.,GjanciP., PetrioliC., PhillipsC. A.,and D. Turgut, "Maximizing the value of sensed information in underwater wireless sensor networks via an autonomous underwatervehicle," in Proc. IEEE Conf. Comput. Commun., 2014,pp.988–996

[IV] Liang.W, RenX.,JiaX., and XuX., "Monitoring quality maximization through fair rate allocation in harvesting sensor networks,"IEEE Trans. Parallel Distrib. Syst., vol. 24, no. 9, pp. 1827–1840,Sep. 2013.

[V] Liang.W, SchweitzerP.,and XuZ.,"Approximation algorithms for capacitated minimum forest problem in wireless sensor networks with a mobile sink," IEEE Trans. Comput., vol. 62, no. 10,pp. 1932–1944, Oct. 2013.

[VI] Sandra Sendra, Jaime Lloret, Miguel García and José F. Toledo Power saving and energy optimization techniques for Wireless Sensor Networks .2011

[VII] Sandra Sendra, Jaime Lloret, Miguel García and José F. Toledo Power saving and energy optimization techniques for Wireless Sensor Networks .2011

[VIII] H. Chen, H. Wu, J. Hu, and C. Gao., "Agent-based Trust Model in Wireless Sensor Networks., "Eighth ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing", 2007, pp.119-124

[IX] A. Boukerche, and X. Li., "An Agent-based Trust and Reputation Management Scheme for Wireless Sensor Networks", IEEE GLOBECOMM, 2005.2nd ACM workshop on Security of ad hoc and sensor networks (SASN '04), October 2004, pp 66-77

[X] M. Blaze, J. Feigenbaum, and J. Lacy, "Decentralized trust management," inSecurity and Privacy, 1996. Proceedings., 1996 IEEE Symposium on, 1996, pp. 164-173.