Energy Efficient and Secured Key Based Management in Area Monitor by WSN

K.R. Asha, M.C. Supriya

Abstract*: Popular Technology for monitoring Environment, observation of battle field, caring of health, tracking of object, managing during various types of attack is by Wireless sensor networks. Whenever, area which is strictly monitoring by WSNs it has to handle all the critical situation. That is, when area affected by radiation creates node outage problems with in the critical areas monitoring by WSNs. For that solution should be needed when communication problem arises between the nodes. Reliable Transferring of information from nodes to the base station, less utilization of energy to improve the network life time and also along with these secure mechanisms are also needed to save the sensed information from hostile environment. In this paper clustering process with security mechanisms are used. Key based security approach used to validate data inside cluster and outside the cluster during data reaches to the base station. RSA encoding of the data to hide data from external persons. A security mechanism of our scheme shows that our protocol is effective in defending against radiation attack and intentionally node attacked hackers. Key based security approach implemented in Linux OS and simulate it using NS2 simulator to assess its time, energy, communication, and memory performance..

***Keywords* : key based security and WSN.**

I. INTRODUCTION

Innovative WSNs in a very fast manner become popular with reasonable cost, low power, and multi functionality wireless sensor nodes. Tiny sensor devices are embedded devices networking through wireless communication media [1, 2]. That devices are Unified with a physical hostile environment, which are very sensitive areas needs extreme security. When Ever attackers, intentionally try to attack the sensitive area through the radiation and try to hack the information which is sensed by the nodes of WSNs .In that situation due to radiation attack, node outage problem will be created and sensed nodes are stopping their services by behaving transfaulty node [22-24]. Transfaulty nodes are sensing the information properly but failure to communicate with neighbor nodes. This problem is not permanent, whenever the effected of radiation is decreases, then the communication can be achieving between the nodes with delay of packet sending, with loss of packets and more energy is utilized with in the nodes[25-29]. For that situation, in our previous work we are getting solution for that problem by considering mode transferring, efficient routing mechanisms, clustering mechanism and data reduction mechanisms for efficient and effective transferring of information to the base station. But along with radiation attack, attackers hacked the any of the nodes present in radiation attacked area to send malicious data then security mechanism is essential to monitor the sensitive and critical area with effective and safe security mechanisms in a well-equipped manner. In this paper we are focusing on different type of security mechanisms and effectiveness of key management techniques for enhancing and supports efficient key revocation for compromised nodes. Minimizes the impact of a node compromise. A security analysis of our scheme shows effective in defending against radiation attacks that creates transfaulty nature in nodes of WSNs. Here implement Key based security approach used to validate data inside cluster and outside the cluster and RSA encoding of the data to hide data from external persons. A security analysis of our scheme shows that our protocol is effective in defending against the attacks. We implemented security mechanism in Linux OS and simulate it using NS2 simulator to assess its time, energy, communication, and memory performance and to improve the network life time.

The main significant things presented in the manuscript helps in easy way to improving the performance of key management system in Wireless sensor network. The paper also indicates research movements. Section I Discusses about the Existing study where different review studies are discussed for security schemes in WSN followed by discussion of research problems. In Section II Our proposed work is discussed. In section III gives results by simulation concerned to the proposed mechanism. Finally, the conclusive remarks are provided in Section IV.

II. LITERATURE SURVEY

Mojtaba Jamshidi et al [3] To avail better security in WSN Key Predistribution Scheme is Applied In this paper, a hybrid Key Predistribution Scheme uses three different keys, primary pairwise, polynomial, and ordinary. Here J-SIM simulator has been used to implement and its performance is evaluated by considering network size and resiliency against node attack. Simulation results have been compared with various scheme to show proposed scheme is secured and better one.

In this scheme, effectiveness of the scheme dependence on large number of captured nodes are suitable for Key

Revised Manuscript Received on July 08, 2019.

K.R. Asha, Department of Master of Computer Application, SSIT, Tumkur, India. srisaitechnologymadurai@gmail.com

Dr.M.C. Supriya, Department of Master of Computer Application, SSIT, Tumkur, India.

Predistribution Scheme and not considering any other considerations. If the node capture is low, performance of the scheme is not good. It Works better for large numbers of node captured by attracter compare to other schemes.

Majid R et al [4] to avoid communication problems, uses existing cryptographic concepts and advantages of asymmetric encryption to get better key distribution. For implementation, a fast modular exponentiation algorithm and a shortest public exponential techniques will be used to increase the node's data computation to consume less power.

Yet there is a need of better advanced mechanisms to improve the minimum energy utilization for algorithms to perform data manipulation and needs investigation of other attacks against the proposed protocol to increase its security.

Sofiane Aissani et al [5] designed for, transmit the data in highly secured way between sensor nodes and base station, more stability concerned to attacks, less storage utilization for keys and less computation regarding key generation.

However this system will needs more energy during over all operation and during Communication overhead.

Jai Prakash Prasad et al [6] for secure communication between sensor nodes to sink node in spherical gird based WSN, Elliptical Curve Cryptography (ECC) scheme is used. In this technique sensor nodes are randomly distributed. Transmission of data between sources to base station by number of hops in fast manner and avoids communication overheads with less packet loss.

But here, energy of each node which comes in the path will be used because transmission is taken place hop by hop by manner. So energy consumption will be more.

Danyang Qin et al [7] in this paper, authentication and security is given to the nodes which is hacked by attackers. For that distribution of key has been distributed to nodes before deploying, security has been given to network during network deployment and authentication to the node will generated when it needs to communicate with other node.

Here more attention is given to security but still needs given importance to routing for transmitting the information from nodes to base station which will avoids the energy of the nodes presented in the network.

Jitendra Singh et al [8] for secure communication RSA scheme has been used to avoid problem rise during the communication and reduce the computation complexity arises during the key generation.

Yet it needs improve the performances and reduce the energy utilization during communication.

Chinyang Henry Tseng et al [9] presented system for protecting the patient's medical data in secured way in each and every point using Elliptic Curve Cryptosystem. To manage a large number of sensors, clustering concept is used. Data collected from the sensors will be transmitted to access point and then data will be sent to main access point

However, secure communication is found in Wireless sensor network. But secure channels is built between secure sensors and the nearest Secure access point. There is no direct communication with the Root Secure access point. Whenever secures access point is damaged due to some circumstances, then secure sensors are unable to send the data to Root secure access point and number of secure sensors are increase. Then there is a need of including new secure access points. This will leads decreases in network performances.

Osman Yagan and Armand M. Makowski[10] presents schemes for providing secure keys for sensors to achieve more security during attack by hackers and less association with computation complexity of the large network.

Here there is a need of addressing the problem related to wireless communication and use of better and efficient key distribution scheme is needed.

Jun Zhao [11] presents concerned to security. Most critical parameters to get connectivity even when in the presence and absences of attacks in the networks. They also given importance to node replication attack to achieve secure transmission in the WSNs.

However more importance is given to get connectivity and attack between the nodes. There is need of efficient transmission mechanisms.

Ying Zhang et al [12] develops a dynamic key management method. The method can achieved by updating of dynamic keys which solve the security defense problem of system. When the cluster heads are captured by attacker. By the simulation indicates that this method is based on clustering routing protocol and consuming minimum storage. This method is stronger ability of resistance to capture.

Here yet there is need of more secure measurements to avoid capturing of cluster heads in the network.

Chin-Ling Chen et al [13] presents analysis about secure communication and given the scheme that supports a direct accessing of data from the cluster to user using mobile device. But not discussed about efficient communication by saving energy and avoiding irrelevant communication.

Seung-Hyun Seo Et Al. [14] delivers a effective key management protocol by using certificatelees concept to get communication in secured way in dynamic wireless sensor networks and by considering mobility in node. Protocol gives efficient key updates when a node leaving or joining a cluster. This assures forward and backward key secrecy and also supports efficient key cancellation for compromised nodes and decreases the contact of a node compromise on the security of other communication links. Simulator to be used to assess its time, communication and memory performance, but there is need of quality of service in this work.

Jongho Won et al [15] discussing the energy problems related concerned to the development of security measures in WSN. Securing data aggregation is achieved by considering security protocol without any certificate and signcryption scheme for securing data aggregation are considered. Computational time was minimizing but importance is not considers for scalability measurements.

Wenliang Du et.al [16], Authors propose a key pre-distribution scheme, this method essentially advances the flexibility of the network related to the current schemes. Scheme uses parameter for security. By considering the specified values for the parameter decision will be taken concerned to network is

secure or not. Memory utilization is taken more in this scheme, when more values consider for security parameter. Here importance is given only to network flexibility against node attacks but does not bother about memory usages.

Sk.Md. Mizanur Rahutman et al [17]. Proposes Key management, it is very much important for security in wireless sensor networks. In current schemes establish shared keys for all pairs of neighbor sensor nodes. Due to that more number of keys need to be loaded on each sensor nodes, for that more space is need for nodes in wireless sensor network. To avoid this, author propose a novel key agreement protocol. In that, any two nodes that need to communicate each other, that are independently compute the same secret key by using pairing and identity-based encryption properties. This will definitely decreases space for key in node. Additionally, the security analysis of the protocol shows that it is robust against a number of attacks. But not discussed about effective communication by saving energy and avoiding irrelevant communication.

M.R. Alagheband et al [18] Authors propose a dynamic and secure key management model for hierarchical heterogeneous sensor networks. Secure communication is needed in applications that uses the WSNs. However, because of restricted communication and hardware capabilities WSNs failure to give its service in crucial environment. Key management very essential for security in WSNs In this study, the authors propose a dynamic key management structure based on elliptical curve cryptography and sign cryption method for heterogeneous WSNs. For prevention of SN compromise both periodic authentication and a new registration methods are used. Author comparing the scheme with the number of seminal hierarchical heterogeneous WSN key management schemes, the structure proves that, this is better in terms of communication, computation and key storage. Yet, here it needs less complication in computation and minimum usage of memory.

David Sánchez Sánchez.et.al [19] Authors proposes for mobile sensor networks apply combinatorial design theory to pre-distribute Blundo's polynomials. Again to increase scalability approach is combined with Liu and Ning polynomial evaluation optimization. This method, without a decrease in network scalability or resiliency solves the combinatorial design existence problem of Çamtepe and Yener key pre-distribution scheme. This scheme has some advantages regarding including direct pairwise key establishment, which helps in enables authentication, tolerance during node captures by attackers, increased scalability and less computational and decreases communication overhead. But to get effective scheme need of considering other parameters like memory usage, energy usage and effective transmission.

Sarita Agrawal et al [20] Authors proposed a novel key update protocol in mobile sensor networks, which is used in the health care system in efficient way. For real-time update security for the network topology, in this scheme uses AVL tree for dynamic updated key. By using random inputs in mobile sensor networks key update protocol securely updates the session key between pair of sensor nodes. Yet, some problems like memory usage, energy efficiency need to be addressed, one of which will gives more security issue.

Chan et al. [21] proposed the scheme whenever small scale attack is taken in networks by generating keys which gives the more security by considering node to node within the network without involving the base station.

Here security is achieved with in the network but whenever attack is taken between the nodes and base station security measure is not taken hence security measure is needed.

The existing works discussed in the literature expose that, key management is effective in hostile environment to secure the data from the hackers. Hence there is need of effective key management to transmit the data in a secure way to the base station and along with need to give our attention to efficient utilization of energy in the sensor nodes by using efficient clustering mechanisms to lessen the usage of energy of nodes are needed, avoiding the same data transmitting to base station by data aggregation technique are needed and also whenever radiation attack has been taken in that area ,in that situation node behaves like a transfaulty node then communication failure between the nodes will be taken place for that, communication mode transfer mechanisms are needed. For all these, our previous work will be used to overcome the problems arises during that situations to improve the life time of the network.

III. PROPOSED WORK

WSNs applications are needed in critical environment. WSNs needs efficient secure mechanisms to transfer the sensed data from member nodes to base station in secured manner. For that, we proposed efficient key based mechanisms to achieve. Applying secure mechanism in wireless sensor network is not only sufficient along with that energy efficiency, efficiency on routing, data aggregation is needed and communication mode transfer is needed whenever external attacks like radiation or electromagnetic waves affect sensor nodes. This creates node outage problem that is node will stop its services. Sensor node will Exhibits transfaulty behavior. Hence to monitor hostile environment in case of radiation attack and intentionally hack nodes to send the wrong data to base station, using our previous work concepts and secure mechanism through key management, transfer the sensed data to base station for improve the life time of network. Our scheme involves following for secure and efficient transmission of sensed data during radiation attack and intentionally attack nodes in WSNs to disturb communication by the hackers.

The wireless sensor network are created with 'n' sensor nodes.

Generating node secrete key by KGC

Sharing node secrete key with members and base station

Radiation attack on specified area

Radiation aware Communication mode adjusting is done

Clustering of network

Selection of cluster head

by stability based mechanism

Generating cluster key by cluster head

Sharing the cluster secrete key with members to achieve Intra cluster transaction

data aggregation for avoiding continuous transaction of same data

The aggregated data is encoded by RSA algorithm

Cluster head will use node secrete key to achieve inter cluster security

Cluster head will transmit the data to base station along with node secrete key.

Checking the node secrete key and decode the data in base station.

For effective communication mode transferring our previous work mechanism is used to work in radiation-affected environments and intentionally hacker hack the sensor nodes in wireless sensor network to inject malicious data. First to continue communication in radiation prone environment between sensor nodes, a sensor node has dual mode of communication. That is radio frequency (RF) communication mode and acoustic communication mode. In normal situation sensor nodes working in RF mode whenever radiation attack affects the node then it is switched to acoustic mode. Communication between the nodes will be continued and by this node outage problem will be solved in radiation prone environment. For this we are using our previous work and along with this if hacker hacks the wireless sensor network created with 'n' sensor nodes. Each nodes in the network having their own node secrete key and it is generated by using key generation center then key will be shared between the nodes and base station whenever the nodes are going to participate.it is going utilize the key. Before transmits the sensed data from member nodes to base station the nodes are divided into m clusters, in each cluster, head selection algorithm of our previous work will be used to elect a node as head node. Head selection is based on based on remaining energy, node coverage and mobility of the node. The node which is having maximum remaining energy and maximum node coverage and minimum mobility will be elected as head node. Whenever node is elected as elector at the time it will generated its own cluster key and it will informed to the neighbor node. The member nodes are going to utilize cluster secrete key and it will be generated by simple rand function. Then member nodes with in the cluster will forwarded the data to elector along with the cluster secrete key. Member nodes will be validate with in the cluster head by verifying the cluster secrete key. There is no problem with attacker when attacker is present inside that cluster. First level security is achieved. That is intra cluster security is achieved. After validating received data from the members of cluster, aggregation of data will be taken place. Before aggregated data will be forward to the base station, encoding of aggregated data will be taken place using RSA algorithm in cluster head. Know the data is going outside from cluster head to base station. Send data may be hacked by hacker. Hackers may be leaked the data or change the data is another problem. To overcome this, cluster head will utilize the node secrete key. The aggregated and encode data will be transmitted through cluster head along with the node secret key. Whenever it will come to base station then base station verify the node secrete key send by the cluster head and validate the packet. Know Second level security is achieved. If it is attacked node does not have their node secrete key at time the base station will take care whether the key is utilize by the particular packet is validate or not. First cluster head key is validated after that node secrete is validate. If is not validate it will drop entire data and it won't waste the time to decode the data. If it is not hacked or not modified, the original data will be reach to base station. Keyes used in our work is generated by using simple random function, that will be used to avoid complication and to save memory for our key management process.

The Remaining Energy is the amount of energy present in a wireless sensor node at the current instance of time, is given by the equation (1)

REM_ Eng= E_Ginit – E_Gcons(t) (1)

Where E_Ginit (t) is the initial energy of the node and E_Gcons is the energy consumed by the node after the period of time Tt and is given by the equation (2).

E_Gcons (Tt) = (N_DPT * C1) + (N_DPR * C2) (2)

Where N_DPT is the number of data packets transmitted, N_DPR is the number of data packets received and C1 and C2 are Constants in the range (0, 1).

Node coverage N_Dis(x) of the node is find out from ratio of average distance with its neighbors. It is find out by the equation (3)

N_Dis(c) =∑_1^(N(c))▒〖 ((x,y)∈E/ y∈N(x))/ |Neg(x)| 〗 (3)

Where |Neg(x)| gives number of neighbor's node, x and y is the node, Ed is the set of edges of a cluster of network Graph G (Vx, Ed).

Mobility Mob_Node (n) of the node is calculated by using the equation (4)

Mob_Node (n) = 1/TT ∑_(t=1)▒√ (〖 (〖xc〗 _t- 〖xc 〗 _(t-1))〗 ^2 + 〖(〖yc〗 _t- 〖yc〗 _(t-1))〗 ^2) (4)

Where (xct, yct) and (xct-1, yct-1) are the co-ordinate positions of node Vx at time t and t-1

Average of the data collected by cluster members in the cluster is calculated by avgcul (c) is find out by using (5)

Avgcul(c) =∑_(i=1)^M(c)▒ 〖dataNd(i)〗)/|MemCul(c)| (5)

Where | MemCul(c) | is total number of members in a cluster and data (i) is the data of the ith node in a member set of the cluster.

Deviation percentage, DPClu of the deviated members in the cluster c calculated by using (6)

DPClu= (DMClu(C)/|MemClu (c)|) *

100.

Input :
Nd : set of sensor nodes in the WSN
NdSecKey : Node secrete key
Clu : set of cluster in the network N
CluSecKey: :Cluster secrete Key
CluHead(c) : cluster head of the cluster
Memclu(c) : member set of the cluster
dataNd[n] : collected data of the sensor node n
avgClu(c) :average of collected data in the cluster c
agdataClu[c] : aggregated data of the cluster head
DmClu[c] deviated members count of the cluster c
DTh : Threshold to identify data deviation
DMClu(c) deviated members count in the cluster c
MTh: Threshold to decide on the data aggregation
DPClu : deviation percentage of the deviated members in the cluster c
1: for each cluster 'c' in the network Nd
2: for each member in cluster c
3: Generate CulSecKey with in the CluHead
4; Share CulSecKey with member in cluster
3: Collect data - dataNd[m] at the sensor node 'm along NdsecKey
4: Transmit the data to head node with cluSecKey
5: m ⇨ luHead(c)
6 :cluster head validate the key if the data send by the valid node
otherwise data is not accepted by cluster head
7: data reduction phase with encode the data by RSA algorithm
8: Computing average avgClu(c) of the collected data at head
CluHead(c)
9: for each member 'm' in cluster c
10: diff[m] = avgClu(c)-dataNd[m]
11: if(diff[m]>DTh) then
12: DMClu(c) ++
13: Computing deviation percentage DP of members in cluster c
14: if(DPClu < MTh)
15: avoid the dataNd[m] from aggregation
16: else
17: add dataNd[m] into aggregation queue
18: validating member threshold at cluster head
19: NetSeckey=int(rand()*1000)
20: sending aggregate data agdataClu[c] from the aggregation Queue
21: Find energy aware route to reach base station
22: Transmit the data to base station along with NdSecKey
23: CluHead(c) ⇨ BS
24: base station validate the Node secrete key from the cluster then if it is valid then data is accepting and decode the data by RSA algorithm
25: end for

IV. SIMULATION ANALYSIS

The proposed method is tested on Network simulator (NS2). Sensor nodes are distributing in the environment of simulation. Parameters needed for our mechanisms are as shown on Table-1. The simulation of the proposed scheme has been checked for 50, 100,150 and 200 nodes deployed in the 3000×2500 simulation area. Communication can achieved using UDP communication protocol between the nodes. Traffic in wireless sensor network is handle by CBR traffic model. To propagate radio waves two-ray ground is used for that purpose. To receive the signal from all the nodes from all direction Omni directional antenna used. The proposed scheme is evaluated by considering reduction of energy consumption in efficient way for improve the life time of the entire network and with secure mechanism. In the simulation result we observed with less packet loss, efficiently and reliable transfer of sensed data.

Table-1. Simulation **P**arameters

Channel Type	Wireless
Simulation Time	50 ms
No of nodes	50,100,150,200
Area of Simulation	3000x2500 m
Transmission range	250m
Network Interface Type	WirelessPH
Initial energy	100 Joules
Energy consumption	0.0001 Joules/meter
Area affected by radiation	1000-2000 X-axis, 750-1500 y-axis
Range of sensing	30 m
Range of communication in RF mode	90 m
Communication Range in acoustic mode	70 m
Speed of radio frequency signal in air	$3*10^8$ m/s
Speed of ultrasonic sound through air	330m/s

The proposed method gives with secure way transmitting the sensed data from sensor nodes to base station. Our

reliability and secure based data transaction with data reduction using RSA algorithm to encode and decode the data. Reduction of energy consumption in nodes is very less compare to method without security and scheme considered for effective transmission in the hostile environment. That is, when radiation attack will cause node outage problem which stopping the functionality of WSN's component and intentionally node is attacked by the hacker.

Figuare-1 shows comparison of method with security and without security in particular instant of time. Lot of energy is reaming in nodes of WSN improves the life time of the entire network, data can be transferred in secure way with energy efficiently.

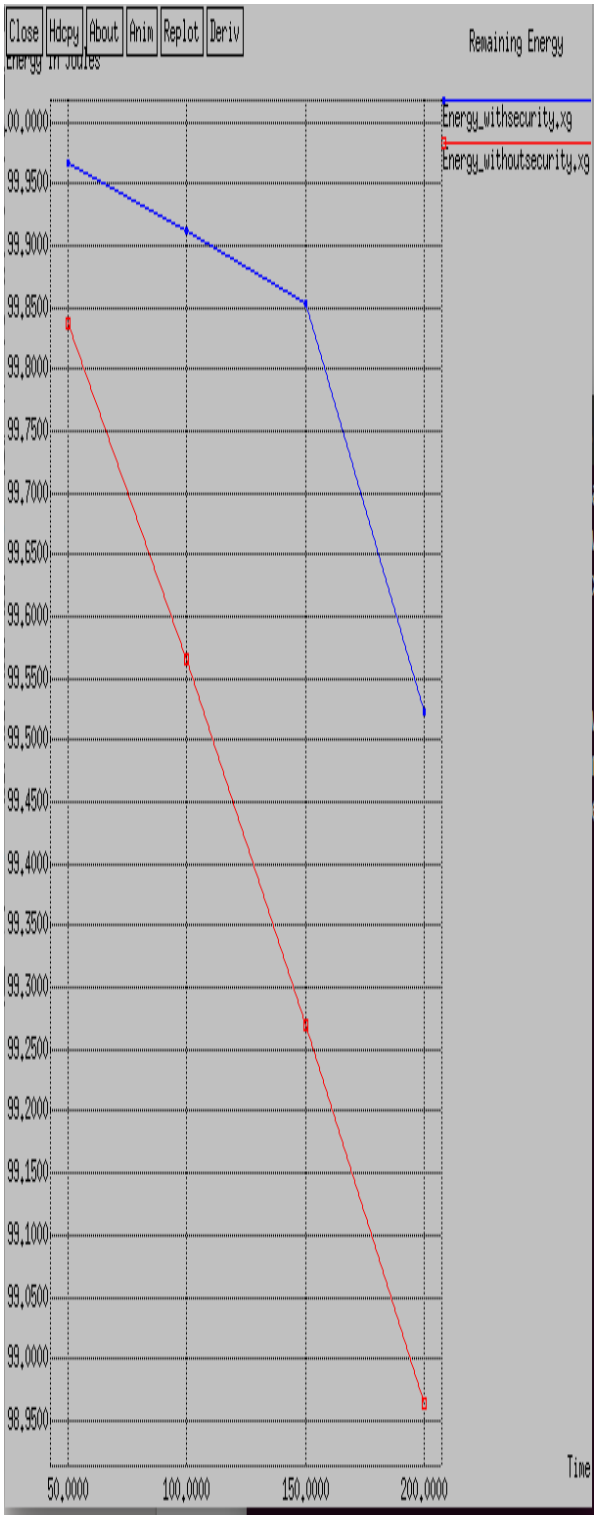

Fig. 1: Comparison of Residual energy for of 50,100,150 and 200 with security and without security.

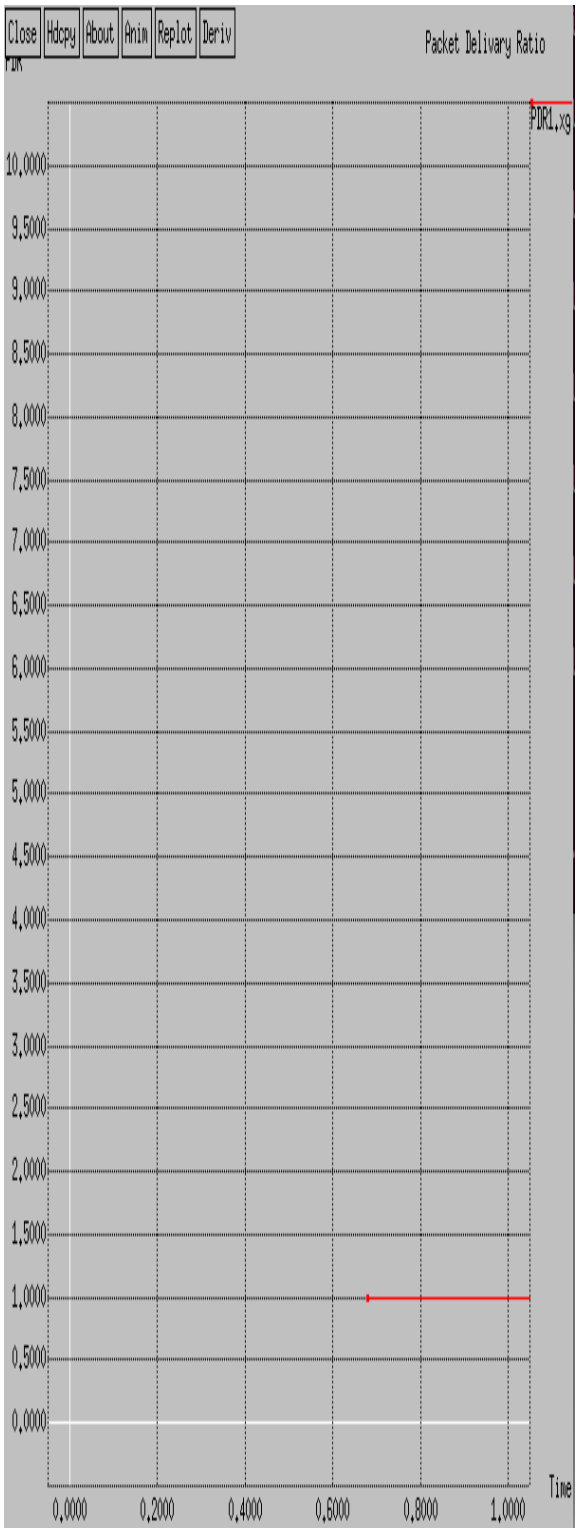

Fig.2: Packet Delivary Ratio of nodes in with security

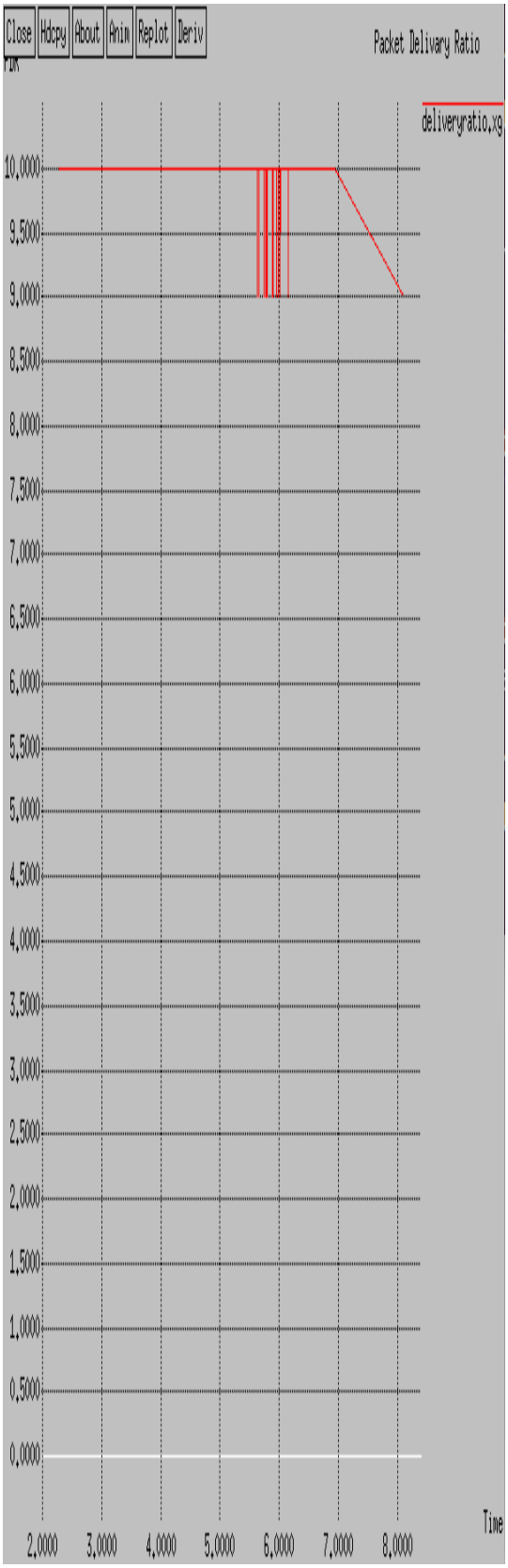

Fig. 3: Packet Delivary Ratio of nodes in Usual Method without security

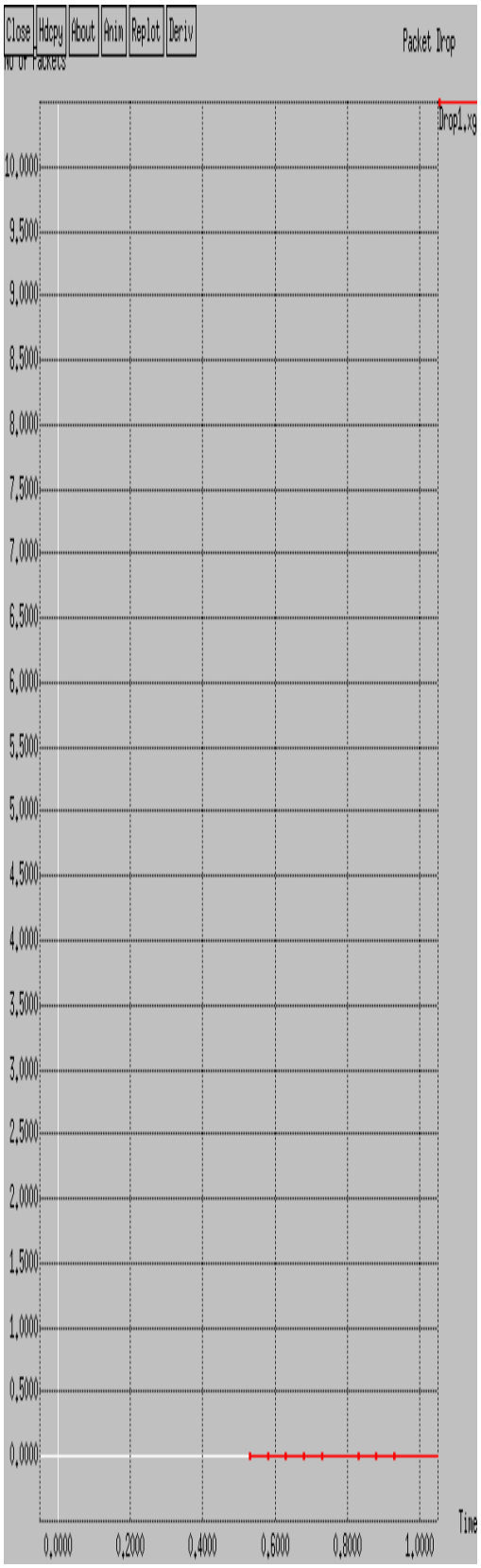

Fig. 4: Packet Drop of nodes with security

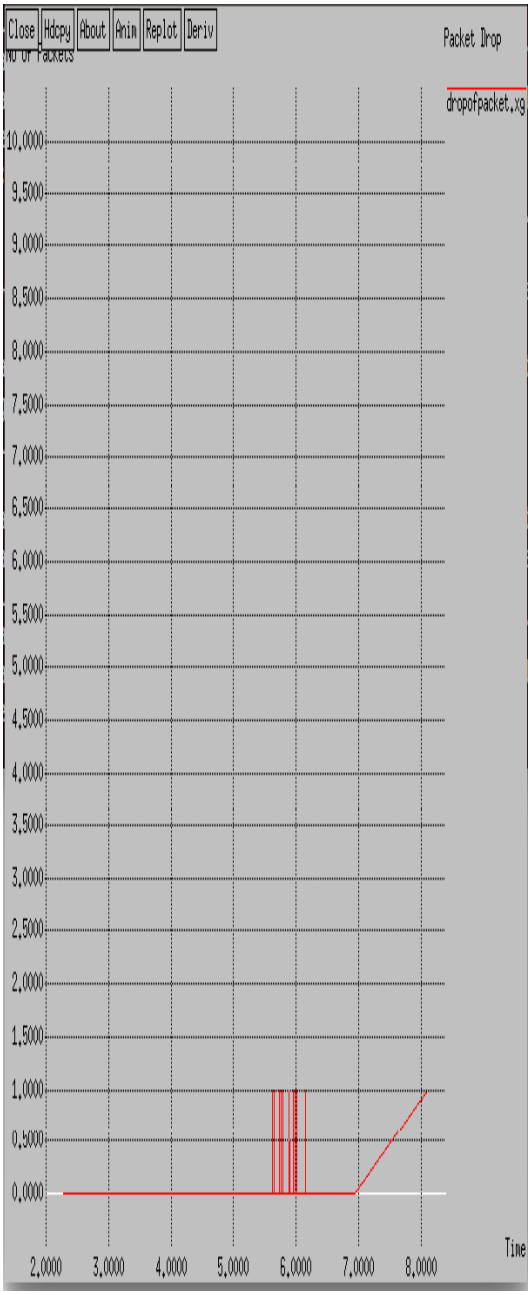

Fig. 5: Packet Drop of nodes without security

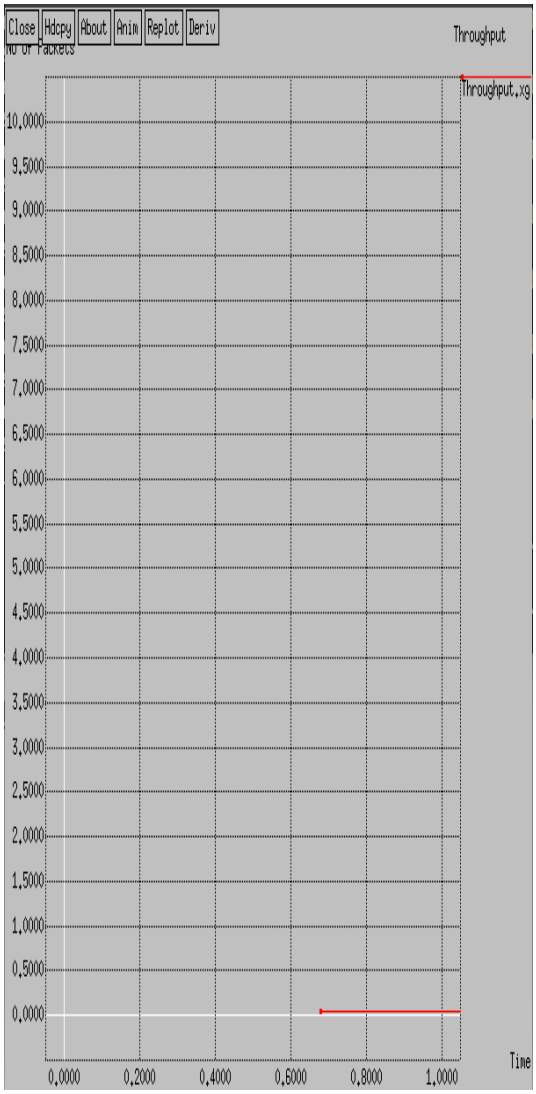

Fig. 6: Through put of nodes in with security

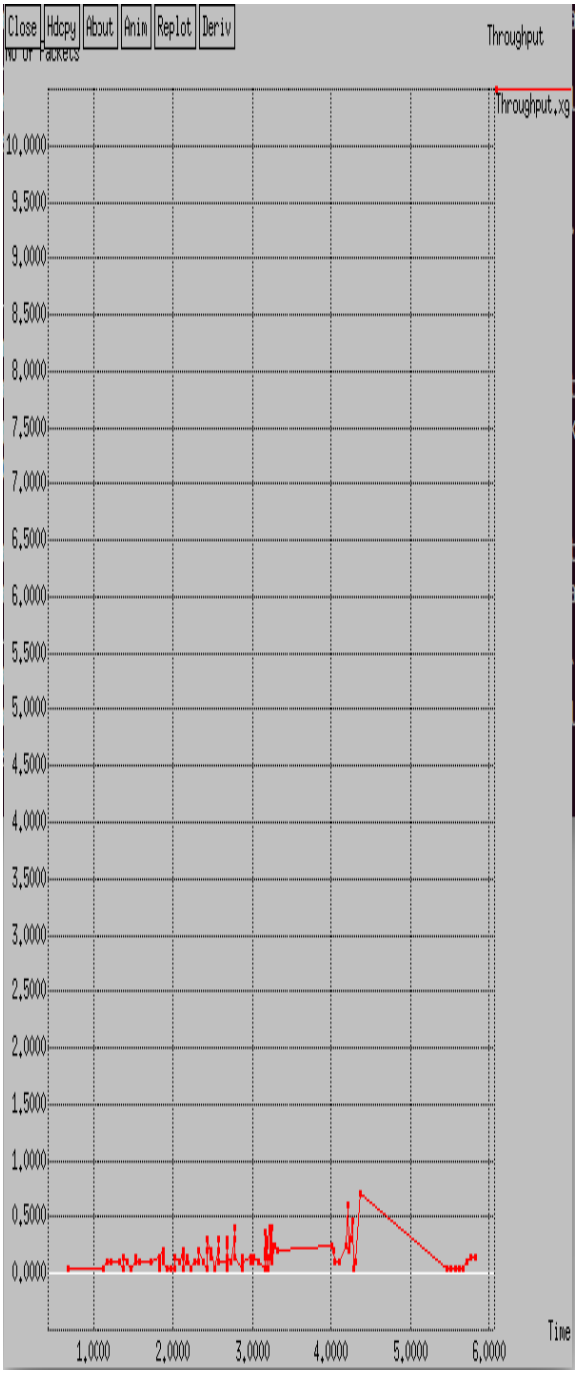

Fig. 7: Through put of nodes without security

Figure-2 and Figure-3 shows Packet Delivery Ratio of nodes in method with security and without security, Figure-4 and Figure-5 shows Packet drop of nodes in Method with security and without security and Figure-6 andFigure-7 shows through put nodes in Method with security and without security respectively. In the proposed method sensed data can be reliably reached to base station with secure manner. That will be observed in the simulation results.

By using the our method with security, we were able to transmit data with security in faster manner as compare to others and along with we give importance to energy constraint of wireless sensor network in radiation affected environment and intentionally disturb by the hackers..

V. CONCLUSION

More Achievements in the area of wireless sensor network and wireless communication will be going on in the recent years. Number of research and contributions are given to the field of Engineering and Technology. That helps with better performance in critical work in the field of hostile environment. Wireless Sensor nodes in Wireless senor networks provided with limited power, whenever radiation attack is taken place in the area monitored by WSNs and intentionally nodes are attacked by hackers which will decreases the life time of network and invalid data will reaches the base station. Our approach will considers these type of accidental events to avoid the communication failure and also proposed a technique for improve the energy efficiency of the nodes to increase the lifetime of network. In radiation affected environment and along with security is also given with in the cluster and also outsides the cluster. Data sensed by wireless sensor are collected and reduce the same amount of the data which will forwarded from cluster to base station for avoiding more transaction. Reduction of data leads less consumption of energy in an effective way. In future work, it has been planned to give more security measurements with in the network and avoid the transfaulty behavior of the nodes to improve the energy of nodes in efficient way..

ACKNOWLEDGMENT

The authors would like to thank the anonymous referees and the editor for their constructive comments and valuable suggestions which have helped improve the quality and presentation of the paper.

REFERENCES

1. F. Akyildiz, S. Weilian, Y. Sankarasubramaniam, and E. Cayirci, “A survey on sensor networks”, Commun. Mag., vol. 40, no. 8, pp.102–114, Nov. 2002.
2. I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, “Wireless sensor networks: A survey”, Comput. Netw. vol. 38, no. 4, pp. 393–422, 2002.
3. Mojtaba Jamshidi, Hamid Bazargan, Abdusalam Abdulla Shaltooki, Aso Mohammad Darwesh,“A Hybrid Key Pre-Distribution Scheme for Securing Communications in Wireless Sensor Networks”, International Journal on Informatics Visualization, vol 3,No 1,pp 42-46, 2019.
4. Majid R. Alshammari, Khaled M. Elleithy,” Efficient and Secure Key Distribution Protocol for Wireless Sensor Networks”, Journal of Sensors, Volume 2016, Article ID 1547963, 9 pages, 2016.
5. Singh, V. Kumar and R. Kumar, "An RSA based certificateless signature scheme for wireless sensor networks", 2015 International Conference on Green Computing and Internet of Things (ICGCIoT), Noida, pp. 443-447, 2015.
6. C. H. Tseng, S. H. Wang and W. J. Tsaur, "Hierarchical and Dynamic Elliptic Curve Cryptosystem Based Self-Certified Public Key Scheme for Medical Data Protection", in IEEE Transactions on Reliability, vol.64, no. 3, pp. 1078-1085, Sept. 2015.
7. O. Yagan and A. M. Makowski, "Wireless Sensor Networks Under the Random Pairwise Key Predistribution Scheme: Can Resiliency Be Achieved With Small Key Rings?", in IEEE/ACM Transactions on Networking, vol. 24, no. 6, pp. 3383-3396, December 2016.
8. Zhao, "On Resilience and Connectivity of Secure Wireless Sensor Networks Under Node Capture Attacks", in IEEE Transactions on Information Forensics and Security, vol. 12, no. 3, pp. 557-571, March 2017.
9. Zhang Y, Zheng B, Ji P, Cao J. “A key management method based on dynamic clustering for sensor networks”, International Journal of Distributed Sensor Networks, Jul 1; 11(7):763675, 2015.
10. Chen CL, Chen CC, Li DK. “Mobile device based dynamic key management protocols for wireless sensor networks”, Journal of Sensors, 2015.
11. S. H. Seo, J. Won, S. Sultana and E. Bertino, "Effective Key Management in Dynamic Wireless Sensor Networks", in IEEE Transactions on Information Forensics and Security, vol. 10, no. 2, pp. 371-383, 2015.
12. J. Won, S. H. Seo and E. Bertino, "Certificateless Cryptographic Protocols for Efficient Drone-Based Smart City Applications", in IEEE Access, vol. 5, pp. 3721-3749, 2017.
13. Wenliang Du, Jing Deng, Yunghsiang S. Han, Pramod K. Varshney,” A Pairwise Key Pre-distribution Scheme for Wireless Sensor Networks”, ACM Transactions on Information and System Security, Volume 8 Issue 2, Pages 228-258, 2005.
14. Sk.Md. Mizanur Rahman, Khalil El-Khatib,“Private Key agreement and secure communication for heterogeneous sensor networks”, J. Parallel Distrib. Comput, J. vol. 70 pp. 858–870, 2010
15. M.R. Alagheband, M.R.Aref,”Dynamic and secure key management model for hierarchical heterogeneous sensor networks”, IET Information Security, vol.6, Issue 4 , pp 271-280, 2012.
16. David Sánchez Sánchez, Heribert Baldus, “A Deterministic Pairwise Key Pre-distribution Scheme for Mobile Sensor Networks”, First International Conference on Security and Privacy for Emerging Areas in Communications Networks, 2005.
17. Sarita Agrawal, Rodrigo Roman, Manik Lal Das, Anish Mathuria, and Javier Lopez,” A Novel Key Update Protocol in Mobile Sensor Networks”, International Conference on Information Systems Security, vol 7671, pp. 194–207, 2012.
18. H. Chan, A. Perrig, and D. Song,“Random key predistribution schemes for sensor networks,” in Proc. IEEE S&P, pp. 197–213, 2003.
19. Pushpendu Kar, Sudip Misra,"Reliable and Efficient Data Acquisition in Wireless Sensor Network in the Presence of Transfaulty Nodes", IEEE Transactions on Network and Service Management, 2015.
20. S. S. McClure et al., “Radiation effects in micro-electromechanical systems (MEMS): RF relays,” IEEE Trans. Nucl. Sci., vol. 49, no. 6, pp. 3197–3202, Dec. 2002.
21. H. R. Shea, “Radiation sensitivity of microelectromechanical system devices,” J. Micro/Nanolithogr. MEMS MOEMS, vol. 8, no. 3, pp. 1–11, Jul. 2009.
22. I.F. Akyildiz, D. Pompili, T. Melodia, “Underwater Acoustic Sensor Networks: Research Challenges," Elsevier's Journal of Ad Hoc Networks, Vol. 3, Issue 3, pp. 257-279.
23. Liansheng Tan, Mou Wu,”Data Reduction in Wireless Sensor Networks: A Herachical LMS Predication Approach”, IEEE Sensors Journal, vol.16 No. 6, 2016.
24. J.Praiseline Karunya,T.Aruna ,“Performance Analysis of Energy-Aware Sensor Node Design in Wireless Sensor Networks”, International Journal of Electrical, Electronics and Data Communication, ISSN: 2320-2084 Volume.2, Issue-2, 2014.
25. Younis, O. and Fahmy, S., HEED: “A hybrid, energy-efficient, distributed clustering approach for ad hoc sensor networks”, IEEE Transactions on mobile computing, pp.366-379, 2004.
26. Mao Y, Chengfa L., “EECS: an energy efficient clustering scheme in wireless sensor networks,” IEEE international performance computing and communication conference; p.535–40, 2005.
27. Shigei, N., Miyajima, H., Morishita, H. and Maeda, M.,” Centralized and distributed clustering methods for energy efficient wireless sensor networks”, In Proceedings of the International Multi Conference of Engineers and Computer Scientists, Vol. 1, pp. 18- 20,March, 2009

AUTHORS PROFILE

K.R. Asha Department of Master of Computer Application, SSIT, Tumkur, India.

Dr.M.C. Supriya Department of Master of Computer Application, SSIT, Tumkur, India.