Cluster Based Context Aware Secure Routing in Distributed Sensor Networks

[1]Shivanand B Lamani, [2]Ravikumar K, [3] Arshi Jamal

Assistant Professor
Computer Science Department
[1]Akkamahadevi Women's University, Vijayapur, India
[2]GFGC, Gangavati, India
[3]GFGC, Sindhanur, India

Abstract: **Distributed Sensor Network (DSN) built with smart sensor nodes by high computing network. A DSN has been attractive platform for researchers from many years and it's to provide effective computing and making secure communication or routing between source and sink node. However, sensor networks are vulnerable in an environment with respect to attacks. The proposed system presents a context aware secure routing mechanism in DSN by using cluster approach. This approach incorporates efficient cluster head selections, context discovery, context interpretation, and secure routing mechanisms in DSNs. This paper proposes a cluster based context ware secure routing in DSN by employing Grid Based cluster approach. The objective of the proposed work is to improve the effective performance of networks. The proposed work had been simulated in terms of packet delivery ratio, network lifetime, energy consumption, throughput, and packet dropping ratio.**

Index Terms – DSN, Distributed networks, clusters, Sink node, CSRP Protocol.

I. Introduction

This chapter introduces briefly about distributed sensor network, traditional approach of data collection, DSN approach for data collection, general architecture of sensor node, challenges in Distributed Sensor Network, different aspects to overcome DSN challenges, application of DSNs, benefits and limitation of DSN, problem definition, proposed work, and organization of project.

1.1 Distributed Sensor Network

Smart environment will be the accompanying transformative progression wander in building, utilities, military, shopping centre, present day home, shipboard and transportation structures mechanization. Sensor data is gathered from various sensors of various modalities in disseminated areas. This data can be used to make smarter environment [1]. Be that as it may, to accomplish these difficulties will be huge like distinguishing the pertinent values, watching and collecting the information, review and check the data, formulating significant client data and doing decision-making, underneath Fig. 1.1 demonstrates the Scenario of distributed sensor network environment, where sensor can be deployed for smarter computing

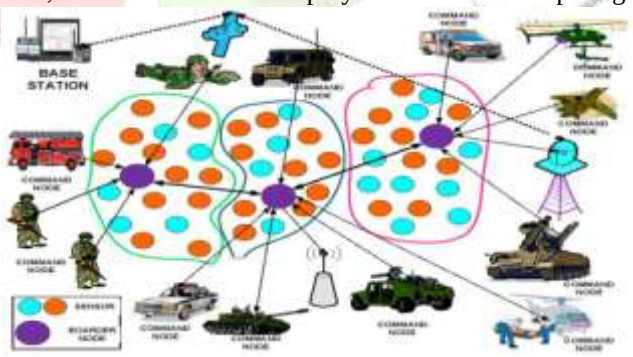

Fig. 1.1 Different Applications of Distributed Sensor Networks.

Fig. 1.2 demonstrates the case of how information is accumulated from the DSN comprises of number of sensors that are interrelated by a communicating network. Sensors are extremely implanted devices, which are coordinated with a substantial environment and fit for gaining signal, processing the signals, conveying and performing basic computing undertakings.

Fig 1.2 Data Collection in DSN.

While this new class of network can possibly empower extensive variety of applications, it likewise postures genuine difficulties like regular network topology transform, restricted operation, memory and power supply, chance of failure is more inclined with respect to the sensors. With every one of these limitations a productive and powerful strategy to extort information from the network is difficult job. Fig. 1.3 demonstrates the case of sensor node [2].

Fig 1.3 Example of Sensor Node.

1.1.1 Traditional data Collection Approach

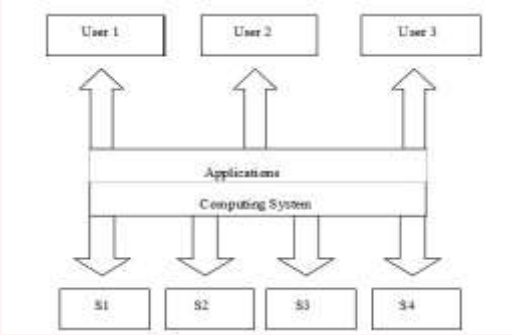

Figure 1.4 Traditional Data Collection Approach.

In conventional approach the information from accumulation of sensors are assembled by associating the sensors to interface cards in a manipulate framework. The information is exhibited to application in reasonable arrangements, and applications show data that is combined from such information to clients [3]. Because of unified approach architecture in not fault tolerant as appeared in Fig. 1.4.

1.1.2 Distributed Sensor Approach

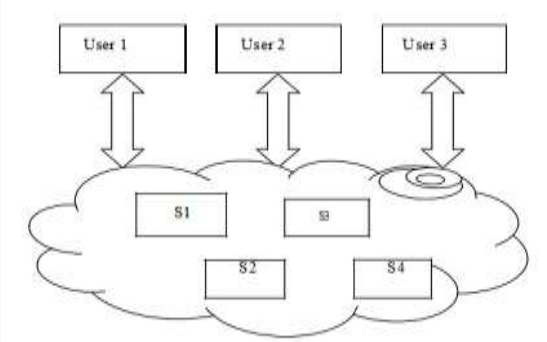

Fig.1.5. Distributed Sensor Approach.

In Distributed Sensor Approach, sensors are arranged through wired or remote media. There is no focal PC that plays out the synchronization assignments. The network itself is PC, and client interfaces with this network straightforwardly, potentially in intelligent or positive ideal models. The information assembled by different sensors is incorporated to integrate new data utilizing information fusion methods as appeared in the Figure 1.5.

1.1.3 Architecture of DSN

Architecture of DSN Figure 1.6 demonstrates the block diagram of Distributed Sensor network architecture, outlines the diverse segments in a sensor node from functionality perspective. An authoritative goal of DSNs is to settle on decisiveness or pick up realization in perspective of the information combined from distributed sensors. A basic data handling can be conveyed then be incorporated/intertwined at an upper preparing focus to decide realization and help deciding. A general DSN contains game plans of sensor nodes, a course of action of processing elements (PEs), and a conveying network interrelate the diverse PE's. No less than one sensor is connected with each PE. One sensor can report the more than one PE.

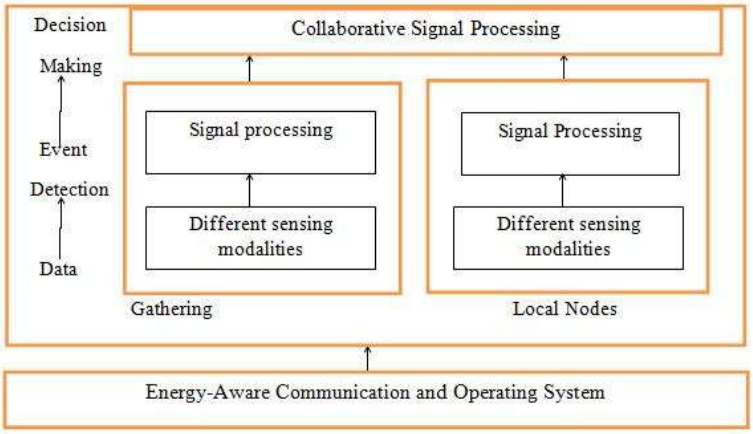

Fig. 1.6 Functional Architecture of DSN.

Fig. 1.6 functional Architecture of DSN Data's are exchanged from sensor to their related PE(s), where the data integration happens. PEs can likewise coordinate with each other to accomplish a superior estimation of the environment and report to more elevated level PEs [4].

II. Proposed Work

The proposed model works with the efficient construction of clusters and CH selection using context awareness in the network. Context Aware Secured Routing Protocol (CSRP) had been simulated more successfully in DSNs. CSRP comes up with; the architecture, how the formation of cluster is done, context discovery, context interpretation, and secure routing are presented.

2.1 System Architecture

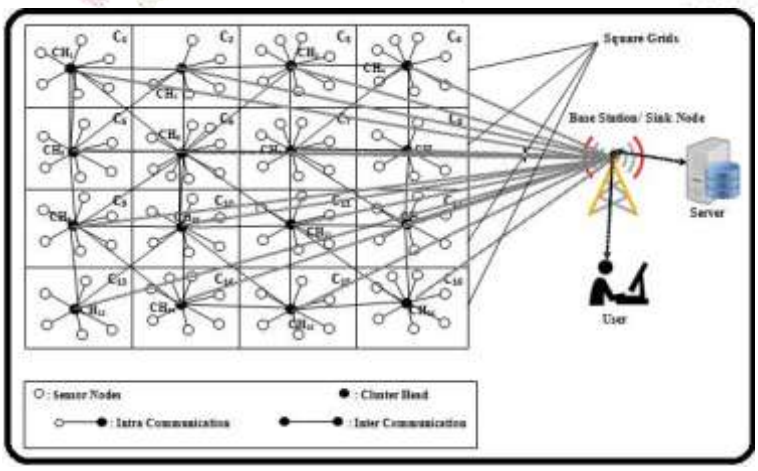

Fig. 2.1. System Architecture.

The proposed architecture has collection of intellectual SN_S with high speed network as shown in fig. 2.1. In real time environment, SN_S are disposed arbitrarily. All these SN_S are equipped with GPS configuration. The proposed system architecture associates with the following components viz., intelligent sensor nodes, CHs, and sink node or base station. Every node in the network come up with initial amount of energy and network bandwidth, all sensor nodes are assumed to static in the network, and used to compute the efficient path over the CHs. Here in sensor network it can be seen two different sorts of communications and those are communication in intra-cluster and communication in inter-cluster. Communication takes place between CM node and its own CH, this is called as intra-cluster communication. The communication happened in the middle CHs and sink node is named as inter-cluster communication.

Every node senses the information from time to time, forwards it's information to the CHs. CHs gathers the encrypted information from all CM_S inside cluster, aggregates all data to remove the redundant information. CH transmits aggregated information to the sink node over the CHs. At long last, sink node makes the move after receiving data from SN_s. As it can be observed in the sensor network, all CHs are periodically monitoring the status of the respective cluster. Periodically, all CHs receive the HEARTBEAT messages from the cluster member nodes because of authentication of nodes. If CH does not receive the HEARTBEAT message, it assumes that node is malicious or dead node or attacked by someone else in the clusters. Sink node also receive the HEARTBEAT message from its CHs in the network due to authentication. Each CH node maintains the CM Knowledge Base (CMKB) as shown in fig. 3.2 for authentication of node in each clusters of the network. CMKB is read and updated by the sensor nodes or CHs. CMKB associates the following parameters are: cluster member identifier (CM_{id}), CH_{id} , node status (i.e., Active or Sleep), node energy, context data types or priority levels of data, signal strength, locations, and etc.

CM_ID	CH_ID	Status	N_E	B_T_r	Context_Level	C_n	SS	Location
{2,4,6,9,5}	CH_1	Active/Sleep	≥0.57	≥10%	Boolean Values{True or False}	C_{c1}	≥10%	(3,9)
{1,7,8,9,11}	CH_2	Active/Sleep	≥0.57	≥10%	Boolean Values{True or False}	C_{c2}	≥10%	(2,6)
{12,13,15,17,18}	CH_3	Active/Sleep	≥0.57	≥10%	Boolean Values{True or False}	C_{c3}	≥10%	(4,5)
{23,25,26,27,29,30}	CH_4	Active/Sleep	≥0.57	≥10%	Boolean Values{True or False}	C_{c4}	≥10%	(1,8)
{31,34,36,37,38,39}	CH_5	Active/Sleep	≥0.57	≥10%	Boolean Values{True or False}	C_{c5}	≥10%	(7,2)
—	—	—	—	—	———	—	—	—
—	—	—	—	—	——	—	—	—
—	—	—	—	—	——	—	—	—
—	—	—	—	—	——	—	—	—

CM_ID: Cluster Member ID — CH_ID: Cluster Head ID — N_E: Node Energy in Joules
B_T_r: Bandwidth Required to Transmit in MBPS — C_n: Number of Clusters — SS: Signal Strength

Fig.2.2.Cluster Member Knowledge Base.

The sink node also maintains the Cluster Knowledge Base (CKB) as shown in fig. 3.3 for authentications of nodes in the network. CKB comprises the set of parameters like: CH identifier, CH status, cluster bandwidth, CH energy, location of CHs, number of neighbour nodes from each CHs, number of possible paths form each CHs, number of hop counts from CHs to sink node, and key value(private key). This knowledge base is read and updated by the sink node or CHs in the network.

C_ID	Status	C_E	B_Tr	C_Type	Location	N_N	N_P	N_H	Key Value (32_bit)
C1	Active	≥0.10J	≥10%	Emergency or Non Emergency	(8,12)	5	2	3	CMC1EBSH_C
C3	Active	≥0.10J	≥10%	Emergency or Non Emergency	(4,9)	3	4	4	CMC3EBSH_C
C4	Active	≥0.10J	≥10%	Emergency or Non Emergency	(12,9)	4	6	5	CMC4EBSH_C
C8	Active	≥0.10J	≥10%	Emergency or Non Emergency	(6,10)	4	4	2	CMC8EBSH_C
C10	Active	≥0.10J	≥10%	Emergency or Non Emergency	(5,2)	2	3	3	CMC10EBSH_C
C15	Active	≥0.10J	≥10%	Emergency or Non Emergency	(8,9)	3	7	4	CMC15EBSH_C
——	—	—	——	——	—	——	——	—	—
——	—	—	—	—	—	—	—	—	—
—	—	—	—	—	—	—	—	—	—

C_ID: Cluster Identifier C_E: Cluster Energy B_T_r: Bandwidth Required for Transmission of data in MBPS C_Type: Content Type
N_N: Number of Neighbor nodes N_P: Number of possible paths N_H: Number of hop count from source to destination

Fig. 2.3.Cluster Knowledge Base.

2.2 Cluster Formation

In DSN, nodes are disposed arbitrarily in the network. Let's consider 'L' as the Length and 'B' as the Breadth of the square area of DSN correspondingly. The network is categorized into number of square grids by using Eq. (1), area of the cluster/grid size is definite by using Eq. (2).

Centre of the square grids = (L × B) / 2 (1)

Area of Grid Size = K / C_N (2)

2.3 Cluster Formation and CH Selection Algorithm

Step 1. Deploy the 'N' number of sensor nodes randomly.

Step 2. Categorize the network into number of Square Grids are as follows:

$N\_SG_i = L \times B / 2$ Є for every Grids (Gi)

Step 3. Selection of CH_i in each G_i is as follows:

for each cluster (C_N) do
for each sensor node(S_N) do
if (rand(CH_i) > E(S_N)) Є V_i
C_N (CH) = = CH_i;
else
C_N (CM_i) = = CH_i;
endif
endfor
endfor

2.4 Context Discovery

In the propped scheme, the context information is used to discover the context data in terms of node energy, node bandwidth, and Boolean data in each cluster of the network. Suppose CH forwards the packet or data to sink node in the network that must be satisfied the following condition:

$$CM_E \geq Th_E \;\&\&\; CM_B \geq Th_B \;\&\&\; Data=1 \quad (3)$$

When context is discovered in particular cluster member node its energy (CM_E) and its bandwidth (CM_B) is compared against the threshold level energy and bandwidth respectively. The proposed context discovery algorithm is as follows:

for each C_N do
for each CM_i do
if ($CM_E \geq Th_E$ && $CM_B \geq Th_B$ && Data=1)
Send the context data to respective CH_i ;
Else if($CM_E \leq Th_E$ && $CM_B \leq Th_B$)
Context Data (CM_i)== TRUE;
Else
Context Data (CM_i) == FALSE;
end if
end for
end for

2.5 Context Interpretation

In proposed scheme, context interpretation plays a major role. Context interpretation phase gathers information from all sensor nodes at CHs by the CM_i nodes in respective clusters of the network. Based on context information, CH_i interprets the data in-terms of priority levels or context types of data. Context interpretation factor 'λ' at CH_i is the union of all cluster member context data in each cluster. Let 'δ' be the cluster member context data in each cluster. The context interpretation model is defined as follows:

$$\lambda = \bigcup_{CM_i=1}^{N} \delta\,(CM_i) \in C_N$$

$$\delta\,(CM_i) = D(CM_1 \cup CM_2 \cup CM_3 \cup \text{----------} \cup CM_N) \in C_N$$

Each CH decides the following interpretation of data in-terms of emergency level of context or highest priority of data, less priority of data, non-emergency of level of data or low priority of data based on the value of 'λ'. The context interpretation scheme is proposed in the work is as follows:

for each C_N do
for each CM_i do
If (δ >1)
High Priority Data/Emergency Level of Context

elseif (δ = 1)
Next Priority Data/Next Emergency Level of Context
else
Low Priority Data/Non Emergency Level of Context
end if
end for
end for

2.6 Secured Routing

A CH_i finds all the possible paths from source to sink node through intermediate nodes (neighbour CHs) within the network. According to the value of the trust path, source CH generates the 32 bit key value (i.e., Private Key or Secret Key) for encryption. The value of private key is stored in its knowledge base. CH forwards the encrypted data to sink node through its best possible path (inter-communication). The best path could be shortest or efficient path in the network. Finally, sink node decrypted the data with its own private key. Sink node broadcast the beacon message for requesting all possible paths from its CH nodes, based on this, sink node generates the private key or secret key (32 bit key) for decryption of data. The value of private key is placed in its knowledge base.
The value of private or secret key is generated based on the parameters in both CH and sink node like: cluster member identifier, cluster head identifier, number of hop counts, and sink node identifier. However, if CH is nearest to sink node i.e, CHs with one hop separation from the sink, it means there is no need of intermediation so it can straightforwardly forward their information to the sink node. Before forwarding data, to sink node or CM_i to CH_i, Each CH_i ensures the trust value of CM_i and its neighbor CH_i nodes for authentication due to limited power, processing, and memory of sensor nodes that ensures the recent developments of data encryption and algorithms for data. In the proposed work, CH_i validates the CM_i data as well as checks correctness of messages from the neighbor CH_i in the network. The CH_i also evaluates the value of trust within the cluster is defined as follows:

$$TRUST(CH_i, CM_i) = \{(M_N(CH_i, CM_i)) \in (0, 1)\}$$

$$\begin{cases} (M_N(CH_i, CM_i)) = 1 & \{TRUST\} \\ (M_N(CH_i, CM_i)) = 0 & \{NON\text{-}TRUST\} \end{cases}$$

$M_N(CH_i, CM_i)$ is the validation result of N^{th} information that the node CH_i take delivery of information from the node CM_i depending upon the significance either 0 or 1. There are two parameters are to be considered for validating the data in the proposed scheme as follows: 1) Periodically CM_i node sends the HEARTBEAT messages to its respective CH_i in each cluster, and 2) If the trust value is more than the threshold level of cluster bandwidth in the network. If anyone fails in the cluster, CH_i assumed that node CM_i is not trustworthy or malicious node or dead node and the node CMi. is deleted from the cluster. Hence MN(CHi, CMi) is set to 0 otherwise 1.

A secured path from the source node (CH_i) to sink node is used to come up with N_CHi 'N'(no. of neighboring nodes) number of nodes trusted cluster heads. Therefore, the trust value of all possible paths from the CH_i to sink node is the product of the nodes trust value. The trust value of the trust path is given by:

$$TRUST\ PATH(CH_i, BS) = \prod_{CH_i, BS \in P} Trust(CH_i, N\_CH_i)$$

Where, Trust (CH_i, N_CH_i) is the trust path between CH and number of neighbor nodes (CH nodes) in the network.

III. Simulation

The given scheme had simulated in different network situations by utilizing 'C' programming language. Simulations are conducted broadly with arbitrary number for 100 iterations. This chapter shows the simulation model, procedure, performance parameters and results.

3.1 Simulation Model

The proposed method associates the set of sensors scattered arbitrarily. The proposed DSN split into number of grids to form the clusters. The performance parameters of the proposed are simulated effectively for achieving better network performance.

3.2 Simulation Procedure

Proposed simulation scheme associates the following variables: S_N = 500, E_N = 2Joules, N_s = 1, Size of the network = 1000*1000 meters, TR = 100 meters, E_S = 50nJ/Bit, E_T = 50nJ/Bit, P_i = 64Bits, 128Bits, 512Bits, 1024Bits and so on, and TH_E = 0.05 Joules, BN = 4mbps.

Begin

1) Dispose the number of nodes arbitrarily in DSN;
2) Divide network into numeral of clusters or square grids;
3) Select the number of CHs using proposed algorithm;
4) Apply the proposed scheme for secured routing;
5) calculate the performance parameters;
6) Plot the graphs;

End

3.3 Performance Parameters

The accompanying performance parameters were utilized in projected method:

1) *Packet Delivery Ratio (PDR):* It is characterized as the node's quantity increases, the PDR increases with respect to context interpretation factor (λ) in the DSN. It expresses in milliseconds (%).
2) *Network Lifetime:* As the rounds with respect to context interpretation factor (λ) increases, the life of network declines in DSN. It is articulated in percentage (%).
3) *Throughput:* It is the relation of numeral context packets sent and the numeral context packets received successfully with respect to trust path between CH_i and sink node. It is articulated in percentage (%).
4) *Energy Utilization/ Consumption:* As the percentage of context interpretation factor (λ) inclines with the nodes numeral, energy consumption of each node raises for sensing and transmitting of data in DSN. The increment of energy utilization of each SN is considered in mJoules. The calculation of energy utilization of each SN(CH and CM) in network is as follows:

$E = (E_S \times P_i + E_T \times P_i) \times D_i$

Where,

E_S – energy requisite for sensing packets,

E_T – energy necessary for transmission packets,

P_i – packets size in bits.

Let E is the value of energy consumed for the transmission of a bit per distance D_i.

5) *Dropping Rate:* It is defined as the percentage of trust path between sensor nodes or CHs and sink node increases with given active number nodes, the decrease in dropping rate of packets, that is the ratio of context packets or data dropped to packet sent through the trust paths is defined as follows:

$$\text{Dropping Rate(\%ge)} = \left(\frac{P_F - P_R}{TP_F} \right) \times 100$$

Where,

P_F = No. of data/packets forwarded, P_R = No. of data/packets received,

TP_F = Total no. of forwarded data/packets.

3.4 Results and Discussions

The fig. 3.1 depicts the packet delivery ratio (PDR) with numeral of active nodes in the networks. As the numeral of active nodes inclines, raise in the PDR gradually by the sensor nodes with respect to the value of context interpretation factor (λ) in the networks. The CHi associates with context interpretation model for delivering packet to sink node. The value of 'λ' ≥ 25%, ≥ 50%, and ≥ 75% are considered in this work. The proposed protocol CSRP achieves the better context interpretations by the sensor nodes for transmitting secured data efficiently.

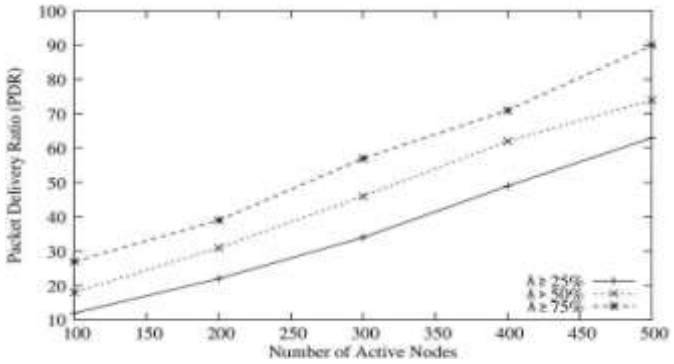

Fig.3.1.Packet Delivery Ratio (PDR) vs. Number of Active Nodes.

The fig. 3.2 depicts the network lifetime with known numeral of active nodes in DSNs. As the numeral of rounds increases, gradually decline in network lifetime of the network with respect to value of 'λ' because of more communication overhead or congestion between nodes. If the value of 'λ' increases, energy consumption increases among the sensor node with the rounds. SN_s interpreted less percentage of information in network; sensor nodes are uses to consume less amount of energy. The proposed protocol (CSRP) performs better network lifetime. In other protocols (LEACH, GAF, and PEGASIS), end to end delay, communication overhead, and number of dead nodes are high because of the arbitrary alternation of CHs in networks.

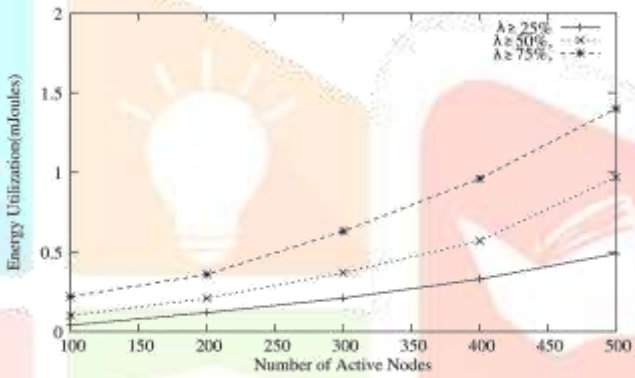

Fig.3.2. Network Lifetime vs. Number of Rounds.

The fig. 3.3 presents the energy utilization among the active sensor nodes in the DSNs. The increase the percentage of 'λ', energy consumption gradually increases among the sensor nodes. The proposed CSRP protocol utilizes or consumes less amount of energy for transmission of packets because proposed protocol CSRP depends on the value of 'λ' in the network, transmit the packet or data through only its trust paths. The some other protocols (like LEACH, PEGASIS, GAF, and so on) require more energy because of its more end to end delay for packet transmission, context interpretation, and clustering information.

The throughput of the network with numeral of active sensor node is shown in fig. 3.4. Generally, the numeral of active nodes increase, gradually increase in throughput of the network. The percentage of trust between CH and BS are increases, the number packets sent and receive successfully by the CH and BS respectively to achieve the better throughput of the network. The proposed CSRP protocol works on the basis of trustworthy paths between CH and BS.

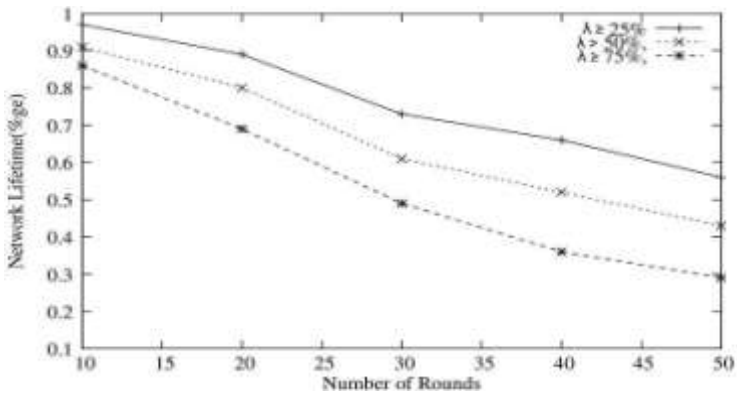

Fig.3.3 Energy Utilization vs. Number of Active Nodes.

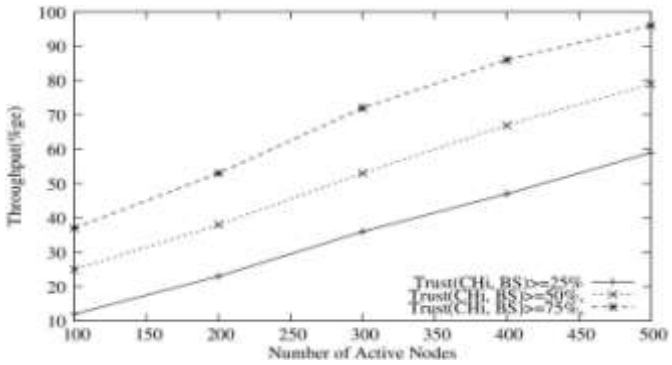

Fig.3.4.Throughput vs. Number of Active Nodes.

The fig.3.5 depicts the percentage of packet dropping with the percentage of trust path between SN and sink node in network. As the percentage of trust path increases with respect to the given variable size of the active nodes, the percentage of packet dropping ratio decreases due to some congestion and communication overhead in the network.

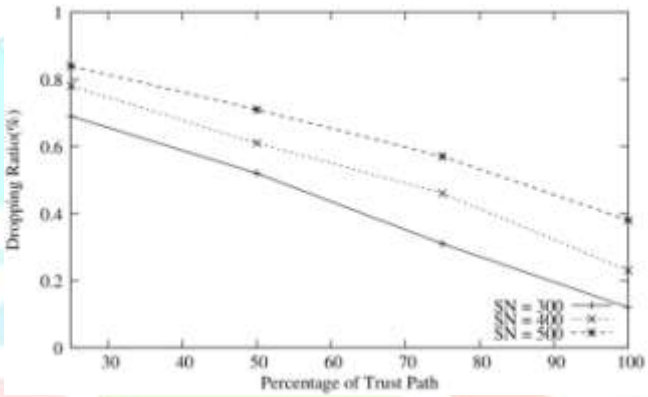

Fig.3.5. Dropping Rate vs. Percentage of Trust Path.

CONCLUSION

The proposed method is efficient with respect energy utilization and reactive to network. Detects the energy depletion of sensor nodes in each cluster, evaluates the trust path between CH nodes and sink node as well as trust cluster member nodes of each cluster in the network. The proposed model is simulated in terms of context aware efficient CHs selection in each cluster, the context could be residual energy and bandwidth, enhances the secured routing through trust paths across the CHs in the network that performs the better network lifetime. This work also measures the performance parameters using proposed CSRP protocol, which is robust and fast. Results of simulation are much expressive to tell that proposed system is more proficient than the approaches which don't have context awareness. CSRP protocol forwards the secured data from sensor nodes to sink nodes.

References

[1]: F. Akyildiz, W. Su, Y. Sankarasubramaniam and E. Cay irci, "Wireless Sensor Networks: A Survey"
[2]: B. Braden, D. Clark and S. Shenker, "Integrated Services in the Internet Architecture: An Overview"
[3]: E. Crawley, R. Nair, B. Rajagopalan and H.Sandick, "A Framework for QoS-based Routing in the Internet"
[4]: "Energy-Centric Enabling Technologies For Wireless Sensor Networks" Manish Bhardwaj, Seong-Hwan Cho, Nathan Ickes, Eugene Shih,
[5]:"A Dynamic Geographic Hash Table for Data-Centric Storage in Sensor Networks" Thang Nam Le, Wei Yu, Xiaole Bai and Dong Xuan.
[6]: C. Schurgers and M. B. Srivastava, "Energy Efficient Routing in Wireless Sensor Networks"
[7]: "A Fair Scheduling Algorithm with Traffic Classification for Wireless Networks"
You-Chiun Wang, Shiang-Rung Ye, and Yu-Chee Tseng.
[8]: H. Karl and A. Willig, "A short survey of wireless sensor networks"
[9]: "Issues in Designing Middleware for Wireless Sensor Networks", Yang Yu, Bhaskar Krishnamachari, and Viktor K. Prasanna
[10]: "Quality of Service in Wireless Sensor Networks", Hwee-Xian TAN
[11] Data Aggregation in Wireless Sensor Network Nandini. S. Patil, Prof. P. R. Patil.
[12] The Impact of Data Aggregation in Wireless Sensor Networks_ Bhaskar Krishnamachari Deborah Estrin, Stephen Wicker
[13] Robust Node Localization for Wireless Sensor Networks Radu Stoleru , John A. Stankovic Sang Son

[14] Multiple Sink Based Compressive Data Aggregation Technique For Wireless Sensor Network, Mohamed Yacoab M.Y.
[15] Controlled Mobility for Sustainable Wireless Sensor Networks Aman Kansal, Mohammad Rahimi, Deborah Estrin, William J Kaiser, Gregory J Pottie, and Mani B Srivastava University of California, Los Angeles.
[16] Node Localization In Wireless Sensor Networks P.K Singh, Bharat Tripathi, Narendra Pal Singh
[17] D. Ganesan, A. Cerpa, W. Ye, Y. Yu, J. Zhao and D. Estrin, Networking Issues in Wireless Sensor Networks, Journal of Parallel and Distributed Computing (JPDC), Special Issue on Frontiers in Distributed Sensor Networks, Elsevier Publishers, Dec 2003.
[18] S. Ratnasamy, B. Karp, L. Yin, F. Yu, D. Estrin, R. Govindan and S. Shenker, GHT: A Geographic Hash Table for Data-Centric Storage, Proceedings of the ACM Workshop on Sensor Networks and Applications, Atlanta, Georgia, USA, Sep 2002.
[19] F. Bauer and A. Varma. "Distributed algorithms for multicast path setup in data networks," in Transactions on Networking, vol. 4, no. 2, 181-191, 1996.
[20] B. Cain, T. Speakman, D. Towsley, "Generic Router Assist (GRA) Building Block Motivation and Architecture," RMT Working Group, Internet-Draft <draft-ietf-rmt-gra-arch-01.txt>, work in progress, March 2000.