Received: December 14, 2017

International Journal of
Intelligent Engineering & Systems

http://www.inass.org/

TDP: A Novel Secure and Energy Aware Routing Protocol for Wireless Sensor Networks

Suyambu Karthick[1]*

[1]*Sea Sense Softwares Pvt. Ltd., Kanyakumari, Tamil Nadu, India*
* Corresponding author’s Email: karthicksuyam@gmail.com

Abstract: Now a day the usage of Self-Organizing Networks (SONs) is increasing, because of its broad application. Unlike common networks, the SONs have the capability of reconfiguration, whenever any defect occurs in the network. However, while routing in this network, the loss of data occurs due to its security lack. Hence many researchers have presented their research for providing secure routing in various SONs. However, the security is still an issue in the routing of SONs especially in Wireless Sensor Network (WSN). Here in this paper, a novel protocol for the secure routing of WSNs has developed. The proposed protocol is named as Trust-Distrust Protocol (TDP). As per the proposed protocol, the routing is done in four stages. The initial stage is topology management using the k-means algorithm. The second stage is Link Quality Appraisal (LQA), where the quality of every network node is evaluated. The third stage is grading, in which it is based on the LQA value and a grade point is allotted to every node in the network. In the last stage, the most secure path for the routing is determined based on the grade points. The proposed protocol is tested in one of the major kinds of SONs, like WSN using the NS2. By comparing with the existing LEACH protocol, the performance is evaluated. Ultimately the proposed protocol outperformed the performance of the existing routing protocol and suggested for rounding in SONs.

Keywords: Wireless Sensor Network, secure routing, energy-aware routing, improved k-means algorithm, routing protocol.

1. Introduction

The wireless network becomes a part of day to day life, because of its tremendous application. Self-organizing wireless network is encouraged to provide anytime, anywhere networking service. Wireless Sensor Network, Mobile Ad hoc Network (MANET), Vehicular Ad hoc Network (VANET) and Wireless Mesh Network (WMN) are the most usable self-organizing network. Among them, WSN has its unique advantages, and widely used in industrial and military purpose [1].

WSN is configured with any sensor nodes, which can act as a sender as well as a receiver. Each sensor nodes has its battery backup, storage and an antenna. The sensor network can operate in a specified frequency band, and didn't have any specified topology. Security and energy become major issues, it should be concentrated throughout the communication in WSN. Sensor networks have the self-organizing feature and thus the automatic selection of sender and receiver is applicable hence security become a milestone in WSN [2]. WSN can support multimedia information transmission, in this case, the energy and Quality of Service (QoS) should be concentrated while routing [3-5].

Recent researches in WSN have proposed different routing protocol, among them energy is most considered objective in their routing strategy. Routing protocol has most of the attention because it can vary from the network architecture and its application [6]. In micro sensor networks it can contain hundreds or thousands of sensing nodes. It is essential to develop cheap and energy efficient sensor nodes [7]. In contrast with IP-based communication, which depends on global addresses as well as routing metrics of hop counts, the sensor nodes typically lack global addresses [8]. The primary challenge in designing WSN is the provision of the functional, and the non-functional, for example, data latency and integrity respectively [9].

In this paper, a novel routing protocol for WSN is introduced, which is named as TDP. The proposed protocol has four stages of operation, in the first stage topology management is done. The WSN do not configure any desired topology. Hence it is essential to maintain a topology to achieve proper communication. An improved k-means algorithm is applied to the topology management. The second stage is Link Quality Appraisal (LQA), where the quality of every node is analysed. The third stage is Grading, in which based on the quality of the node a grade value is assigned to every node. Then in the final stage based on the grade point value a secure and low energy consuming path will be selected for routing. The outline of the paper is as per the following: the recent research related to the WSN routing is given in section 2. Proposed trust distrust protocol for the WSN routing is described in section 3. Implementation results and discussion is given in section 4. Then in the subsequent sections, the conclusion and reference to the paper are given.

2. Related work

Some of the current research related to the routing in WSN is listed below;

Wireless sensor networks are one of the most usable technologies in this era. However, the sensor nodes are limited by energy resources, hence developing an energy-efficient routing protocol for WSN become the research motivation. Gurbinder Singh Brar et al. [10] have exhibited a hybrid optimization based PEGASIS-DSR routing protocol that utilizes cache and directional transmission idea of both proactive and responsive routing protocol. Xiaonan Wang et al. [11] have delivered the addressing based routing techniques (ABRS) for WSN. Based on perceptions that sensor networks may neglect to be designed with an address because of lack of routes and address space along a tree will not be ideal. Ju Ren et al. [12] have developed a model to assess energy consumption, lifetime and traffic load of sensor networks in data gathering WSN. Their propagation comes about the display that their proposed model could assess energy hole evolution process inside an ER smaller than 5%.

Juan Luo et al. [13] have focused on minimizing energy consumption and maximizing the system lifetime of 1D queue organize where areas of sensors were unchangeable and predetermined. For this matter, they get information from opportunistic routing theory to advance the system energy consumption. Trong-Thua Huynh et al. [14] have proposed another distributed clustering strategy to select the best cluster head for every cluster in WSNs keeping to trade-off end-to-end delay and energy consumption.

Viji Gripsy Jebaseelan and Anithalakshmi Srinivasan [15], have developed a new lightweight route selection scheme with the security concern. Saravanan Nallusamy et al. [16] have proposed Mobile Agent-based Energy Efficient Reliable routing protocol for MANET. Sankar Sennan and Srinivasan Palanisamy [17] have introduced Load and battery discharge index (BDI) based composite routing metric in IPV6 Routing Protocol for Low power and lossy network (RPL).

To accomplish the efficient cluster head selection in WSN based IoT, Praveen Kumar Reddy, and Rajasekhara Babu [18] have used Fuzzy C-Means (FCM) clustering algorithm. They proposed a novel method with the combination of Optimal Secured Energy Aware Protocol (OSEAP) and Improved Bacterial Foraging Optimization (IBFO) algorithm. Banoth Rajkumar and Gugulothu Narsimha [19] have proposed an incorporation mechanism for primitives to provide complete cryptography services for Mobile Ad-Hoc Networks (MANETs). Nirmala Hiremani and Tiptur Gangaraju Basavaraju [20] have proposed an algorithm to improve the lifetime using PSO.

Imbalanced energy consumption was one of the problems in the cluster based WSN. Hence Soundaram Jothi and Muthial Chandrasekaran [21] have proposed an efficient data aggregation tree for communication and routing. Hsiang-Hung Liu et al. [22] have considered the shortest distance between two points is a straight line and that two straight lines in a plane are likely to intersect and develop for WSNs as an improved protocol called straight-line routing (SLR). This technique suggested for efficient energy based routing in WSN.

The existing techniques [10, 18, 20] uses optimization algorithm, in general, the optimization takes time. So while use in WSN it is tough to achieve the overall network performance. The techniques in [19], concentrated on security, so consumed high energy hence it becomes a significant problem in these techniques. The techniques proposed in ref [17, 20, 21,], only concentrates on energy-aware routing. Now a day many advanced techniques were proposed routing in WSN by concentrating energy and security. Thus in this paper to overcome these drawbacks proposed a novel protocol for secure and energy aware routing in WSN.

3. Proposed trust-distrust protocol

Providing secure routing in WSN becomes a challenging task, hence many research works have been presented. Still, there is a vacuum for research in the routing protocol for WSN. In this paper, I have developed a novel strategy for the routing in WSN, which can also provide the security during data transmission. The proposed routing strategy is named as TDP. In this section, the description of the proposed routing protocol is described in detail. The lack of continuous network connectivity becomes a noticeable technical problem in WSN.

In this paper a novel routing protocol for the WSNs is developed, the proposed approach comprises of four phases they are topology management, fitness value calculation, trust-distrust setting and path selection. In WSN proving a constant link between sensor nodes is a complex task. Thus in the proposed system, a virtual topology is generated to ease the routing process. An improved k-means algorithm is utilized for the topology management. Then the fitness value of every node is determined by sending and receiving sample packets. Subsequently, based on the fitness value the trust-distrust value is defined for the nodes based on this value then the routing path is selected. The architecture for the proposed TDP is given in Fig. 1.

3.1 Topology management

In WSN to realize the management of the overall delivery topology, employed the topology management. In the proposed protocol an improved k-means algorithm is used for managing the topology. The improved K-means algorithm clustering technique which groups the nodes based on the similarity. Clustering is a soft computing technique which can gather similar objects or items in the same group.

The attributes considered here to group the node is distance and energy. Hence in this paper, the sensor nodes are grouped based on the distance between each node. The nearest nodes with closer energy level have kept in the same group. In WSN clustering the selection of a center node (cluster head) is one of the challenging tasks. An improved k-means algorithm is applied in the proposed protocol for the clustering and cluster head selection.

Steps involved in the improved k-means algorithm for clustering the nodes in WSN is as follows:

Step 1: Consider ‘k' initial centroid for clustering the sensor nodes into ‘k' cluster. In the conventional k-means algorithm, the initial centroid is placed at a random position. In the proposed improved k-means algorithm initial centroid is placed at an equal distance to each other.

Step 2: Euclidian distance based clustering is undergone. To find the minimum variance clustering of nodes into k clusters. To find the k centroids, $\{m_j\}^k \mid j$=1 in R_d is,

$$\left(\frac{1}{n}\right) \times \sum \left(\min_{j} d^2(X_i, m_j) \right), \;\; for\ i = 1 \text{to}\ n \qquad (1)$$

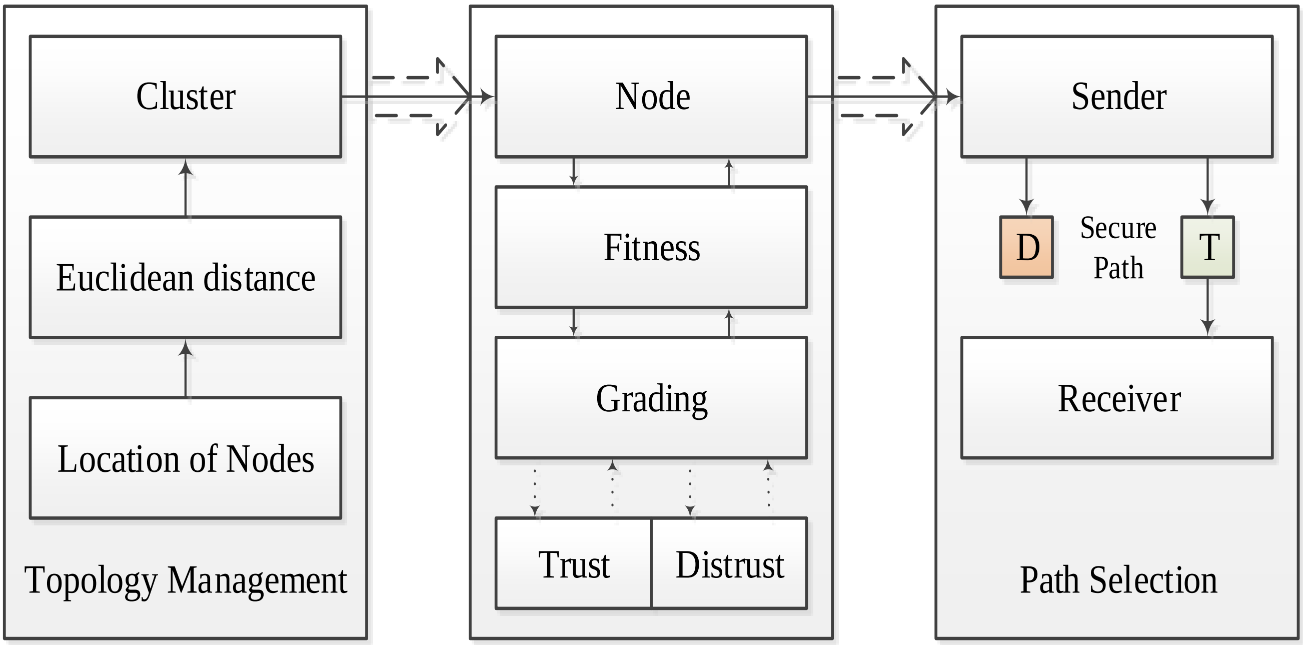

Figure.1 Architecture of TDP

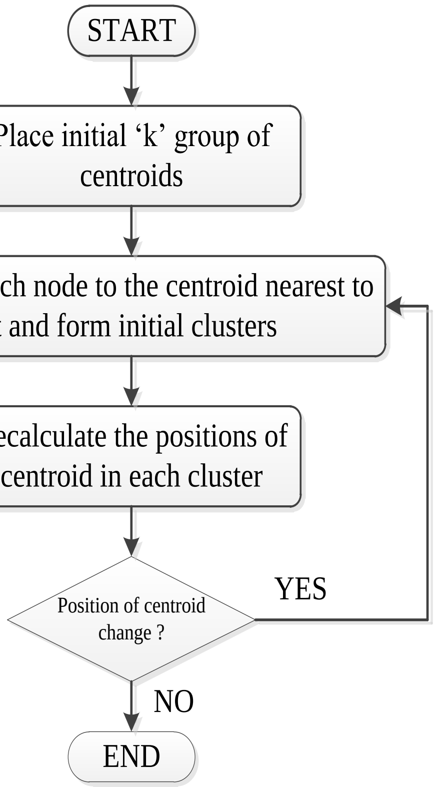
START
Place initial ‘k’ group of centroids
Assign each node to the centroid nearest to it and form initial clusters
Recalculate the positions of centroid in each cluster
Position of centroid change ?
YES
NO
END

Figure.2 Flowchart for clustering the nodes in WSN

Where, $d(X_i,m_j)$ is the Euclidean distance between X_i and m_j. Then the points $\{m_j\}^k \mid j=1$ known as the cluster center.

Step 3: Centroid update by recalculating the centroid position.

Step 4: If the position of centroid changes, the iteration is repeated by moving to Step 2, otherwise the clustering gets finalized.

The above steps can perform clustering of nodes into ‘k' clusters, and cluster heads are to be chosen as shown in Fig. 2.

The improved k-means algorithm can group the nodes in the nearest region, and the cluster head is assumed as a base node so that the link can provide easily. Then the fitness value for every node in WSN has to be calculated and it is discussed in the subsequent section.

3.2 Link quality appraisal

In this phase the trust ability or the quality of every node in the WSN is calculated, it ensures the denial-of-service (DoS) attack. The DoS attack consists of efforts to temporary or permanent interrupt in communication path. Hence to ensure the trust ability of a node in WSN, a sample set of packets is sent and receive it back by the same node, the sending and receiving ratio represents the fitness value of the particular node.

For example, consider two sensor nodes ‘X' and ‘Y', here ‘X' wants to verify the fitness value of sensor node ‘Y'. The sensor node ‘X' sent a set of hello packets to ‘Y'. Sensor node ‘Y' receive the packets and retransmit it to ‘X'. If the number of packets transmitted and received by ‘X' is same, then the fitness value of node ‘Y' is 100%. In our protocol, the cluster head acts as the base node. Hence the base node alone verifies the fitness of other nodes in their cluster. The fitness value of a node can be found out by using the Eqn. (2).

$$F_i = \frac{FP_i}{RP_i} \times 100 \tag{2}$$

Where;
‘F_i’- Fitness Value of i^{th} node
‘FP_i’- No of packets forwarded by i^{th} node
‘RP_i’- No of packets received by i^{th} node

3.3 Grading

In general term, the trust and distrust is a kind of appreciation, to motivate and hour best participant in everywhere. In this paper, the trust and distrust is a kind of ranking based on the trust ability of nodes in WSN. Eqn. (3) gives the formula for calculating the trust-distrust value.

$$TD = \frac{F_i}{10} \tag{3}$$

Where, TD is the Trust-distrust it is calculated to define the fitness value out of 10.

The syntax for calculating the trust-distrust setting is shown in Fig. 3, the trust value is given for the node having TD value is higher than five and if the TD value is five or less than five distrust values is given. For example if the nodes N1, N2, N3, N4, N5, N6, N7, N8, N9 and N10 having TD values as 10, 9, 8, 7, 6, 5, 4, 3, 2 and 1 respectively. Then the trust-distrust setting become T5, T4, T3, T2, T1, D1, D2, D3, D4 and D5 respectively, where T5 means Trust-5 and D5 means Distrust-5. Hence the highest trust node is highly believed for secure routing, and highest distrust node is never considered for routing.

```
if (TD>5)
        Trust  from 1 to 5
else if (TD≤5)
        Distrust from 1 to 5
end
```

Figure.3 Syntax for honouring Trust-distrust

3.4 Path selection

Selection of path is one of the crucial processes in every network, and it became a challenging task in WSN. In the proposed system the path is selected by trust-distrust setting. The operation of path selection based on the proposed approach is shown in Fig. 4. The path selection is a major process in the WSN so in the proposed system the path is selected based on the trust-distrust setting.

Initially, the nodes in the WSN are grouped based on the distance, and the trust value for every node is calculated by sending the sample packets. Then based on the fitness value, the trust-distrust value is provided for every node, and this value is considered for the path selection and the operation of the path selection is shown in Fig. 4.

Let us consider a WSN has 18 nodes; initially, it is clustered into two by applying k-means algorithm, so the cluster1 contains 7 nodes, and cluster2 contains 11 nodes. A node from cluster1 is considered as a source node and node in cluster2 is considered as destination shown in Fig. 4. First, the source node sends the information to its base node, and it forwards it to the corresponding base node, then the corresponding base node conveys the information to destination node through the trust-distrust procedure.

For sending the information from source to its base, it analyzes the trust-distrust value of its adjacent node, and the appropriate node is selected. The source nodes never send directly to its base unless it is in adjacent. Here the source node checks the trust-distrust value of adjacent, where two nodes are adjacent to the source among them one have distrust value and another has trust value, so the trusted node is selected. Base node is adjacent to the selected node, so it directly sends the information to the base.

After receiving the information by the based node, it analyses the destination address, which whether the destination is also present in its group otherwise it transmits the information to the adjacent base nodes,

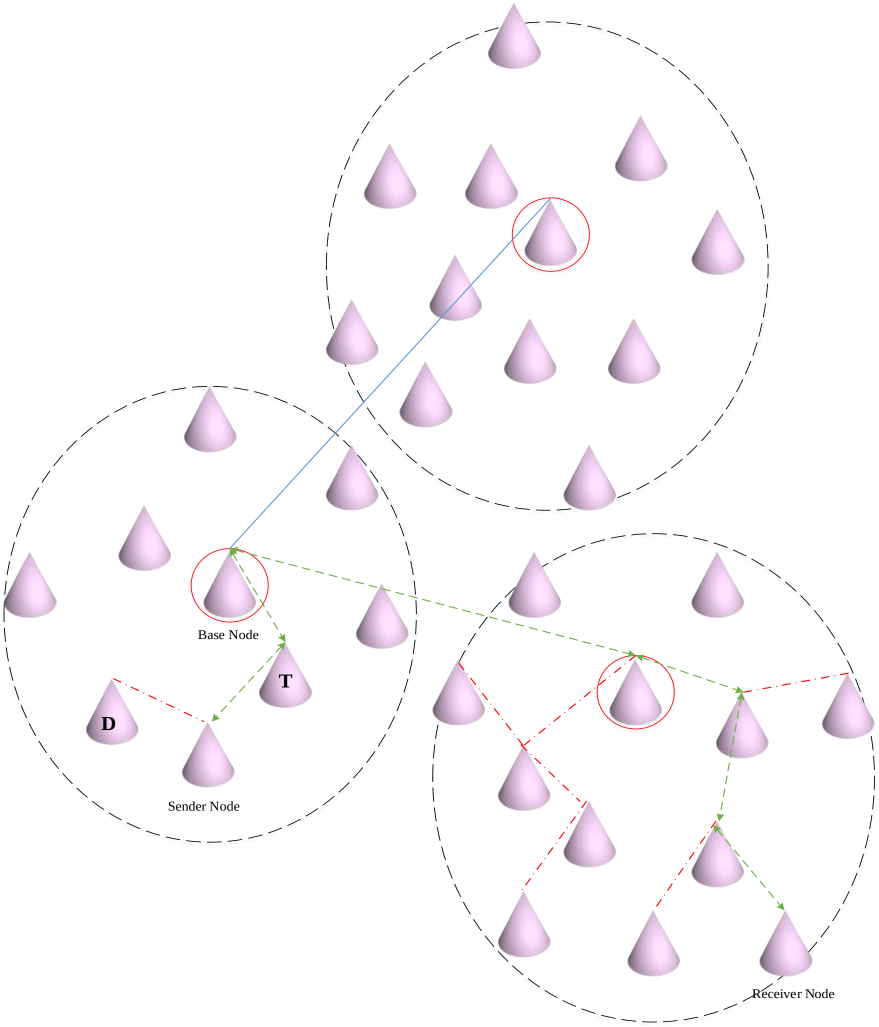

Figure.4 Path selection

Header
Information
Trailer

Figure.5 Packet format

then the process is repeated to reach the destination in cluster2 as given in Fig. 4.

In Fig. 4, the operation of path selection is displayed. In the figure, the conical shape represents the sensor nodes. Large circle represents the portion of a cluster, and a red circled cone represented as the base node (centroid) of the cluster. Red color link denoted the rejected path, and green dotted line representing the selected link for the routing. The packet format is shown in Fig. 5.

The Header and Trailer are in fixed size having the sender and destination address. The nodes in the WSN receive the packet and check whether the destination address is same as its address otherwise the node transmits the packet to its base node.

The base node checks whether the destination node exists in its group otherwise transmit it to the other group. While selecting the path based on the trust-distrust values the loss can minimize by preventing from the DoS attacks. Moreover, the path is in short range so the continuity can maintain for a long time than the usual WSN. Hence form this overall system the proper routing can achieve in WSN, by enhancing the security and reducing the loss.

4. Implementation results and discussion

The proposed TDP for the secure routing in WSN has implemented in the working platform of NS2. Table I gives the simulation parameter.

In our work 250 nodes are placed in WSN. Then the deployment area is covered by six clusters. Initially, cluster heads are selected to form a cluster within the transmission area. In Fig. 6, the marked area represents the cluster head, and six clusters are formed.

Table 1. Simulation Parameters

Parameter	Values
Number of nodes	250
Area(deployment)	300*300 m^2
Initial energy	1 Joules
MAC Type	IEEE 802.11
Data packet size	1024 bits/ sec
Transmitted power	0.02 watts
Received power	0.01 watts
Frequency range	5 GHZ
Transmission range	120m

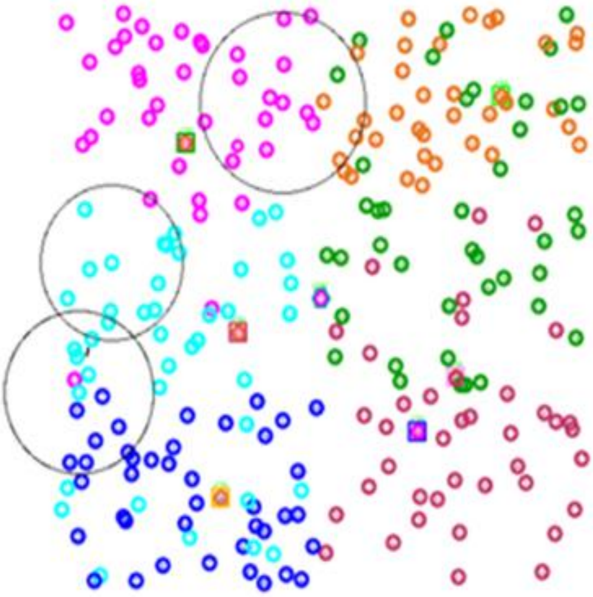

Figure.6 Node placement in WSN

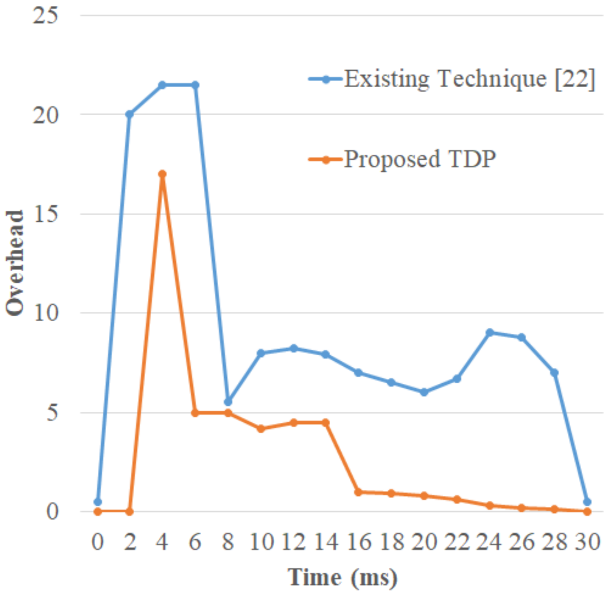

Figure.7 Overhead analysis

The computed quantitative relation between the amount of management and also the number of transmitted packets is termed as overhead analysis and is shown in Fig. 7.

As the sensor nodes are tiny with small battery backup, it is essential to ensure its overhead while routing. In a better network, the overhead should be in minimum so that the network lifetime can be maintained. Hence the overhead of our proposed protocol is analysed and is compared with the existing technique. From the overhead analysis, the overhead of the proposed work is better than the existing technique.

The time taken to route a packet from sender to receiver is denoted as the delay. The delay comparison is shown in Fig. 8. The rate at which the whole data get transmitted and received by corresponding nodes is called as throughput, the comparison based on throughput is shown in Fig. 9.

The amount of information loss, while routing is termed as packet loss ratio, the loss of packet should be minimum in a system. The comparison based on packet loss is shown in Fig. 10. The total energy required to complete communication is denoted as energy consumption, the comparison chart based on energy consumption is shown in Fig. 11.

In this performance analysis, we have observed that the proposed system has reduced overhead, delay, packet loss and energy consumption which are shown in Figs. 7, 8, 10 and 11, respectively. On the other head, the proposed system has improved throughput which is shown in Fig. 9.

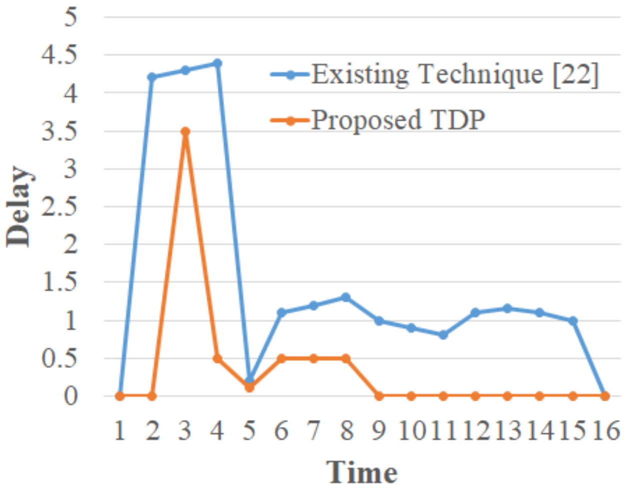

Figure.8 Delay analysis

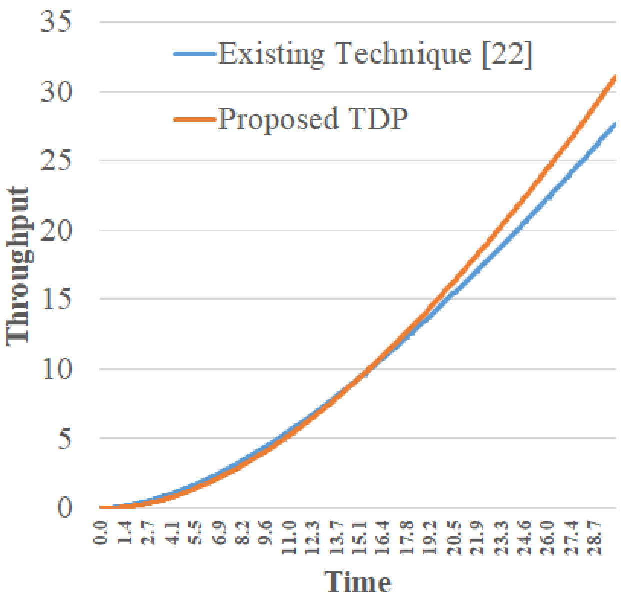

Figure.9 Throughput analysis

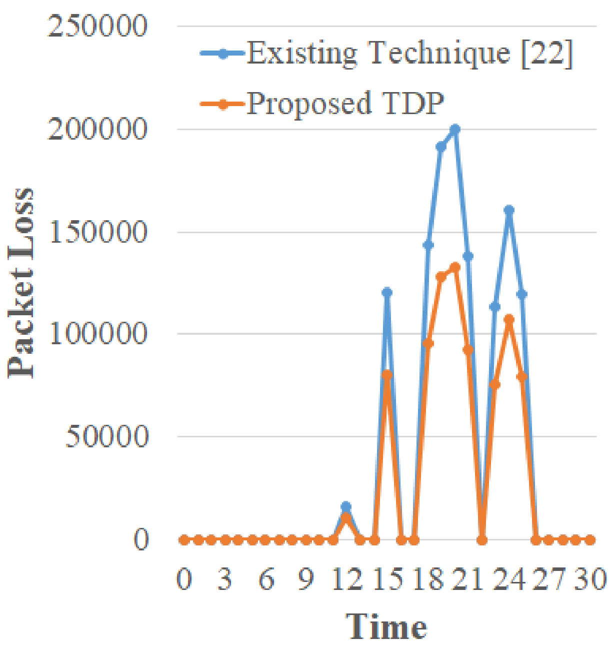

Figure.10 Packet loss analysis

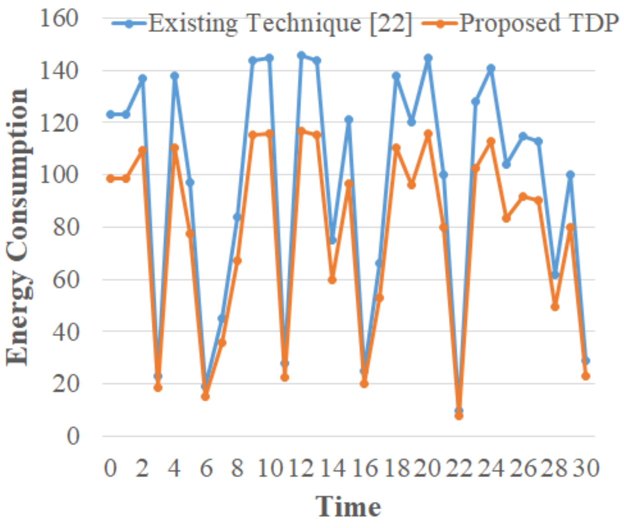

Figure.11 Energy consumption analysis

5. Conclusion

In every network system, security of information is the most concentrated issue, in case of WSNs, it is a challenging task. The security of the WSN can be achieved by proper routing. Hence in this paper a novel routing protocol is proposed named as Trust Distrust Protocol. In the proposed protocol initially, the topology management is done by using an improved k-means algorithm. Then the fitness of every node is calculated by sending and receiving a set of sample packets (or hello packet), the ratio of receiving to transmitting is denoted as trust ability or the fitness of a node. Based on this fitness a grade for every node is defined, it is similar to the ranking of nodes in the range of five. At last the best suitable path for transmission is selected based on the grade of the node. The proposed system for the routing in WSN has implemented in NS2, and the comparison is made with the existing technique ref [22]. The proposed protocol is evaluated based on the Overhead, Delay, Throughput, Packet loss and Energy consumption analysis. The results show that the proposed TDP provides better results than the existing technique. Hence from the performance comparison, I proved that the proposed system has improved average success ratio and reduced energy consumption. Hence it proves that the security of the proposed system is achieved by this enhance success ratio. Ultimately the performance analysis proves that the proposed protocol becomes one of the best choices for routing in WSN with high security and reduced energy consumption. In future work instead of cluster-based routing, an agent-based system can be proposed for further improvement in WSN routing.

References

[1] A. Wood, J.A. Stankovic, G. Virone, L. Selavo, Z. He, Q. Cao, T. Doan, Y. Wu, L. Fang, and R. Stoleru, "Context-aware wireless sensor networks for assisted living and residential monitoring", *IEEE Network*, Vol.22, No.4, pp.26-33, 2008.

[2] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: attacks and countermeasures", *Ad Hoc Networks*, Vol.1, No.3, pp.293-315, 2003.

[3] K. Akkaya and M. Younis, "An energy-aware QoS routing protocol for wireless sensor networks", In: *Proc. of 23rd International Conference on Distributed Computing Systems Workshops*, Providence, Rhode Island, USA, pp.710-715, 2003.

[4] L. Doherty, K.S.J. Pister, and L. El Ghaoui, "Convex position estimation in wireless sensor networks", In: *Proc. of IEEE INFOCOM 2001, Twentieth Annual Joint Conference of the IEEE Computer and Communications Societies*, Anchorage, AK, USA, pp.1655-1663, 2001.

[5] I. Stojmenovic, "Position-based routing in ad hoc networks", *IEEE Communications Magazine*, Vol.40, No.7, pp.128-134, 2002.

[6] K. Akkaya and M. Younis, "A survey on routing protocols for wireless sensor networks", *Ad Hoc Networks*, Vol.3, No.3, pp.325-349, 2005.

[7] W. R. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "Energy efficient communication protocol for wireless microsensor networks", In: *Proc. of the 33rd Annual Hawaii International Conference on System Sciences*, Maui, HI, USA, pp.1-10, 2000.

[8] M. Chen, T. Kwon, and Y. Choi, "Energy-efficient differentiated directed diffusion (EDDD) in wireless sensor networks", *Computer Communication*, Vol.29, No.2, pp.231-245, 2005.

[9] M. Younis and K. Akkaya, "Strategies and techniques for node placement in wireless sensor networks: A survey", *Ad Hoc Networks*, Vol.6, No.4, pp.621-655, 2008.

[10] G.S. Brar, S. Rani, V. Chopra, R. Malhotra, H. Song, and S.H. Ahmed, "Energy Efficient Direction-Based PDORP Routing Protocol for WSN", *IEEE Access*, Vol.4, No.1, pp.3182-3194, 2016.

[11] X. Wang, H. Cheng, and Y. Yao, "Addressing-based routing optimization for 6LoWPAN WSN in vehicular scenario", *IEEE Sensors Journal*, Vol.16, No.10, pp.3939-3947, 2016.

[12] J. Ren, Y. Zhang, K. Zhang, A. Liu, J. Chen, and X. S. Shen, "Lifetime and energy hole evolution analysis in data-gathering wireless sensor networks", *IEEE Transactions on Industrial Informatics*, Vol.12, No.2, pp.788-800, 2016.

[13] J. Luo, J. Hu, D. Wu, and R. Li, "Opportunistic routing algorithm for relay node selection in wireless sensor networks", *IEEE Transactions on Industrial Informatics*, Vol.11, No.1, pp.112-121, 2015.

[14] T.T. Huynh, A.V. Dinh-Duc, and C.H. Tran, "Delay-constrained energy-efficient cluster-based multi-hop routing in wireless sensor networks", *Journal of Communications and Networks*, Vol.18, No.4, pp.580-588, 2016.

[15] V.G. Jebaseelan and A. Srinivasan, "ArcRectZone: A Lightweight Curved Rectangle Vector Based Secure Routing for Mobile Ad-Hoc Sensor Network", *International Journal of Intelligent Engineering and Systems*, Vol.10, No.6, pp.116-124, 2017.

[16] S. Nallusamy, S. Appavupillai, and S. Ponnusamy, "Mobile Agents based Reliable and Energy Efficient Routing Protocol for MANET", *International Journal of Intelligent Engineering and Systems*, Vol.9, No.3, pp.110-116, 2016.

[17] S. Sennan and S. Palanisamy, "Composite Metric Based Energy Efficient Routing Protocol for Internet of Things", *International Journal of Intelligent Engineering and Systems*, Vol.10, No.5, pp.278-286, 2017.

[18] P.K. Reddy and R. Babu, "An Evolutionary Secure Energy Efficient Routing Protocol in Internet of Things", *International Journal of*

Intelligent Engineering and Systems, Vol.10, No.3, pp.337-346, 2017.

[19] B. Rajkumar and G. Narsimha, “Secure Light Weight Encryption Protocol for MANET”, *International Journal of Intelligent Engineering and Systems*, Vol.10, No.3, pp.58-65, 2017.

[20] N. Hiremani and T.G. Basavaraju, “An Efficient Routing Protocol Adopting Enhanced Cluster Formation Technique Accompanied by Fuzzy Logic for Maximizing Lifetime of WSN”, *International Journal of Intelligent Engineering and Systems*, Vol.9, No.4, pp.185-194, 2016.

[21] S. Jothi and M. Chandrasekaran, “Cluster Based Compressed Data Aggregation and Routing in WSN”, *International Journal of Intelligent Engineering and Systems*, Vol.9, No.4, pp.69-78, 2016.

[22] H.H. Liu, J.J. Su, and C.F. Chou, “On Energy-Efficient Straight-Line Routing Protocol for Wireless Sensor Networks”, *IEEE Systems Journal*, Vol.11, No.4, pp.2374-2382, 2017.