Cryptographic Data Security for Reliable Wireless Sensor Networks

Ravi Kant1, Dr. Varsha Namdeo2, Dr. Dinesh Kumar Sahu3

1, 2, 3 Dept. of Computer Science Engineering
1, 2, 3 RKDF Institute of Science & technology, Hoshangabad Road, Bhopal, Madhya Pradesh

ABSTRACT

Wireless sensor network is extensively used technology now a day in real time application. It consists of a number of autonomous sensor nodes which are organized in various areas of interest to accumulate data and jointly convey that data back to a base station. But the sensor node has limited battery energy and it is also found that the WSN more vulnerable to severe kinds of security threats such as denial of service (DOS), Sybil, hello flood attack etc. In this, we proposed group communication using election algorithm to make the network most energy efficient and also make the network secure. The simulation of the proposed methodology is done between different network parameter such as PDR, end-to-end delay, throughput and energy consumption using the network simulator NS-2.34.

Keywords:- *Battery, PDR, Security, Threats, Throughput, Wireless sensor network*

1. INTRODUCTION

Wireless sensor network (WSN) is extensively used technologies of the innovative area. The sensing electronics extents the ambient conditions associated to the environment nearby the sensors and renovate them in to an electrical signal. In various applications, the distribution of sensor nodes is performed in an ad-hoc manner without cautious planning and engineering. In the last few years, rigorous exploration studies addressing the prospective of association among sensors in data gathering and handling and in the coordination and administration of the sensing accomplishments were conducted. Nonetheless, the sensor nodes are self-conscious in energy supply and bandwidth. The quick deployment, self-organization and fault tolerance characteristics of wireless sensor networks make them a very promising sensing technique for military, environmental, scientific and health applications [1]. Energy conservation is serious in WSNs. Replacing or recharging the batteries is not an option for the sensors deployed in hostile environments. Usually, the communication electronics in the sensor use most of the energy. Immovability is one of the major anxieties accompanying with the progression of WSNs [2]. A number of WSN applications necessitate definite sensing, coverage, and connectivity all over its operating time duration. The death of the first node might cause unpredictability in the network. Consequently, all of the sensor nodes in the network must be active in order to accomplish the goal during that period. One of the main obstacles to confirm these marvels is the unbalanced energy ingestion rate. Numerous techniques have been proposed to decrease the energy consumption rate, likewise clustering, proficient routing, and data accumulation.

In a classic WSN application, sensor nodes are distributed in a province from where they collect data to accomplish definite goals. Data assortment may be an event-based process. The WSN must be very steady in some of its applications such as security monitoring and motion tracking. The death of only one sensor node may agitate the coverage or connectivity and hence may weaken the immovability in this type of applications. Therefore, all of the organized sensor nodes in the WSN must be vigorous during their operational lifetime. Nevertheless, the sensor nodes are usually equipped with one-time batteries and most of the batteries are of low-energy type. Due to this intended, each sensor node must proficiently use its available energy in order to get better the lifetime of the WSN. Different techniques are used for the resourceful handling of this low obtainable energy in a sensor node. Group communication and election algorithm is one of the well known techniques.

In Section II discuss related work for decreasing the energy consumption. The Section III discusses about the different routing techniques. Section IV describes the proposed methodology and last section presents conclusion the paper.

2. RELATED WORK

Several techniques has been proposed or implemented to enhance the network lifetime and to form a secure network. In this section we discuss different methods proposed and implemented by various researchers in field of energy consumption and related to security threats over the network. **Luigi Coppolino et al [3]** proposed a hybrid, lightweight, distributed Intrusion Detection System (IDS) for wireless sensor networks. This IDS uses both misuse-based and anomaly-based detection techniques. It is composed of a Central Agent, which performs highly accurate intrusion detection by using data mining techniques, and a number of Local Agents running lighter anomaly-based detection techniques on the motes. Decision trees have been adopted as classification algorithm in the detection process of the Central Agent and their behavior has been analyzed in selected attacks scenarios. The accuracy of the proposed IDS has been measured and validated through an extensive experimental campaign.

K. Parameswari et al [4] proposed to develop an energy efficient secured data aggregation protocol for wireless sensor networks, which will alleviate the node misbehavior in thewireless sensor networks. The protocol involves mechanism for energy efficient aggregator selection. Mechanism for efficient node selection for reducing the network lifetime and the delay. Source node authentication by the sink. Aggregate or authentication as per listed in the packet header, by the sink. This protocol can be constructed on top of the preexisting key distribution and encryption schemes in the wireless sensor networks. **Roshan Zameer et al [5]** proposed a mechanism to provide security with a reactive security scheme that includes studying the behavioral aspect of attacks and congregating the security demands. This method in sequence conglomerates the security and the network rescue mechanism free from attacks and their impacts on the network. The simulation results such as Packet Delivery Ratio (PDR), malicious node movement, delay; transmission power illustrates various attack behaviors in WSN along with the reception power rate observed by the sink node and the Packet loss. **Sudharsan Omprakash [6]** proposed, a Secured Energy Efficient Clustering and Data Aggregation – [SEECDA] protocol for the diverse WSN, in which the security, energy proficient clustering, data aggregation are pooled to accomplish a best performance in terms of QOS by energy and security measures. The proposed approaches incorporate a security method, and an innovative cluster head election mechanism and the route will be chosen with less energy needed. The simulation result shows that the SEECDA balances the security, energy effectiveness and extends the network life time are high when compared to LEACH, EEHCA and EDGA, EECDA respectively. **Malika BELKADI et al [7]** presented the Secured Directed Diffusion routing protocol and regarding to the different types of transmissions in this protocol, it use three types of keys. These keys are: the individual key of a node u (IKu), which is used to secure communication between a node and the base station, the pair-wise key (Kpair) to secure communication between a node and one of its neighbors and finally the global key (BK), all the nodes in the sensor network share this key with the base station. The base station uses global key to encrypt the interest message and all the nodes in the network uses this key to decrypt the announcements from the base station. The nodes store the interest information in their interest cache and then encrypt the message using the global key to further broadcasting it. The communication cost is reduced by using this key. With the help of these keys they reduce the power consumption of nodes, so the lifetime of the network will be extended. **Babaket al [8]** proposed an algorithm which makes healthier use of energy and bandwidth which are two restrictions in wireless sensor networks. In the algorithm mobile agent is used to cluster the network and also create the tour to attain collected data from each cluster-head and deliverit back to the sink node. With suitable parameters set, simulation shows that the proposed algorithm exhibits better performance than original direct diffusion in terms of energy consumption [9].

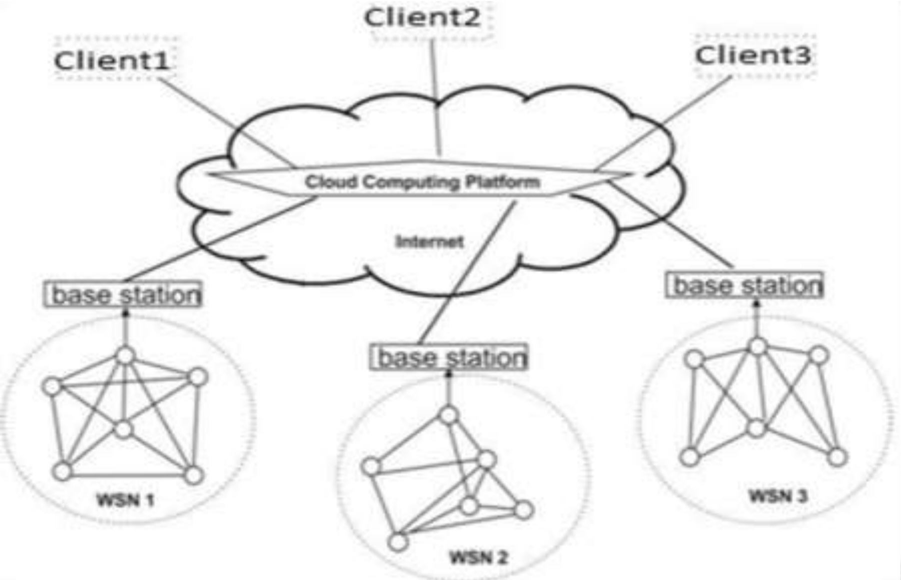


Fig. 1 Wireless Sensor Networks

Di Tang [10] proposed new secure and efficient cost-aware secure routing protocol to deal with these two conflicting issues through two modifiable parameters: energy balance control (EBC) and probabilistic-based random walking. They determine that the energy consumption is rigorously disproportional to the consistent energy exploitation for the given network topology, which significantly reduces the lifetime of the sensor networks. To resolve this problem, they also proposed well-organized non-uniform energy exploitation strategy to optimize the lifetime and message delivery ratio under the same energy resource and security prerequisite. We also provide a quantitative security analysis on the proposed routing protocol.

3. OVERVIEW OF ROUTING TECHNIQUES

The efficiency of energy can be improved using some algorithms. That route the data as per network and data communication systems. In this we will some of the energy efficient routing protocols which will be discussed which are LEACH (Low Energy Adaptive Clustering Hierarchy), PEGASIS (Power Efficient Gathering in Sensor Info. Systems) and TEEN (Threshold Sensitive Energy Efficient Sensor Network), HEED (hybrid energy-efficient distributed clustering method for ad hoc sensor networks) etc.

LEACH

The function field of sensor network is the environment surveillance and location tracing. In such situation, the end user does not require any frequent data as each node of the data is not associated to each other. The responsibility of LEACH (low energy adaptive clustering hierarchy) is to merge ordinary date by cluster head and sent to sink. For that cause, any frequent data is not sent to the sink [11].

The LEACH postulations are as follows.

(i). Every node has adequate energy to send data to the sink and can manage transmission energy.

(ii). Every node has data to send at any time and close nodes have data associated with each other.

The key objective of routing protocol for routing is transferring data from convey node to object node and finding the most appropriate path with exactness. Accordingly, with limited shared resources, energy disbursement needs to be optimized on transmission bandwidth in the network overhead or surrounded by the nodes. For this motive, the sensor network circumvents replica of data among the adjoining sensor nodes by clustering simplify routing and energy expenditure can be supervised proficiently.

PEGASIS

The power-efficient gathering in sensor information systems [12] is a voracious chain-based power efficient algorithm. In addition, PEGASIS is based on LEACH. The key characteristics of PEGASIS are:

- The Base Station is preset at long distances from the sensor nodes.
- The sensor nodes are identical and energy constrained with consistent energy.
- No mobility of sensor nodes.

PEGASIS is based on two ideas that are chaining and data fusion. In PEGASIS every node can take twirl of being a leader of the chain where the chain can be created using greedy algorithms that are organized by the sensor nodes. PEGASIS presupposes that sensor nodes have a global understanding of the network nodes are motionless (no alliance of sensor nodes) and nodes have locality of information about all other nodes. PEGASIS performs data fusion excluding the end nodes in the chain. PEGASIS better than LEACH by removing the transparency of cluster formation decreases the sum of distances that non leader node have to broadcast less the number of transmissions and receives all nodes and use only one transmission to the BS per round. PEGASIS has the identical problems that LEACH suffers from. Also the PEGASIS does not extent, cannot be useful to sensor network where comprehensive knowledge of the network is not simple to obtain. Power efficient gathering in sensor information systems (PEGASIS) is an enhancement of the LEACH protocol. Rather than designing several clusters it makes chains of sensor nodes so that each and every node transmits and receives from a neighbourhood and only one node is selected from that chain to transmit to the base station. Collected data transfer from node to node, amassed and eventually sent to the base station.

HEED

A hybrid energy-efficient distributed clustering methodology for an ad hoc sensor networks has a complement the insufficiency of the cluster head election algorithm in LEACH. HEED has the following features [11].

(i). Sensor nodes are the analogous type of nodes and consume energy.

(ii). Sensor nodes have no mobility.

(iii). Sensor nodes do not have their individual location information.

TEEN

Threshold sensitive energy efficient sensor network protocol is used for precipitous changes in the sensed attributes in the network. It uses a data centric mechanism and makes clusters in a hierarchical manner. Two threshold values are transmits to the nodes: hard threshold and soft threshold. The hard threshold is the least promising value of an attribute. Sensor nodes mail data to the cluster head only if they found the sensed value is higher than the hard threshold.

If sensor nodes found that the sensed value is less than the feature value of threshold than they do not send the data to the cluster head. Due to this way only relative data is send by the sensor nodes. In addition, when sensor node again sense value greater than the hard threshold value than they check the difference between current and earlier value with soft threshold. If the dissimilarity is again greater than the soft threshold than the sensor nodes will send recent sensed data to the cluster head. This process will remove encumber from the cluster head [13].

4. PROPOSED METHODOLOGY

The energy efficiency of cooperative communication has recently been investigated in [14] and [15]. The authors of [14] investigated the energy issues in a clustered sensor network, where sensors collaborate on signal transmission and/or reception in a deterministic way. It is shown that, if the long haul transmission distance (between clusters) is large enough, cooperative communications can dramatically reduce the total energy consumption still when all the association overhead is considered. Based on [14], the authors in [15] combine the cooperative communication scheme with a cross-layer design framework for multi-hop clustered sensor networks. The system is optimized to improve the overall energy efficiency and to reduce the network delay.

Cooperative communication for clustered sensor networks has also been investigated in [16]. In [17], the authors analyze distributed space-time block coding (STBC)-based cooperative communication for multitier clustered wireless sensor networks. Based on their analysis on the SER and throughput performance, the authors show that cooperative communication is more energy efficient than direct communication. However, the number of cooperative nodes in each cluster is fixed, and the inherent circuit energy consumption of wireless transceivers is ignored, which has recently been reported to be important for low-power wireless sensor networks. In this paper we uses group communication and election algorithm to make the network energy efficient and form secure network for data transmission.

An Election algorithm is a particular principle algorithm, which is run for selecting the coordinator procedure among N number of procedures. These coordinator or leader process plays a significant role in the distributed system to sustain the consistency through synchronization. For example, in a system of client server mutual exclusion algorithm is preserved by the server process Ps, which is chosen from among the processes Pi where i=1, 2... N that is the group of processes which would use the crucial region. Election Algorithm is essential in these circumstances to prefer the server process among the existing process. Eventually all the processes must agree upon the leader process. If the coordinator process fails due to diverse reasons then instantly the election should happen to choose a new leader process to take up the job of the failed leader. Whichever process can instigate the election algorithm whenever it encounters that the failure of leader process. There can be situations that all Nprocesses could call N synchronized elections. In anytime, process Pi is one amongst the following two states, when the election happens: Participant refers to the process is directly or indirectly involved in election algorithm, nonparticipant refers to the process in not engaged with the election algorithm currently. The goal of Election Algorithm is to choose and declare one and only process as the leader even if all processes participate in the election and at the end of the election, every process should agree upon the new leader process without any mystification. With no loss of simplification, the elected process should be the process with the largest process identifier. This may be any number demonstrating the order /birth/ priority/ energy of the process. All the process has a changeable called LEAD, which contains the process id of the current leader. When the process participates in the election, it sets this lead to NULL.

Any Election Algorithm should assure the following two belongings [10].

1) **Safety:** Any process P, has LEAD = NULL if it is participating in the election, or its LEAD =P, where P is the highest PID and it is alive at present.

2) **Likeness:** All the processes should agree on the chosen leader P after the election. That is, LEAD = PID Pi where i=1, 2,...,N.

Energy Conservation and group communication using election/bully algorithm
Step 1: Set Mobile Node

M = {MN_1, MN_2…...MN_{i-2}, MN_{i-1}, MN_i, MN_{i+1}, MN_{i+2},
MN_{i+3}, $MN_{i+4........}$ MN_n} **//Set of mobile Node's Step 2: S**et initial energy for each nodes

E = **{**$en_{1,}$ $en_{2,}$ -------, $en_{i-2,}$ $en_{i-1,}$ $en_{i,}$ $en_{i+1,}$
en_{i+2}, en_{i+3}, en_{i+4}--------------- en_n} **// each node energy initialize here**

Step 3: Select random node

MN_i є N for election message generation

Step 4: Measure Speed, Where

$Speed_i$ = Dist / (t_2-t_1) **// t_1 initial time,**
t_2 Broadcast Time, D distance travel

Step 5: Broadcast Elected message

Elct-msg($en_{i,}$ $MN_{i,}$ $Speed_i$) **// en_i energy of i^{th} node, $Speed_i$ is speed of i^{th} node**

```
            Set new $MN_i$ = $MN_j$ ;
            New $MN_i$ will generate election msg; THEN
            Goto step 5:
                    }
            Else
            {
            $MN_{i,}$ will act as a coordinator;
            }
            Else
            { Says ack as: Out of range; }
```

After Group Formation how to sends data to group

```
 //Manage and broadcast group message through coordinator under MANET
Set mobile node = M;        // mobile node
Set group coordinator = $MN_i$;   // $MN_i$ € M, $MN_i$ select on the bases of energy and speed
Send group_join msg ($M_n$ , $MN_i$, No) // group join message
        {
        IF (range <=550 && $MN_i$ == “true”) THEN
                {
                Join group member’s = {M1, M2…..$M_{n\}}$
                // $M_n$ € $MN_i$, if $M_n$ is in radio range zone
                }
                Else
                { Says ack as: Out of range }
        }
        Set sender node = S;
        Set routing protocol = AODV;   //Routing Protocol $PDR_{u,v}$ =0.0;
        Broadcast _RREQ(S, $MN_i$, rr)
        {
                IF (rr <= 550 && neighbour >= 1) THEN
                {

                THEN THEN
IF (radio-range<=550 && neighbour == True)

 {
 Record time at $t_n$;            // $t_n$ time in second’s
 Get neighbour $MN_{i-1,}$ $MN_{i-2,}$ $MN_{i+1}$, $MN_{i+2}$
        Forward RREQ and create Rtable and
         IF ($MN_i$ ==”true”) THEN
        {
Accept route packets and send group information
                                                }

Get info MN[j][$en_j$][$Speed_j$]  // j pointer not equal I, j node number, $en_j$ energy, $speed_i$ speed of node  }
Now Compare
 IF (MN[$en_i$] < MN[$en_j$] && MN[$speed_i$]> MN[$speed_j$])
THEN
        {
        $MN_i$ eliminate from competition
S = sends actual data to $MN_i$ node; group-msg (S,$M_n$, type);  //call function
        }
}
Else
{ Node out of range or unreachable; }


        $PDR_{u,\ v}$ = $PDR_u \cap PDR_i \cap$--------$PDR_j$ $\cap$ $PDR_v$
        //check pdr
        If ($PDR_{u,\ v}$ <5)
        Node has been less/discharged energy, then stop to send packet to them
        Else
        Communication starts, then sends packets to them Group-msg(S, Mn, type)  // type contain packet info
        {
        Search Mn nodes in radio range;
        Broadcast actual data to all group members Mn;
        }
```

5. EXPERIMENTAL RESULTS

We have discussed an improved algorithm in previous section and it is compared with previous algorithm. The implementation of an algorithm is done in well known network simulator NS-2.34 [18]. The simulation environment is setup to simulate the algorithm in which we take an area of 900x900 to transmit the packet CBR/TCP protocol AODV is used and the node consist the energy 0.45 joule for the simulation time 400s. In this work, mainly focuses for providing better security by consuming less energy. The comparison of above is done using different parameter such packet delivery ratio, throughput, routing load, delay etc.

Measuring Parameter

The performance of the WSN can be measured by using different parameter such as Throughput, Packet delivery ratio, end to end delay, routing load [19].

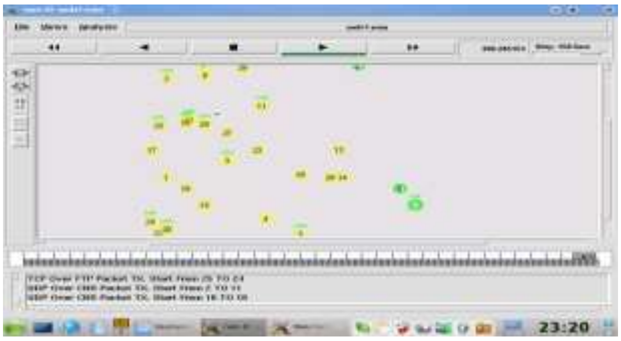
Throughput:

It is the average rate of successful message delivery over a communication channel.

Initial Energy	.75 joule
Simulation Time	400
Protocol	AODV

Scenario setup

Table 1 shows the simulation setup of our proposed algorithm. In this Scenario setup there are 30 mobile nodes placed defined with trajectory with 900m × 900m area. The simulation time was taken 400 sec. Here the locations of nodes are random with a speed of 0.45/packet.



TCP Over FTP Packet TX, Start from 25 TO 24
UDP Over CBR Packet TX, Start from 2 TO 11
UDP Over CBR Packet TX, Start from 16 TO 08

Fig. 2: A Snapshot of scenario setup for energy efficient Routing

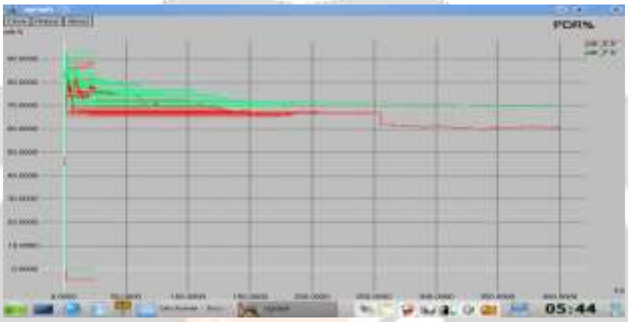


Fig. 3: A Snapshot of scenario setup for energy efficient Routing

In general, packet delivery ratio decreases as the number of load and network size were increased. The proposed algorithm is compared with the existing method in which our methodology provides greater no of the packet delivery ratio.

$hroughput \leq$

Packet delivery ratio

Packet delivery ratio is defined as the ratio of data packets received by the destinations to those generated by the sources.

Mathematically, it can be defined as:

PDR= S1÷ S2

End to end delay:

The average time it takes a data packet to reach the destination. This includes all possible delays caused by buffering during route discovery latency, queuing at the interface queue. This metric is calculated by subtracting time at which first packet was transmitted by source from time at which first data packet arrived to destination.

Mathematically, it can be defined as: **Avg. EED=S/N Table 1: Simulation environment**

Simulator	NS-2.34
Area	900x900
Nodes	30
Packet	CBR/TCP
Speed	0.45/packe t

Fig. 3: Comparison of PDR% for existing and proposed methodology

The undesirable increase in End-to-End delay could be observed in Fig.4 as compared when the network size increases. In our work, the end to end delay is calculated increase in network size with respect to simulation time. The simulation result of proposed work decreases the delay comparing with the existing methodology.

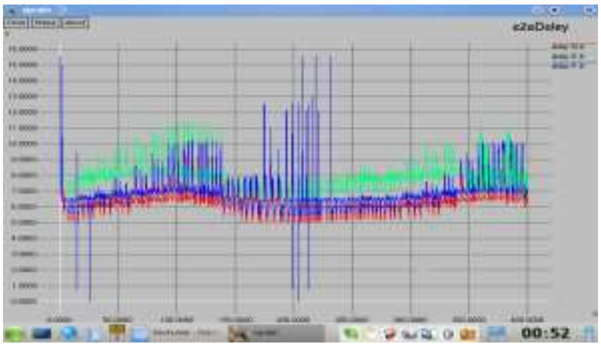


Fig. 4: Comparison of End to End Delay with existing and proposed methodology

The average energy consumption is compared with the existing and our methodology in which energy consumption is very less than the existing methodology as shown below in fig. 5

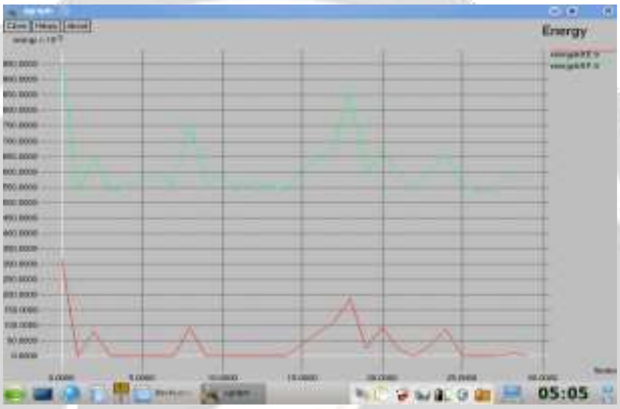


Fig. 5: Comparison of energy in joule Vs no. of nodes with existing and proposed methodology

In figure 6, throughput is calculated between the network size and simulation time, throughput is the average no of delivery of packets in the given time period. After simulating the methodology it proves that our approach gives better throughput than the existing ones.

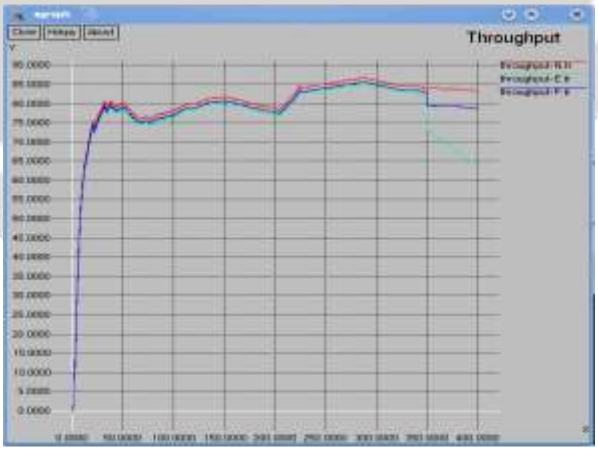


Fig. 6: Comparison of Throughput with existing and proposed methodology

6. CONCLUSION

The basic requirement for the communication, secure and energy efficient network is the primary requirement which can be influence by different malicious node while the sensor node has limited energy to transmit the packets. In this paper we proposed group communication method using election/bully algorithm to lessen the consumption ratio of nodes energy. The comparison of proposed algorithm is done with the existing methodology and the simulation result proves that our method is more efficient.

7. REFERENCE

[1] Adil Bashir, Ajaz Hussain Mir, “An Energy Efficient and Dynamic Security Protocol for Wireless Sensor Network”, International Conference on Advanced Electronic Systems (ICAES) , 2019 in proceeding of IEEE xplore

[2] Subramanian Ganesh, Ramachandran Amutha, “Efficient and Secure Routing Protocol for Wireless Sensor Networks through SNR Based Dynamic Clustering Mechanisms” Journal of Communications and Networks, vol. 15, no. 4, august 2018

[3] Luigi Coppolino, Salvatore D’Antonio, Alessia Garofalo, Luigi Romano, “Applying Data Mining Techniques to Intrusion Detection in Wireless Sensor Networks” Eighth International Conference on P2P, Parallel, Grid, Cloud and Internet Computing, 2019.

[4] K.Parameswari, M.Mohamed Raseen, “Aggregating Secure Data In Wireless Sensor Networks”, International Conference on Current Trends in Engineering and Technology, ICCTET’13 in proceeding of IEEE.

[5] Roshan Zameer Ahmed, Anusha Anigol, R. C. Biradar, “Reactive Security Scheme using Behavioral Aspects of Attacks for Wireless Sensor Networks”, International Conference on Advances in Computing, Communications and Informatics (ICACCI), 2020, in proceeding of IEEE.

[6] Sudharsan Omprakash, Giridharan Nanthagopal, Santosh Kumar Omprakash, “A secured energy efficient clustering and data aggregation protocol for wireless sensor network”, American Journal of Computation, Communication and Control 2019; 1(1): 18-23

[7] Malika BELKADI, Rachida AOUDJIT, Mehammed DAOUI, Mustapha LALAM, “Energy-efficient Secure Directed Diffusion Protocol for Wireless Sensor Networks”, I.J. Information Technology and Computer Science, 2018, 01, 50-56

[8] BabakNikmard and Salman Taherizadeh, “Using mobile agent in clustering method for energy consumption in wireless sensor network”, International Conference on Computer and Communication Technology (ICCCT), pp.153-158, 2020.

[9] Ali K., Neogy S., and Das P.K., “Optimal Energy-Based Clustering with GPS-Enabled Sensor Nodes”, Fourth International Conference on Sensor Technologies and Applications (SENSORCOMM), pp.13-18, 2019

[10] Di Tang, Tongtong Li, Jian Ren, Jie Wu, “Cost-Aware Secure Routing (CASER) Protocol Design for Wireless Sensor Networks”, Parallel and Distributed Systems, IEEE Transactions 2019 on volume: PP, Issue: 99

[11] Jong-Yong Lee, Kyedong Jung, Hanmin Jung, Daesung Lee, “Improving the Energy Efficiency of a Cluster Head Election for Wireless Sensor Networks”, Hindawi Publishing Corporation International Journal of Distributed Sensor Networks Volume 2018, Article ID 305037, 6 pages

[12] Fan Wu," incentive-compatible opportunistic routing for wireless networks", mobicom’08, September 14–19, 2008, San Francisco, California, USA 2021

[13] Naveen Sharma, Anand Nayyar, “A Comprehensive Review of Cluster Based Energy Efficient Routing Protocols for Wireless Sensor Networks”, International Journal of Application or Innovation in Engineering & Management, Volume 3, Issue 1, January 2020 ISSN 2319-4847

[14] S. Cui, A. J. Goldsmith, and A. Bahai, “Energy-efficiency of MIMO and cooperative MIMO in sensor networks,” IEEE J. Sel. Areas Communication, vol. 22, no. 6, pp. 1089–1098, Aug. 2020.

[15] S. Cui and A. Goldsmith, “Cross-layer design of energy-constrained networks using cooperative MIMO techniques,” EURASIP Signal Process. J., vol. 86, no. 8, pp. 1804–1814, Aug. 2021.

[16] M. Dohler, Y. Li, B. Vucetic, A. H. Aghvami, M. Arndt, and D. Barthel, “Performance analysis of distributed space-time block encoded sensor networks,” IEEE Trans. Veh. Technol., vol. 55, no. 7, pp. 1776–1789, Nov. 2022.