JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

TRIPPLE KEY ESTABLISHMENT FOR SECURE DATA TRANSIMIOSSION IN WSN

Nagendra Nath Giri[1]
Asst. Professor and Head, Dept of CS,
Govt, First Grade College for Women,
Hassan, Karnataka, India

Sumati Behera[2]
Asst. Professor, Dept. of CS,
Govt, Home science college,
Hassan, Karnataka, India

Abstract— ***In the developed field of information and communication systems, the utilization of wireless sensor networks (WSN) is greatly increasing. In WSN applications, data gathering with limited energy consumption and good security is essentially needed nowadays.. The nodes in WSN are vulnerable to several attacks and the data transmission scheme should provide network security. Unique key establishment mechanism to sustain the routing attack. Also, an efficient security algorithm is developed using the concept of triple key distribution where the three nodes share the common keys for the purposed of secure data aggregation. The algorithms were effectively calculated which shows that it can efficiently address the proposed issues to maintains better time and space complexity. An extensive evaluation has been performed where the outcome has been compared with the standard LEACH algorithm. The overall results have shown better energy saving and security management capabilities.***

Key words- ***Wireless sensor, data aggregation, routing attack, triple key.***

I. INTRODUCTION

Wireless sensor networks have attracted important attention in recent years [1] it is crucial to design wireless sensor networks that save energy, and thus, extends the network lifetime. As sensors are usually deployed in large numbers with high density, data aggregator plays an important rule to minimize the network load, and hence, reduce energy consumption [2]. For energy saving , m*any routing algorithms with data aggregator have been* proposed by allowing intermediate nodes to aggregate the data [3]. These protocols focus mainly on the energy-efficient routing and thereby assume that the transmission reliability can be supported by the underlying link layer protocol. However, wireless sensor nodes may often be deployed in coarse and inhospitable physical environments with temporary obstacles. Therefore, the packet error rate (including packet loss and packet error due to bit error) in sensor networks changes much more dynamically and is higher than other networks. In the harsh situation, the packet error rate may go up to 40 percent [4]. How to reliably deliver the sensory information to the sink in an efficient way is indeed a major challenge in such networks. Especially, in a data aggregator tree, unreliable transmission can result in momentary loss of sensor readings of the entire sub-tree. Node or link failures closer to the sink affect the reliability very drastically since data packets sent out by nodes near the sink contain much more information than those around the leaves.

In order to benefit from the energy saving due to data aggregator, we address the problem of offering desired reliability to fused information with minimum energy consumption. To increase the information reliability, the main idea of our scheme is to repeatedly transmit data on fusing routes without acknowledgments (ACKs). There are two benefits of this scheme. The first advantage is that it can work together with any data aggregator routing algorithm and also any aggregator function. The second advantage is that it does not need any ACK control mechanism, and hence, reduces the latency of data delivery. The key challenge here is how to compute the optimal number of transmissions for each node to minimize the total energy consumption.

II. RELATED WORK

This section discusses about all the prominent research work being explored from the literature that claims issues in data aggregation and key establishment to enhance the security in wireless sensor network.

Fan e.t. al [5] have discussed multi-target tracking by considering LEACH as the routing protocol for data aggregator, and FCM Algorithm to do association in cluster heads. The results shows that miss association, missing new target and repeated tracking are avoided and the tracking effect is very well.

Chen [6] proposed a new algorithm named FCM (Improving Life Time of Wireless Sensor Networks by Using Fuzzy c-means Induced Clustering). The author divides all nodes into Q clusters by the Fuzzy c-means algorithm and chose the cluster head according to the node's energy and the distance between the center position of each cluster and base station in the first round.

Xu e.t. al. [7] have proposed a revised cluster routing algorithm named E-LEACH to enhance the hierarchical routing protocol LEACH by considering the remnant power of the sensor nodes in order to balance network loads and changes the round time depends on the optimal cluster size. The simulation results show that the protocol increases network lifetime at least by 40% when compared with the LEACH algorithm.

Tan e.t. al. [8] have developed an analytical framework to explore the fundamental limits of coverage of large-scale WSNs based on stochastic data aggregator models. To characterize the inherent stochastic nature of sensing. The main focus of this paper is to investigate the fundamental scaling laws between coverage, network density, and signal-to-noise ratio (SNR).

Hamzeh [9] have proposed a fuzzy processor to be in charge of performing fuzzy instructions. This processor is applied to track the best path online for forwarding packets instead of traditional offline table based forwarding process. Simulation results show the numerous efficiency of our methodology not only in balancing the power dissipation through network, but also in lifetime improvement, traffic management, and network availability.

Data Aggregation

Due to high node density in sensor networks same data is sensed by many nodes, which results in redundancy. This redundancy can be eliminated by using data aggregation approach while routing packets from source nodes to base station. Data aggregation usually involves the fusion of data from multiple sensors at intermediate nodes and transmission of the aggregated data to the base station (sink).

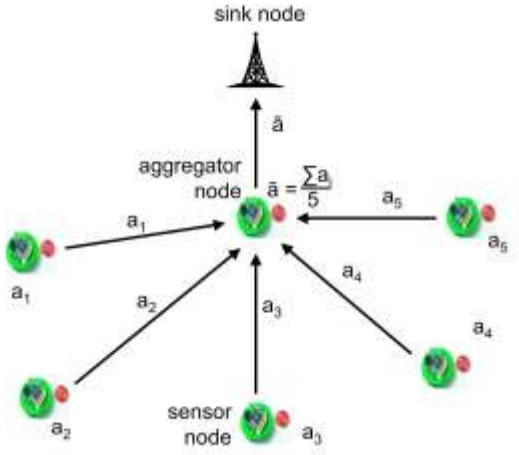

Figure 1 Data Aggregation Phenomenon

The algorithm uses the sensor data from the sensor node and then aggregates the data by using some aggregation algorithms such as centralized approach, LEACH(low energy adaptive clustering hierarchy) [10], TAG(Tiny Aggregation) [14] etc. Data aggregation protocols aims at eliminating redundant data transmission and thus improve the lifetime of energy constrained wireless sensor network. In wireless sensor network,

III. Secure Key Distribution Schema

The main goal of the security measures of the proposed system is to design a framework using the concept of triple key distribution. In this system the three nodes share a common keys for the purposed of secure data aggregation. A pairwise and triple pairwise key distribution is proposed that ensure secure and reliable data transmission among the entities of WSN. The system uses 128 bit key size chosen from key-pool. Therefore, a pairwise key distribution ensures secure communication between 2 nodes while triple key pairwise distribution insures secure communication between Nodes, cluster-node, and base station. Therefore, an optimal secure environment is achieved even before or at the point of initiating the data aggregation process. The prime purposes of the proposed system are as following:

- To propose a new pair-wise key pre-distribution scheme using combinatorial structures for the purpose of collusion attacks.
- To introduce a novel concept of triple key distribution in sensor networks in which every three nodes share a common key.
- To establish pairwise or triple key simultaneously among sensors.
- To apply triple key distribution to secure forwarding and key management in clustered sensor networks for secure data aggregation.

At the beginning, each node is preloaded with a set of identifiers of nodes chosen at random. For each of these identifiers, a pair-wise key is also loaded in the node. After deployment, two nodes can interact each other securely provided they have a pair-wise key. In a static network, nodes can be deployed in such a way that they share pair-wise keys with their neighbors. However, in a dynamic network, new neighbors might not have pair-wise keys to communicate with each other. Pair-wise schemes are preferred over other schemes because of increased security.

V) Algorithm for Pairwise key distribution algorithm

Input: WSN Parameters

Output: Pairwise keys Generation

Steps:

START

1. Define Area of Simulation
2. Initialize x and y Coordinates of the Sink randomly
3. Number of Nodes in the field
4. Optimality of a node to become Aggregator Node
5. Initialize Data Aggregation Energy
6. Initialize Maximum number of Simulation Rounds
7. Creation of the Random Sensor Network Deployment area.
8. Initialize identifier of Node-A: Id_{nodeA}: (p_1, q_1, r_1)
9. Initialize identifier of Node-B: Id_{nodeB}: (p_2, q_2, r_2)

//Add Node-C with Id_{nodeC} (p_3, q_3, r_3) for triple key pairwise distribution (TKPD)

10. If r_1= =r_2 //For TKPD, cond. Is r_1= =r_2= =r_3
11. No common key Explored;

12. Else

13. y=((p1-p2)2+4(q1-q2))mod q

14 If sqrt(y) exists

15 $$x_1 = \frac{(p_1 - p_2) + \sqrt{r_1}}{2} (\text{mod } q)$$

16. $$x_2 = \frac{(p_1 - p_2) + \sqrt{r_1}}{2} (\text{mod } q)$$

17. If $x_1<k$ && $x_2<k$

18. $X_{AB}=K(x_1,x_1i+j)|| K(x_2,x_2i+j)$

19. $Key_{AB}=hash(X_{AB}||id_{nodeA}||id_{nodeB})$

//For TKPD, $Key_{ABC}=hash(X_{AB}||id_{nodeA}||id_{nodeB}||iD_{nodeC})$

20. Return Key_{AB}.

21 Else

22. No Common key

23. End if

24. Else

25. No Common Key

26. End if

27. End if.

28. Flag for registering first dead node

29. If energy of node is more than zero

30. Generate random number between 0 to 1

31. Election of Cluster Heads

32. Cluster count increases

33. Calculate distance between cluster head and Sink

34. Save the distance from BS

35. Save the cluster IDs

36. Compute Energy dissipated

37. Perform Secure Data aggregation

END

Figure 2 shows the result accomplished after performing the simulation study to see that the processing time of the proposed system is highly optimized while maintaining a better uniformness in the processing time. The modified usage of hash function using either SHA1 or MD5 is used for performing sender ambiguity for which literally no keys are stored in any database. The keys are generated, released, used, and eroded to make the processing time quite faster.

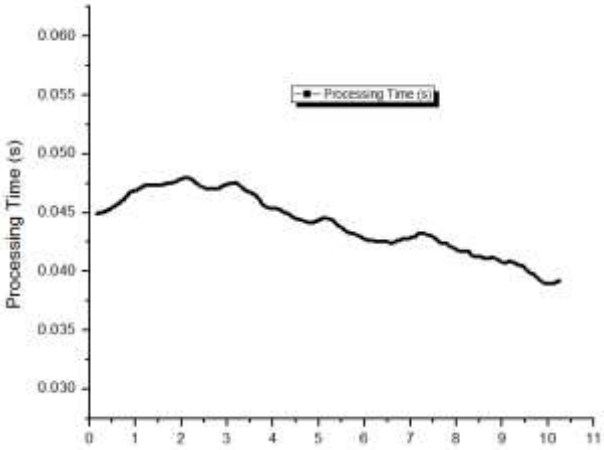

Figure 2 Analyzing Processing time

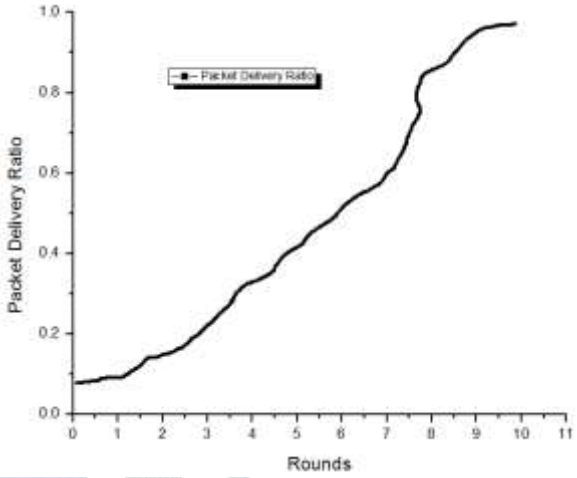

Figure 3. Analyzing Packet Delivery Ratio

Figure 3 highlights the results accomplished from the simulation study that analyzes packet delivery ratio. Another interesting fact noted from this study is that although the traditional radio model of WSN is deployed in the proposed system, the proposed algorithm are actually built on the top of the efficient algorithm scheme known as Elliptical Curve Cryptography and Elgamal Signature Scheme which maintains total confidentiality of source sensor node.

IV. COMPARATIVE ANALYSIS

Depending on the above considered simulation parameters, the proposed protocol is executed and compared with the most famous LEACH protocol . Figure 4 highlights the quantity of alive nodes using the proposed protocol as well as LEACH protocol where it is very obvious that the proposed technique outperforms the LEACH protocol. It can be seen that in LEACH protocol, number of alive nodes starts stiff descent whereas the proposed protocol too has gradual and smooth descent. The results show that proposed protocol can ensure maximization of cumulative lifetime of the wireless sensor network with the proposed key distribution scheme.

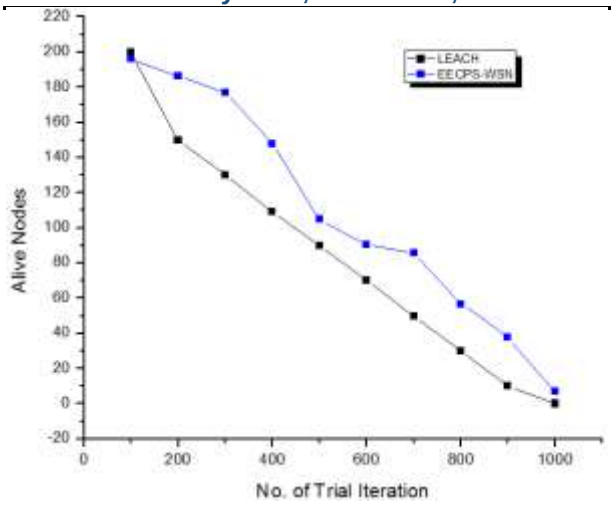

Figure 4. Performance Comparision for Alive nodes Vs. Iteration Trials

For analyzing the power efficiency of the proposed system with LEACH protocol, it is critical for considering the parameter of First Node Death (FND) in order to visualize and compare the efficiency of our algorithm for maximizing the cumulative network lifetime.

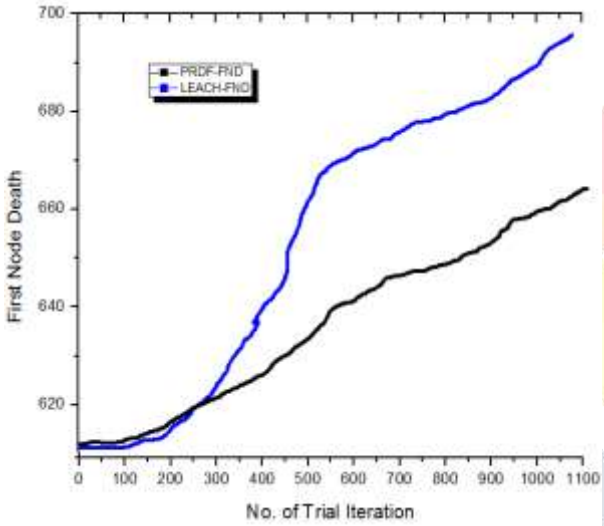

Figure 5. First Node Death values for proposed and LEACH protocols

From Figure 5, it can be seen that the proposed technique actually assist the sensor motes to utilize the power in more consistent pattern. It can also be said that power assigned to the sensor motes in traditional LEACH protocol is often deflects with certain motes with very high power allocation while some are drained of power to zero joules. But it can be seen that in proposed system has overcome the above mentioned issues in LEACH protocol. In LEACH protocols, the motes were running out of power in around ~660 rounds, while in proposed system, the power drained out near to ~ 690 rounds in approximation.

Energy plays very important role in designing routing schema for wireless sensor network where it can be explored that LEACH is one of the famously used mechanism in clustering as it chooses cluster leader depending on non-deterministic model. LEACH is purely based on non-deterministic framework where certain clusters may be very close to each other and can be located in the edge of the WSN. However, the energy efficiency cannot be maximized using these in-efficient cluster leaders. The proposed technique has introduced a protocol that is designed to overcome the issues in LEACH using non-deterministic Logic and selecting energy level.

V. CONCLUSIONS

The proposed schemes have benefit over other pair wise key schemes in terms of security and bandwidth requirements, which is applicable to both static and mobile networks. The proposed system is categorized into pre-stage and post-stage of data aggregation. The framework has been designed to study the triple key distribution in sensor networks, and applied it in secure routing, in clustered sensor networks. After deployment, two nodes can communicate securely provided they have a pair-wise key. In a static network, nodes should be deployed so that they share pair-wise keys with their neighbors. However, in a dynamic network, new neighbors might not have pair-wise keys to communicate with each other. Pair-wise schemes are preferred over other schemes because of increased security. In collusion attacks, an adversary might gather the information from many nodes to construct the pair-wise keys of the uncompromised nodes. In scenarios such as secure data aggregation and secure routing, an efficient session key needs to be established between two nodes. Pair-wise key distribution is a very effective and efficient way of establishing common key.

REFERENCES

[1] A,F.Ian, V.M.Can, "Wireless Sensor Networks", *John Wiley & Sons, 10-Jun-2010 - Technology & Engineering ,pp.520,2010*

[2] G.Elena, B.L.James, A. Michael, G. Lewis, "Wireless Sensor Networks: Deployments and Design Frameworks", *Springer,pp.306, 2010*

[3] I. Akyildiz, W. Sankarasubramaniam, E.. Cayirci " Survey on Sensor Networks," *IEEE Comm. Magazine, vol. 40, no. 8, pp. 102-114, 2002*

[4] S. Lindsey, C.S. Raghavendra, "Pegasis: Power-Efficient Gathering in Sensor Information Systems", *Proc. IEEE Aerospace Conf., 2002*

[5] L. Fan, H. Wang, H. Wang, "A solution of multi-target tracking based on FCM Algorithm in WSN", *IEEE International Conference on Pervasive Computing and Communications Workshops, 2006*

[6] J. Chen, "Improving Life Time of Wireless Sensor Networks by Using Fuzzy c-means Induced Clustering", *IEEE-2012*

[7] J. Xu, N. Jin, X., Lou T, Peng, Q. Zhou, Y. Chen, "Improvement of LEACH protocol for WSN", *9th International Conference on Fuzzy Systems and Knowledge Discovery, 2012*

[8] R. Tan, G. Xing, B. Liu, "Exploiting Data Aggregator to Improve the Coverage of Wireless Sensor Networks", *IEEE/ACM transactions on networking, vol. 20, No. 2, 2012*

[9] M. Hamzeh, S. Arab, S. M. Fakhraie, C. Lucas, "An Improvement on LEACH Algorithm with a Fuzzy Processor", *Proceedings of APCC2008, 2008*

[10] D. L.Peter, G. Dongbin, "A Survey of Deterministic Vs. Non-Deterministic Node Placement Schemes in WSNs", *The Sixth International Conference on Sensor Technologies and Applications, SENSORCOMM ,2012*S.