IJRRECS/August 2013/Volume-1/Issue-4/444-448 **ISSN 2321-5461**

INTERNATIONAL JOURNAL OF REVIEWS ON RECENT ELECTRONICS AND COMPUTER SCIENCE

A PROJECT REPORT ON SECURITY SCHEME BASED THREE TIER SYSTEM

T.Sanjeev Kumar[1], S.Soujanya[2], G.Charles Babu[3]

[1]M.Tech Student, Dept of CSE, Holy Mary Institute of Technology & Science, Keesara, R.R Dist, A.P, India

[2]Assistant Professor, Dept of CSE, Holy Mary Institute of Technology & Science, Keesara, R.R Dist, A.P, India

[3]Professor & HOD, Dept of CSE, Holy Mary Institute of Technology & Science, Keesara, R.R Dist, A.P, India

ABSTRACT:

Applications related to sensor network based wireless communication system a vital role played by the mobile sinks includes accumulation of the efficient data, Local programming based sensor and sensors are compromised based on the differentiation. Here establishment of key in a pair wise manner followed by the data authentication among mobile sinks and nodes based on the sensor. Here a new challenge based security scheme is employed. A probability based scenario with a key based on the Q factor scheme distribution takes place. By the nodes gets captured the hacker can get the security pass word easily. A new strategy is described based on the three tier scenario which gets allowed for the keys usage of a pair wise distribution. It got decomposed into two main aspects one is for establishment of the key and the other is for the network access respectively. Attacks related to the replication node based stationary access got reduced by the setting a priority based on the authentication between the stationary node followed by a sensor. Therefore on experimental analysis it proves that our proposed method is effective than the existing techniques with improving the performance of the system.

Keywords: Sink mobile, Network oriented wireless sensor, Security analysis, Privacy control, Data distribution.

1. INTRODUCTION

As the increase in technology related to the electronic field there is a huge requirement of the network based on wireless sensor nodes to be developed which mainly relies on nodes based on power accumulation low with reduced cost. Here there is no channel in this wireless environment but the transmission of the data place by the help of interdependent nodes [1]. Initially a route is established and beyond the route activation of the nodes takes place and which acts as the data transmitters to the final destination by the help of the power oriented phenomena. And some of the applications includes Tracking and sensing of military, Monitoring health, Capture of data in ill environments and Monitoring of habitat respectively [2][3]. For the computation purpose base station receives the data. For the purpose of the large distance communication multi hop is used but the degradation of the privacy strength takes place by this power loss is more and lifetime of the system is degraded. Here the sensor node of the mobile oriented phenomena are useful for the collection of the data, Programming based on the localization, Navigation, Military, Space, Collection of oceanography data respectively. Here networks based on the sensor plays a critical role for the transmission of the data through wireless environment respectively [5][6]. And the services based on the security includes Privacy, Mobiles and sensor node are separated by the key. Here the transmission of the data takes place in this technology are with oriented with privacy followed by the authentication respectively [7].

BLOCK DIAGRAM

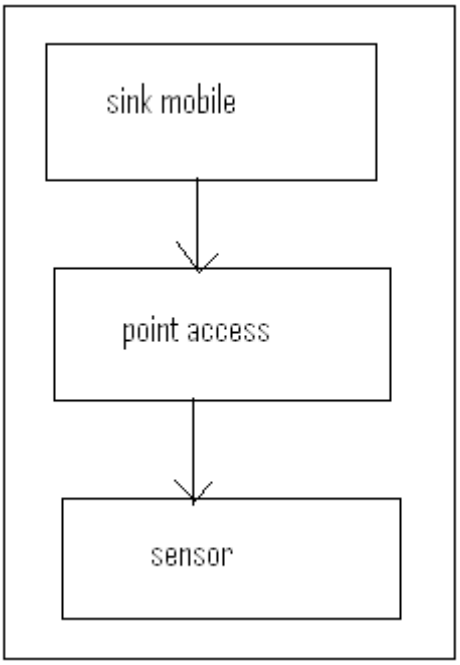

Fig 1: Shows the block diagram of scheme oriented privacy based three tier phenomena

2. METHODOLGY

In this particular paper the main challenge is to overcome the drawback or the associated problem of the managing key. Most of the several existing techniques are suffered from this drawback. So in order to overcome this problem a designed strategy is implemented based on the pre distribution [4][8]. As the keys are randomly distributed for each and every node in the network and the data transmission has been started so if any of the similarity key takes place then both of the nodes has to share the similar key. But this is not a successful method and after this Q based method is implemented and it is also not successful in the scenario of management of data. So here in order to overcome this problem a system or the technique is designed by the name three tier [9].

Three tier:

This is built by the method of scheme based blundo. Where it gives complete assurance over the entire network regarding the security oriented phenomena. This is mainly used for the enabling the system related to security aspect. It is differentiated into two parts They are poll based on the mobile and the pool based on the static oriented phenomena. One is used for providing data authentication where the network oriented sensor is accessed and the other is for the key authentication. Here compulsorily each and every node is accessed with secrete sharing key where in order to overcome the drawback of the previous techniques [10]. Here accessing of the keys and also the security oriented phenomena and its distribution lies everything in the hands of the polynomial.

3. EXPECTED RESULT

A lot of research has been conducted on the present method which has to work effectively and efficiently in order to overcome the drawback of the existing method. There is a huge challenging task related to the security based phenomena is a primary role where several existing techniques are failed to overcome that particular problem. So here a polynomial based implementation is done where it plays a key role in providing security oriented phenomena between the nodal networks respectively. And this particular key is distributed randomly in the entire nodal network where each and every node has to pick separate key and whereas in the existing techniques same key is pick by the similar nodes. That is the difference here . This polynomial phenomena is implemented in the

proposed method by the name three tier. Therefore this system is designed in a effective manner in a several number of the datasets. And a comparative analysis is made with respect to the present method to that of the several other existing techniques. Here the practical experiments are also been conducted and its empirical values are plotted in the below graph and shows the variations between the present method to that of the several other existing methods and quite effectively the performance of the system is evaluated.

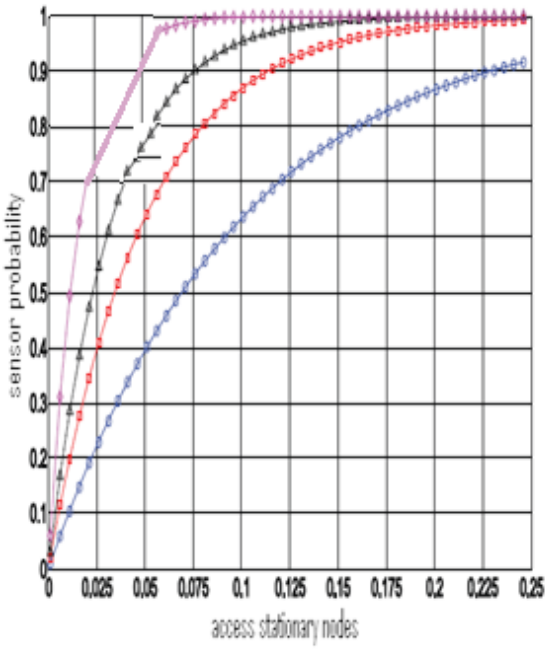

Fig 2: Shows the graphical representation of the access nodes to that of probability

4. CONCLUSION

Here the main intention of the paper is to work on the security based aspect followed by the protection of the data of the user based on the malicious attacks in the form of the hackers. So for the implementation an algorithm by the name three tier based phenomena is designed in a quite efficient and effective manner in order to improve the performance of the system. Actually the main problems of the previous methods are they are unable to overcome the problem related to key based aspect. This is a major problem and got failed to overcome this problem. Here in order to overcome this problem our present approach started implementation of the polynomial based phenomena here. Where it is concerned with respect to the nodes and they have to be completely protected with separate key. No two nodes have the same key. Then after classifies into mobile and static based on the polynomial scenario. In order to transmit the data effectively in the network oriented nodal plane of wireless communication. Here there is no channel complete transmission of the data takes place by the activation of the nodes where less power consumption followed by the less cost. In the above process system plays a efficient role and improves the performance.

REFERENCES

[1] W. Zhang, G. Cao, and T. La Porta, "Data Dissemination with Ring-Based Index for Wireless Sensor Networks," Proc. IEEE Int'l Conf. Network Protocols (ICNP), pp. 305-314, Nov. 2003.

[2] L. Eschenauer and V.D. Gligor, "A Key-Management Scheme for Distributed Sensor Networks," Proc. ACM Conf. Computer Comm. Security (CCS '02), pp. 41-47, 2002.

[3] H. Chan, A. Perrig, and D. Song, "Random Key Pre-Distribution Schemes for Sensor Networks," Proc. IEEE Symp. Research in Security and Privacy, 2003.

[4] D. Liu, P. Ning, and R.Li. Establishing, "Pairwise Keys in Distributed Sensor Networks," Proc. 10th ACM Conf. Computers and Comm. Security (CCS '03), pp. 52-61, Oct. 2003.

[5] H. Chan, A. Perrig, and D. Song, "Key Distribution Techniques for Sensor Networks," Wireless Sensor Networks, pp. 277-303, Kluwer Academic, 2004.

[6] D. Liu and P. Ning, "Location-Based Pairwise Key Establishments for Static Sensor Networks," Proc. First ACM Workshop Security Ad Hoc and Sensor Networks, 2003.

[7] S. Zhu, S. Setia, and S. Jajodia, "LEAP: Efficient Security Mechanisms for Large-Scale Distributed Sensor Networks," Proc. 10th ACM Conf. Computers and Comm. Security (CCS '03), pp. 62-72, Oct. 2003.

[8] A. Rasheed and R. Mahapatra, "An Efficient Key Distribution Scheme for Establishing Pairwise Keys with a Mobile Sink in Distributed Sensor Networks," Proc. IEEE 27th Int'l Performance Computing and Comm. Conf. (IPCCC '08), pp. 264-270, Dec. 2008.

[9] A. Rasheed and R. Mahapatra, "A Key Pre-Distribution Scheme for Heterogeneous Sensor Networks," Proc. Int'l Conf. Wireless Comm. and Mobile Computing Conf. (IWCMC '09), pp. 263-268, June 2009.

[10] L. Lamport, "Password Authentication with Insecure Communication,"Comm. ACM, vol, 24, no. 11, pp. 770-772, Nov. 1981.