Real Time Activity based Pre-key Distribution in three tier security schemes in Wireless Sensor Networks

B.Sangeetha & Mrs.Radhimeenakshi
Tiruppur Kumaran College For Women
Assistance Professor in ComputerScience Department

***Abstract*- Guaranteeing continuous, trusted activity in a wireless sensor network (WSN) is a never an easy task. Ensuring a sensor in a network grid architecture with respect to hardware failure and effects of environment changes is always expensive in terms of computational and energy expenditure. In this paper we propose a real time sensor activity based pre-key distribution in three tier security schemes in wireless sensor networks. Assuming a senor node is active and initiation the pre-key distribution is meaningless in a WSN. In order to identify the activity of the sensor node or a sensor failure, a real time tracking of sensor node properties are weighed before. This real time tracking benefits in identifying the level of application faults.**

I. INTRODUCTION

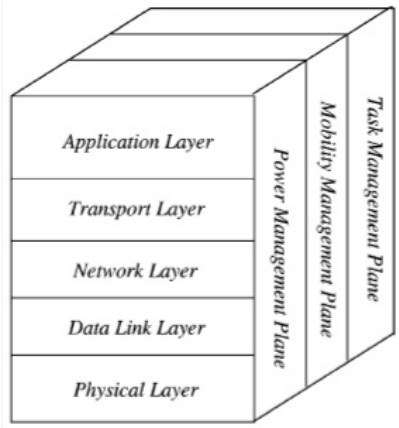
A wireless sensor network (WSN) might contain hundreds or thousands of sensor nodes, each employed for different tasks like, sensing, computing, and communicating with various devices. In a demographic monitoring sensor, the primary goal is to collect geographical information and to send the data to the mobile sink. In WSN the nodes are mobile and it is hard to establish its nature. In the worst case, even we cannot predict the next minute that the senor node might be working or degraded or even faulty. This give arise to necessary to make sure that a sensor node is alive or not.

Malfunction or Failure

Constant innovation on sensors nodes and micro processors led to achieve effective processing, wireless communication, battery life, data transfer, and detection capabilities. Now every sensor is improvised in such a way to process and transmit data to its base station in terms of shorter duration, high data capturing, enhanced data processing etc. Recently lots of algorithms are developed to detect a senor node performance. A sensor node state can be classified into many types based on their present state, like hardware problem, energy drop, compromised in situations of intrusions, or even a complete failure. To this aspect of identifying the current state of a sensor node, a large level of real time application monitoring systems is utilized in common.

II. Related Works

Several works have addressed the problem of how to deal with faults occurring in wireless sensor networks in order to achieve fault tolerance [3][4][5]. There are several researches held to constantly monitor the activity and the state of a sensor node and also its impact on the severity of the failures in the application level. Mean time to repair is applied in indentified faulty sensors to reestablish its state. And sensor nodes crossing the threshold time are ignored or termed as comprised depending on the level of application. A fault map [4] was constructed using a fault estimation model. In order to build the fault map, sensor nodes are required to send additional information that can be used by the fault estimation model. Furthermore, a cluster based algorithm to estimate faults in wireless sensor networks was proposed. In [5], a target detection model for sensor networks was proposed. In addition, two algorithms to facilitate fault tolerant decision making were presented. The first algorithm is based on collecting the actual readings from the neighboring nodes. In the second algorithm, the sensor node obtains the decisions made by the other neighboring nodes to take a final decision. A distributed cluster based fault tolerant algorithm is proposed in [6].

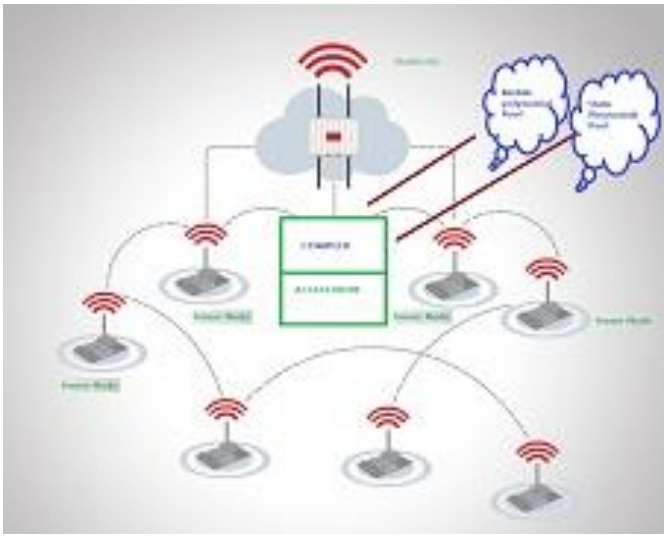


WSN mainly face the problem of mobile sink replication attack. To overcome this problem A. Rasheed [8] proposed a three tier security framework for authentication and pair wise key establishment, based on polynomial pool based key pre-distribution scheme [7]. This technique was able to give network resilience to mobile sink replication attacks. They had preselected sensor nodes as stationary access nodes, which acts as authentication access points that are capable of making the sensor nodes to send their data to mobile sinks. They use two separate polynomial pools: a mobile polynomial pool and a static polynomial pool.

III. PROPOSED WORK

Our proposed work provides a unique approach to identify the state of the sensor node in real time. The state of the node does not mean the physical state of the sensor node but also its quality of function, i.e., a node is failed or not. In other words, we make sure the node is functional in

application of three tier security grid based on mobile and static polynomial pool. Once the sink in the WSN has identified the quality of the sensor, it resumes the data capturing and the transmission process. To achieve this, the sink sends a signal and records state of the sensor node in real time. This ideally stores the state of the sensor node to a meantime of the desired level and refreshes the state once the application level of processing of pre-key based three tier security grid systems in WSN.



Real time Sensor Node Activity

IV.DESIGN AND IMPLEMENTATION

The proposed system of identifying the real time status of a sensory node is to collect the maximum information to establish that the node is stable and alive. The deduction method is based on facts that the sensor node is in line with the corresponding other sensor nodes within the boundary of that place. The basic concept of identifying the fault nodes is to split the node into memory part and redundancy part. The memory part is used to store the information and the redundancy part stores the data for recovery and fault management.

A compiler is used to gather information from the sensor node and transmit the data to the mobile sink. The compiler is more powerful in energy storage, computing and routing features. The compiler is the trusted relay node to the sink and act as a cluster in terms of large volume of nodes. If a fault is detected in the senor, the node stops the compiler to transmit any tasks to the sensor node. It is understood that the clusters are grouped based on the region to balance the loss of data transmission if there are any failures in the complier. In general it is assumed that there are at least two relay nodes in the cluster whenever a task is transmitted to the sensor node. The three tier grid based security scheme is approached throughout the study.

V. 3-TIER SECURITY SYSTEM

To implement a three tier security system, we establish a mobile pool which is between the access nodes and mobile sink and a static pool between the access nodes and sensor nodes. In the study we are making use of Grid architecture along with the mobile polynomial pool. Similar to the Three Tier Security Scheme, this also makes use of the one way hash chain algorithm along with static based polynomial pool [9]. This system overcomes the problem of Three Tier Security framework by introducing a grid communication between the mobile sinks and access nodes. This Grid will give the correct polynomial by which the communication can takes place, then there is no need of searching for the polynomial shares. This technique can reduce the communication overhead.

While deploying a three tier security system between mobile polynomial pool and static polynomial pool, the pre-key distribution techniques is processed only when the sensor node is alive. When failure nodes are identified, the computation process is not initiated or in other words, no task is assigned.

VI. RESULT

Once the sensor node state is functional and pre-key distribution is initiated this is termed as distribution phase. During this phase the query is sent through the network and the data gathering is constructed, this is done through reading of senor nodes in WSN. In the data gathering process, two streams of components are employed, namely data transmission and queue management. Data transfer is to transmit the data and queue management is to identify which messages are to be transmitted or dropped in case of faulty nodes. Based on the Reponses from the sensor node, the results are classified into Positive, Positive and Negative, Positive and retreat.

Positive- Nodes that is active and alive sends only one message

Positive and Negative- Nodes sends Positive for alive and negative for sleep

Positive and Retreat- Nodes that switch from alive to sleep and send one retreat message

REFERENCES

[1] A.A.Taleb, D.K. Pradhan and T. Kocak, "A Technique to Identify and
Substitute Faulty Nodes in Wireless Sensor Networks," Third International Conference on Sensor Technologies and Applications, 2009. SENSORCOMM '09., pp.346-351, 18-23 June 2009.

[2] A. Mainwaring, Culler, D. Culler, J. Polastre, R. Szewczyk and J.Anderson , “Wireless Sensor Networks for Habitat Monitoring,” First ACM Workshop on Wireless Sensor Nerworks and Applications, Atlanta, Georgia, USA, Sept 2002.

[3] Y. Zou and K. Chakrabarty, “A Distributed Coverage and connectivity Centric Technique for Selecting Active Nodes in Wireless Sensor Networks,” on IEEE Trans. on Computers, vol. 54, no. 8, pp. 978-991, Aug 2005.

[4] Yue-Shan Chang; Tong-Ying Juang; Chih-Jen Lo; Ming-Tsung Hsu; Jiun-Hua Huang, "Fault Estimation and Fault Map Construction on Cluster-based Wireless Sensor

Network," . IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing, 2006, vol.2, no., pp.14-19, 5-7 June 2006.
[5] T. Clouqueur, K.K. Saluja, P. Ramanathan, "Fault tolerance in collaborative sensor networks for target detection," Computers, IEEE Transactions on , vol.53, no.3, pp. 320-333, Mar 2004.

[6] Yongxuan Lai; Hong Chen, "Energy-Efficient Fault-Tolerant Mechanism for Clustered Wireless Sensor Networks," Proceedings of 16th International Conference on Computer Communications and Networks, 2007. ICCCN 2007., vol., no., pp.272-277, 13-16 Aug. 2007.

[7] 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.

[8] Sanjay Kumar, Deepti Dohare and Mahesh Kumar "An Efficient Key
Distribution Scheme for Wireless Sensor Networks using polynomial based
schemes" 2012 International Conference on Information and Network
Technology (ICINT 2012).

[9] Three Tier Security Schemes In Wireless Sensor Networks With Mobile Sinks Using Grid., International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 10, October 2013