Security with Energy conservation by Triple Algorithmic Metrics in WSNs

***I.GayathriDevi, [1]Y.Aarti**

***Asst.Professor, Pragati Engineering College, Kakinada, India, igayathridevi9@gmail.com**

[1]Student, Pragati Engineering College, Kakinada, India, aarti533@yahoo.com

Abstract: A wireless sensor network is a network of a number of sensing nodes that perform a certain task. The WSN use tiny inexpensive sensor nodes with several distinguishing characteristics .So wireless sensor networks are becoming significantly vital to many applications and are experiencing an explosive growth. The key requirement of this technology is to provide adequate security, as one of the biggest concerns of WSNs is that they are defenseless to security. Communication security is essential to the success of WSN.So in this paper we focus on three algorithm tic metrics for WSN secure and energy conserved communication. The first algorithm tic metric is "Algorithm for network lifetime improvement and energy conservation". In this live and dead nodes are detected .Then clusters are formed from live nodes, among those one aggregated cluster node is selected. So communication will take place only through the live nodes. The second algorithm tic metric is "Algorithm for creating secure communication". Through this algorithm authentication and confidentiality is achieved. In this the concept of timestamp and compression are introduced for reducing size and increasing capacity. In this paper additionally we provide intrusion detection and prevention by using statistical behavior of the entities.

Keywords — Cluster, Aggregated Cluster node, Timestamp, Authentication, Confidentiality, Network lifetime, Intruder detection.

I. INTRODUCTION

A wireless sensor networks is a special type of network .It is a wireless network consisting of spatially distributed autonomous devices known as sensors to monitor different conditions. It in cooperates a gateway that provides wireless connectivity to distributed nodes and back to the wired world.

WSNs have many unique characteristics .So the security services in a WSN should protect the information communicated over the network. In this network a large number of sensor nodes are deployed for monitoring. However these nodes have severe resource constraints due to lack of processing power and limited energy.WSNs have high need to be equipped with security mechanism to defend against attacks as these networks are normally placed in remote places and left unattended.

In this paper we provide an approach for improving network lifetime and capacity and facilitate secure communication between ACNs

In the first phase clusters are formed by grouping physical live network nodes into small number of logical assemblies by applying cluster formation protocol [9]. These logical assemblies are known as clusters and the header obtained through header formation protocol is known as aggregated cluster node (ACN).

In the second phase assurance that the communication entity is one that it claims to be. Along with this the protection of data from unauthorized disclosure is done.

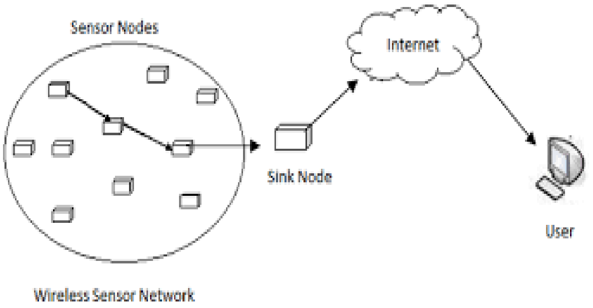

Fig1: Transmission of data through sensor nodes [6]

In this way data is securely communicated between ACNs'.

Since intruder is the main reason for security issues. The last phase deals with intruder detection and prevention.

Finally we conclude this paper by providing three algorithmic metrics to resolve the problems faced in wireless sensor networks.

DOI : 10.18231/2454-9150.2018.0561

II. PROPOSED ALGORITHM

A. Algorithm for network lifetime improvement and energy conservation

The steps are as follows:

1. The distance between the sensor nodes in the round time trip is considered as Round trip time (RTT).

2. The path with the highest RTT is taken as threshold.

3 If RTT is infinity there is a dead node in its path

4 If RTT < threshold then those nodes are treated as live nodes.

5 Now the live nodes are grouped into cluster, the farest node is selected as aggregate cluster node (ACN).

From 3 the dead nodes are identified and the transmission of data takes place only through live nodes.

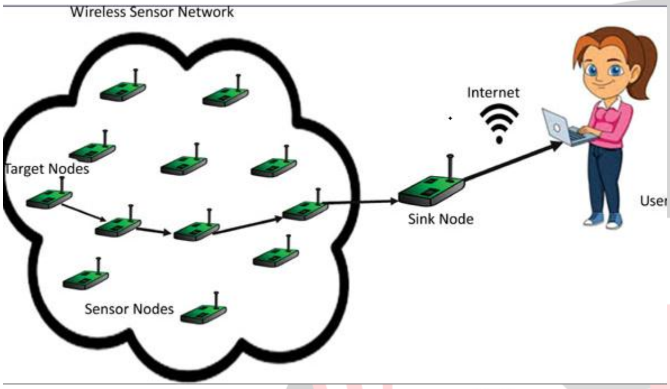

Fig2: Transmission of data through live nodes[16]

By forming cluster and ACNs the transfer between every node to other node is reduced which leads to conservation of energy.

B. Algorithm for creating secure communication

The following are the steps involved

1. Initially the sender and the receiver begin communication by exchanging ID+RS (Random Synchronization).[4]

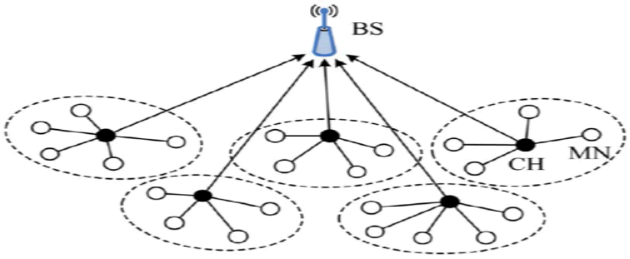

Fig2: Communication between Base station and Aggregated Cluster Nodes [8]

2. If synchronized communication between entities is established then exchange data through secure channel using the following steps

3. The message from the sender is digitally signed using DSS algorithm.

4.The message 'M'+ signature 'S' are encrypted using asymmetric public key cryptographic algorithm (ECC algorithm).

5.The encrypted data is compressed using ZIP algorithm for reducing the size of bandwidth and capacity.

6. The compressed data is attached with a timestamp (TS) and sent to receiver to avoid unauthorized interception of delays.

7. The receiver could verify the time stamp and unzip the code for decrypting the message along with verification of signature.

In this way authentication and confidentiality is achieved.

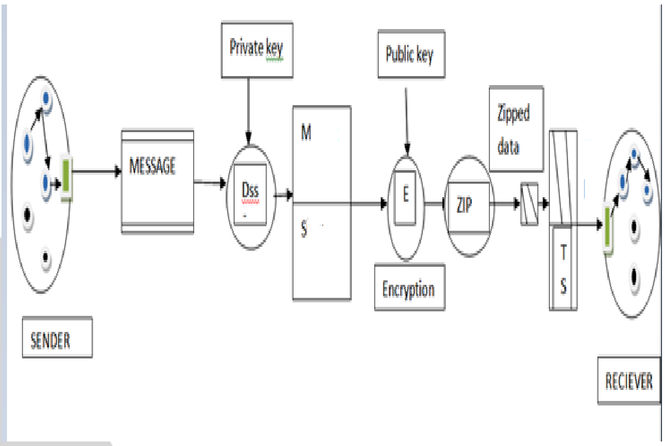

Fig3: Secured data transmission from sender

The total energy consumed by the sensor nodes for transmission (ETx) and reception (ERx) can be expressed as: Ec (u) = ETx (N; d) + ERx (N) [28]

The communication energy ETx and reception energy ERx are defined as follows:

$$ETx (N; d) = Eel \times N + eamp \times N \times (d2)$$

$$ERx (N) = Eelec \times N$$

The optimal linked state routing algorithm is used as routing algorithm between clusters [15]

C. Algorithm for detecting intruder

The following are the steps for detecting intruder

1.The behavior of each live node is stored in a buffer.

2. If the statistical behavior of node is greater than 3, the live node is termed as intruder; else the live node is normal user.

3. Broadcast the intruder information to the nodes in the cluster.

4. The information of intruder is passed to base station to broadcast to all clusters in the base station.

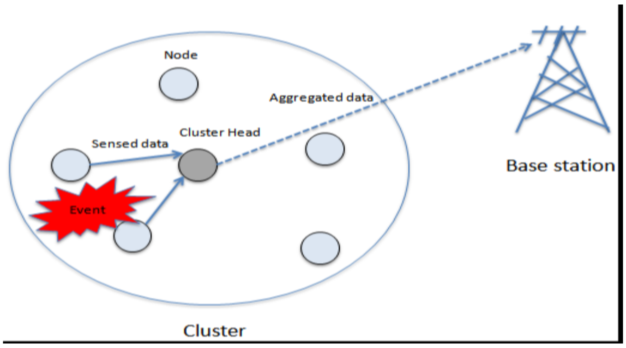

Fig 4: Intruder detection [11]

DOI : 10.18231/2454-9150.2018.0561

In the above figure intruder is termed as event .

5. The path of the intruder is identified and discarded, in this way intruder is prevented in the cluster.

III. CONCLUSION

Security aspects come into play when it is necessary or desirable to protect the information transmission from an opponent who may present a threat to confidentiality and authentication. In this paper we mainly focus on security issues along with network related issues. This improves the live nodes of network capacity and its secure data communication. [10]

REFERENCES

[1] RN. Duche, Nisha P. Sarwade, ”Sensor Node Failure Detection Based on Round Trip Delay and Paths in WSNs” IEEE SENSORS JOURNAL, VOL. 14, NO. 2, pp. 455-464, 2014.

[2] P. Jiang, ”A new method for node fault detection in wireless sensor networks” Sensors, vol. 9, no. 2, pp. 1282-1294, 2009.

[3] Detection of Faulty Sensor Node within Wireless Sensor Network for improving Network Performance Tejashree Phatak1*, S.D. Sawarkar

[4] Security to Wireless Sensor Networks with Network Capacity and Network Lifetime Requirement I.Gayathri Devi, M.Raja Kumar(PhD)

[5] M. Bhardwaj and A. P. Chandrakasan, “Bounding the lifetime of sensor networks via optimal role assignments,” in Proc. IEEE INFOCOM, New York, Jun. 23–27, 2002, pp. 1587–1596

[6] http://www.ijaiem.org/volume3issue3/IJAIEM-2014-03-27-108.pdf

[7] Zone-Based Clustering Approach for Separated Wireless Sensor Network Fields Boselin Prabhu SR* Department of Electronics and Communication Engineering, SVS College of Engineering, Coimbatore, India

[8] https://www.omicsonline.org/open-access/zonebased-clustering-approach-for-separated-wireless-sensor-network-fields-2332-0796-1000e117.php

[9] http://journals.sagepub.com/doi/full/10.1155/2012/301750

[10] http://index-of.es/Hack/Network%20Security%20Essentials%204th%20Edition.pdf [https://arxiv.org/pdf/1301.5065

[11] https://link.springer.com/content/pdf/10

[12] Science & Engineering Bhagwan Parshuram Institute of Technology Delhi, India. deepalivirmani@gmail.com

[13] Yick, Jennifer, Biswanath Mukherjee, and Dipak Ghosal. Wireless sensor network survey. Computer Networks-Elsevier52.12 (2008); 2292-2330.

[14] Al-Karaki, Jamal N., and Ahmed E. Kamal. Routing techniques in Wireless Sensor Networks: A Survey. Wireless Communications, IEEE 11.6(2004); 6-28.

[15] Akkaya, Kemal, and Mohamed Younis. A survey on routing protocols for wireless sensor networks. AdHoc Networks 3.3(2005); 325-349

[16] Afsar, M. Mehdi, and Mohammad-H. Tayarani-N. Clustering in sensor networs: A Literature survey.J.Network and Computer Applications 46(2014); 198-226.

[17] Pantazis, Nikolaos, Stefanos A. Nikolidakis, and Dimitrios D. Vergados. Energy Efficient Routing Protocols in Wireless Sensor Networks: A Survey. Communications Surveys & Tutorials, IEEE 15.2(2013); 551-591.

[18] Rault, Tifenn, Abdelmadjid Bouabdallah, and Yacine Challal. Energy Efficiency in wireless sensor networks: A top-down survey. Computer Networks 67(2014); 104-122

[19] Abbasi, Ameer Ahmed, and Mohamed Younis. A survey on clustering algorithms for wireless sensor networks. Computer Communications 30.14 (2007) ; 2826–2841

[20] Perrig, A., Stankovic, J., Wagner, D. (2004), “Security in Wireless Sensor Networks”, Communications of the ACM, 47(6), 53-57.

[21] Defence Advanced Research Projects Agency (13 Oct 2006) Defence Advanced Research Projects Agency Home [online], available:http://www.darpa.mil/index.html [accessed 13 Dec 06]

[22] C. Vu, R. Beyah, and Y. Li, “A Composite Event Detection in Wireless Sensor Networks,” Proc. IEEE Int’l Performance, Computing, and Comm. Conf. (IPCCC ’07), Apr. 2007.

[23] S. Uluagac, C. Lee, R. Beyah, and J. Copeland, “Designing Secure Protocols for Wireless Sensor Networks,” Wireless Algorithms, Systems, and Applications, vol. 5258, pp. 503-514, Springer, 2008.

[24] M. Luk, G. Mezzour, A. Perrig, and V. Gligor, “Minisec: A Secure Sensor Network Communication Architecture,” Proc. Sixth Int’l Symp. Information Processing in Sensor Networks (IPSN ’07)

[25] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, “Wireless Sensor networks: A survey,” Comput. Netw. (Elsevier), vol. 38, no. 4, pp. 393–422, 2002

[26] An energy efficient approach for routing in wireless sensor networks Maya M. Warriera*, Ajay Kumarb

[27] Akyildiz Ian F, Weilian Su, Yogesh Sankarasubramaniam and Erda Cayirci. Wireless sensor networks: asurvey. Computer networks 38.4(2002); 393-422.

[28] http://www.indjst.org/index.php/indjst/article/view/72334/64022

DOI : 10.18231/2454-9150.2018.0561