Intl J Engg Sci Adv Research 2015 Sep;1(3):168-173

A Survey of Energy Efficient & Secured Data Aggregation in WSN

Sandeep Singh
CSE Department
Rama University,Kanpur, U.P.
er.sandeepkanpur@gmail.com

Hari Ji
CSE Department
Rama University,Kanpur, U.P.
jihari@gmail.com

***Abstract*— Wireless sensor networks (WSNs), feeling process and to communicate important information to the base station that the resource-starved deployed sensor nodes are made of. The communication cost always much higher than the cost of data processing is being done on the one hand and on the resources of sensor nodes because of lack of timely, WSNs generally, effectively reducing the overall number is on the network, processing, employment packet finally transmitted to the base station. The Network Processing substantially further transmission of data in a compact representation that the operation of the data collection employed. However, ubiquitous and pervasive deployment, security protocols and WSN nodes because of lack of resources to the stringent demands enormous resources, WSNs are important otherwise the security concerns. A data aggregator node in production depends on various other nodes when using the data aggregation of these concerns assumes dangerous proportions. Therefore, for data aggregation protocol carefully to ensure the security of the data is to be ready with a constant monitoring. To ensure secure data aggregation, based on our survey of current research efforts in this paper, we secure data aggregation in wireless sensor networks for the confidentiality, integrity and availability to achieve identical encryption and digital signatures, using a novel additive the approach proposed.**

I. INTRODUCTION

Wireless sensor network is formed by a large number of sensor nodes. Sensor nodes can be homogeneous or heterogeneous. These networksarehighlydistributedandthere are a numberoflow cost, low power, low memory and self-organizing sensor nodes are coupled. Sensing unit, processing unit, transmission unit, and power unit sensor nodes [1], etc. The sensor nodes are four main units, such as temperature, pressure, vibration, motion, humidity, sound-sensing capability. To listen the event, the programmed sensor nodes. If an event occurs, then the end point informed by generating wireless traffic sensors or sink node [2,3,4]. The number of sensor nodes in wireless sensor network congestion increases the likelihood of occurrence increases as. Forest monitoring, manufacturing, forecasting systems, military surveillance, health, home, office and many intelligent and smart systems like surveillance WSN applications are different. The energy consumption, communication helps to minimize overheads and tries to reduce local congestion problems, because the data aggregation in wireless sensor networks is an important technique. It is useful to collect data from the sensor nodes and end nodes or sink node allows transmitting useful data [4,5].

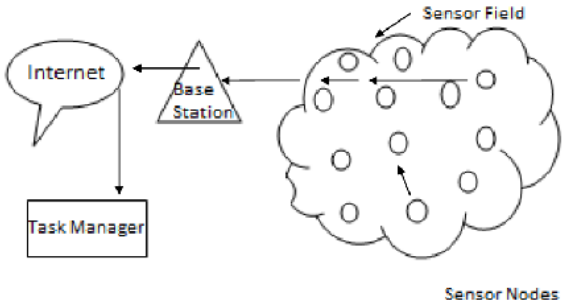

Fig. 1. Communication rctecture of wsn

II. ROUTING MODEL

We focus our attention on a network flow that Efforts are considered to consist of a single data sink. Data from a number of sources to gather information.

We start with a simple model of route plans Using data aggregation (which we term data-centric), and who plans (which we focused word address). In we assume some common elements in both cases -A query to the first data sink / interest sends out a sensor which then responds with the appropriate data nodes Data. They differ on the way data is sent to sync sources [6,7]:

A. Address centric protocol (AC)

A source independently at least along the path passes on the data to sync Questions have taken that route ("end-to-end path").

B. Data-centric protocol (DC)

Sending data sources To sink, but look at the content path routing nodes And perform some form of data aggregation. The data on multiple consolidations function Sources.

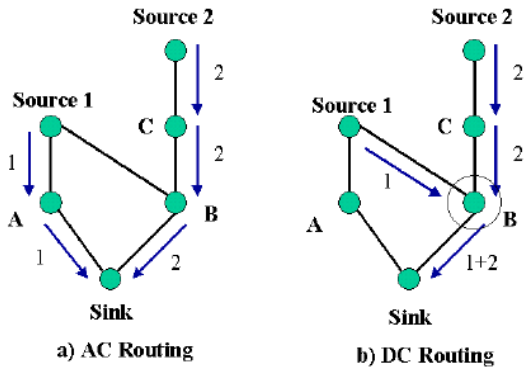

Fig. 2. Illustration of AC versus DC routing

Fig2 is a simple example of the difference between AC and DC schemes. Address centric approach, Sends its information separately for each source (Source 1 data through node "1" label route sink A, and the source 2 data nodes through the "2" label route C & B). The data-centric approach, data two sources have been collecting in Node B, and the United Data (labeled "1 + 2") is sent from B to sink. Last Energy savings results in lower transmission are required as to send information from both sources Sink [8].

III. Energy Efficiency

Wireless sensor networks consist of many sensor nodes is a constant ad hoc network. Each sensor node to a sensing device, a low computational power processor, a short-range wireless transmitter and receiver is equipped with limited battery supply energy [9,10]. Nearby monitors sensor data processing and sensor network nodes and receive data to a base station located next to the data. Immersed in the sensor node WSN nodes collect data and transmit this data to a remote control station. Thus the sensor nodes need more energy for their work and it should be optimized for the efficient performance of WSN. To improve energy efficiency in WSN, various techniques are available. They control topology, data aggregation, routing protocols, such as different approaches are classified [10].

IV. Data Aggregation

Sensor nodes gather sensory information, through monitoring of the geographical area. Wireless sensor networks wireless hop-by-hop transmission of sensory information is collected by the sink node. An appropriate aggregation function for intermediate data obtained from sensor nodes to sink node is used. [11] And so it conserves energy. To reduce the amount of network traffic aggregation and sensor node helps to reduce energy consumption [12].

A data collection technique, data aggregation approach is collected from the sensor nodes using. Data aggregation algorithm sensor data collected from the sensor nodes and then set on a particular node. Many writers in WSN data aggregation technology used for energy efficiency. Different protocols or algorithms are used for data aggregation concept. Data show the following common data aggregation algorithm work [13, 14].

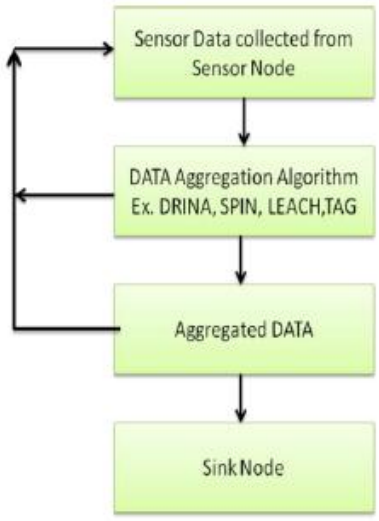

Fig. 3. General Structure of the data aggregation algorithm

Separate data aggregation techniques in wireless sensor networks, such as energy efficiency are available for [15,16]

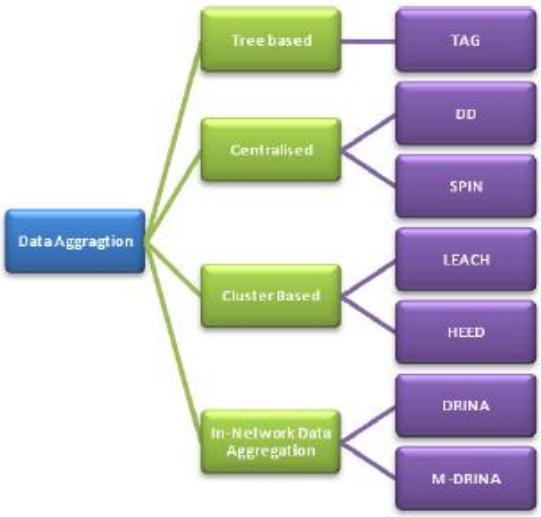

Fig. 4. Hierarchical Structure for data aggregation

A) The tree-based data aggregation

B) centralized data aggregation

C) cluster-based data aggregation

D) In the network aggregation.

The following figure shows the hierarchical structure of WSN data aggregation.

A. *Tree-based data aggregation*

Tree-based data aggregation approach creates an aggregation tree. The tree is a minimum spanning tree, the root node as the source node to node as the sink and leaves treats. In this technique, data is transferred from node to sink leaf node and aggregation nodes is done by the parents.

East. Tags (small aggregation) with the help of the questions that the data aggregation process. Distribute it, low-power, wireless environment provides for the aggregation. [17]

B. *Centralized data aggregation*

Data in centralized data center aggregation technology node is a crowd. This process is a multi-hop wireless protocol used for the path of least hires. The sensor node is a powerful node that can send data packets to a central node. The leader can be asked which set of data. Each intermediate node child nodes sent the data packets addressed to the leader. Therefore, a large number of messages for each node in the external path length equal to the best case for a question to be transmitted. East.DD, spin [18].

1) DD (Direct Spread): This is a period, geographical area, and the gap with the help of the attribute-value pairs, which sense data is data-centric protocol. [19]

2) Spin (for sensor information through negotiation protocol): It uses metadata descriptors or higher. Meta data before transmitting the data through advertising mechanisms are exchanged between sensors. [20]

C. *Cluster-based data aggregation*

This approach also aggregate data for nodes are selected as a treatment for cluster headaches is divided into groups, with some special nodes and forward it to sink nodes are where the nodes are hierarchical organization.
East. Leach, attention

1) Salt water (low energy adaptive cluster hierarchy): The first cluster-based protocol. It runs at different times. Each round has two steps; the first step in self-adaptive mode, the cluster forms and for the second stage is used for data transfer, which is stable, which is a cluster setup. [21]

2) Focus (Distributed Hybrid Energy Efficient): The primary parameters and secondary parameters of energy balance are features of the network topology.

To obtain this load balancing cluster as a metric for selection, the candidate cluster head is used to break the tie. This all nodes are considered as identical. Are all the sensor nodes is equal the initial energy. [22]

D. *Network aggregation*

WSNs in the landscape, in-network data aggregation node to sink in different ways to transfer data packets used by intermediate nodes and nodes gathered from different sources. A data aggregation Aware routing protocol design is a core component in-network data aggregation. INA's idea rather than the entire network to transmit values through feeling, as close as possible to the source of the data required for the determination of derivatives adds.
East. Drina, M Drina

1) Drina (data routing network aggregation): Drina algorithm based cluster approach. It works in three stages. Sensor nodes to communicate with the sink node and sink node data forwarding purposes to be used by the coordinators of the hop tree construction starts in phase 1, hop tree is built. Phase 2 cluster formation and cluster head election detect the occurrence of a new event in the network that is used between nodes. Finally, 3-phase distribution of both packet and hop tree updating reliable is responsible for the installation of a new route. [23]

2) M Drina (revised data aggregation routing network): The clustering nodes to optimize the energy efficiency of our proposed algorithm. Multi-hop communication requires more energy cluster head. The proposed multi-hop communication system that can be used to reduce energy use. Hops as the energy balance in the proposed system, the cluster head selection is based on where the count is based on the current Drina cluster head selection.

Data Aggregation Data aggregation in wireless sensor network is in need of protection as well as a key technology for collecting data security is an important issue. Some key application life-critical applications such as military surveillance and various data transmission, data aggregation, and data reception should be a safe and energy-efficient manner. So many factors must be considered such as to obtain the data, data integrity, data freshness, source authentication, privacy, and safe node localization [24].

a) Data privacy: An unauthorized user cannot access personal or confidential information and data should be prevented from passive attacks that assures. Data can be encrypted using the secret key and sent to the receiver node. Routing information and data both secure should be imposed.

b) Data integrity: the integrity of data on the network nodes of data only authorized users are changing that any tampering assured. The data received in the reordering, that means there is no amendment. It is to send the data should not be corrupted before reaching the destination that ensures. The collected data was compromised node can change the data by inserting false data because it is a very important issue.

c) Data freshness: Data freshness reply to old messages aggregator node is necessary to stop. Freshness and energy performance of the network by obtaining data effectively can be used.

d) Secure node localization: node localization it should be protected and should not be accessed by malicious nodes in the WSN is very important issue. The location of the sensor node has been revealed so all routing information for malicious node location should be safe even if detected.

e) Source Authentication: Data authentication data should be the same as the original data ensures. Source authentication data that is sent by the actual sender allows. Source authentication an attacker to gain access to any node and capture information stored data can prevent the Sybil attack. A WSN attacks on aggregation: It is safer and less physical protection for the sensor node is deployed in the environment because of the attacks are possible on a variety of wireless sensor networks. Various plans to attack different types of protection [19] are performed by the enemy to break. The information stored on this type of attack sensor nodes deployed sensor nodes attacker gains control and takes over:

i) Node compromise Attack: There is a brief discussion of these attacks below. Understanding the node is already stored in the data really can insert false data bits. The advantage of using an anti-aggregator node in the data network is not secure.

*ii) Sybil attack***:** th*is* attack attacker to create multiple identities and different in many ways that can affect data aggregation techniques. After making several fake IDs, it participates in the elections and the aggregator node aggregator nodes as malicious node tries to choose. After that it affects data aggregator node.

iii) Service attack denial: In this type of attack, the attacker over the network through the signal by transmitting radio signals to jam radio frequency interference. The attack aggregator node collected data from various sensor nodes to collect refuse and upper levels of the data in the routing helps.

iv) Selective forwarding attack: Generally the sensor node receives the data from other sensor nodes farther. But what to do in the attack and the aggregator node agreement does not affect the data. Any agreement selective forwarding node can start the attack.

v) Replay Attack: network attacker takes control of the traffic in the records of the traffic. Then enter replays misleading traffic aggregator and aggregator node has been collected, which affects the outcome.

vi) Injection attack: the attacker false data injection into the network. False data collected in the process of aggregation of data will result.

TABLE I. OVERVIEW OF ATTACKS AND SECURITY SYSTEMS

Attack	Cause	Solution
Denial of service attack	By making interference with radio frequency	By using MAC and spread spectrum techniques
False packet, Malleability attack	Due to injection of malicious nodes	By using HMAC
Replay Attack	Without data freshness transmitting same data	By using time stamp to all data packet
Physical Attack	Due to lack security of symmetric key approach	Use of Asymmetric public key approach
Energy Drain attack	Due to energy depletion	By making use of several energy harvesting techniques as: solar power
Sybil attack	By making multiple false identities	By using authentication technique
Sinkhole Attack	By attracting traffic to the specific compromised node	By using proper routing and localization information
Sniffing Attack	Because of capturing data by using malicious nodes	By using protocols with confidentiality of data
Data Integrity Attack	Bye inserting false data	Use of digital signature scheme

V. LEAP PROTOCOL

Leap in wireless sensor network is a very popular security solution and it was proposed Zhu et al in 2004 by the local encryption and authentication protocol (LEAP) is a key Management protocol used to provide protection and support to the network of sensors. It uses μTESLA Base station broadcast authentication and to authenticate the source-hash key to providing a way Packet [25]. The protocol is transmitted between each message that is inspired by the idea Sensor nodes are different from other and different security requirements included. In order Having the same key, exchanging messages when the diversity of security requirements to meet Thus, each person assigned to the apparatus jump offer four types of keys, impractical Node. Established four types of keys: individual keys, pair-wise keys, cluster keys and Group keys [25].

A. *Individual key*

Individual key shared between a node and its corresponding base station is a unique key as they interact between them to provide security. Communication between nodes. It is a node of any unusual behavior that allows the base station to notify a base station is the key to Show its surrounding nodes. As a result, the base station is aware of malicious.

Then such directions to a specific node as important information you can use to encrypt keys Node. Individual keys can be manufactured using the following equation:

Where p is the pseudo random function, ki is the initial key, also known as the master key and IDu is the ID of node u

B. *The pair-wise key*

The pair-wise key shared between a node and its neighboring sensor nodes is a key.

This key privacy or want to establish communication that ensures the safety of a source authentication. In terms of a couple of key transmission secures the advantage of being It is one of a node and its immediate neighbors is shared between the so it prevents from intruders. Individual keys have been set; the nodes can identify your neighbors Your ID waiting for a response from the neighboring node n by sending a message. Add (KP) key can be fabricated by the following equation:

C. Group Key

Global leading sensor nodes within the network are shared by all as a group key is also known.

The base station is broadcast to all nodes within that uses this key to encrypt data Group. The key is sharing the whole group of nodes, since it eliminates the need for a base Station separately with individual keys for individual nodes to encrypt the same message.

The key to the case is updated every once in a while as long as confidentiality is applied Nodes and cluster stops functioning or is removed from the network. A special case of a group the key is known as the cluster key.

D. Cluster key

With many of its neighboring sensor nodes cluster key shared by a node is the key.

U-node cluster using the key generated by a random function and the key that encrypts using pairwise.The key to gaining access to the cluster only authenticated neighbors are able to decrypt, so that Key. Therefore, KC (Cluster key) is generated randomly by the node

The advantage of this protocol reduces the involvement of a base station and that are simply It is efficient in terms of communication and energy. For security purposes, mainly covering the local Communication routing information and messages sent from nodes such as protecting.

The key to decrypt and the kind of installation nodes allows some messages to authenticate Reading from neighboring nodes. Therefore, a cluster of keys allowed using Leap Node to receive only authenticated neighboring nodes allow you to use to protect their data and Decrypt the data.

All in all, these leaps in protocols that they offer are very good that can be said as well, a base station and transmission of packets to the source: both for Verification Mechanism Key revocation and provide fresh as the mechanism. Other benefits offer a leap Networks are its scalability and cluster communications capabilities.

However, the network can affect the big disadvantage of this protocol; it consists of only a single base station and the [7] that assumes compromise. Other Drawbacks, the key is present during the installation process that includes a security weakness and the potential high cost, when four different keys for each node need to store the number of nodes is small.

LEAP protocol, several attempts to use the keying system is through an agreement to ensure that the node is revoked or at least prevent network slow Operations. On the other hand, Leap protocol to prevent attacks on the base station decreases Base station operating a large network in the form of covers, which are so important in itself The proposed solution: better jump Protocol In literature, the majority of key management protocol is usually focused on the aspect that only A quaint base station or sink node in a WSN is used and the value of these protocols Trustworthy. Some systems, however, are used for many sink nodes. [11] In these systems, two Important things should be considered: cost and safety.

LEAP protocol, several attempts to use the keying system is through an agreement to ensure that the node is revoked or at least prevent network slow Operations. A base station, on the other hand, any agreement will be treated the same as a node and an agreement for consideration node also used to remove the mechanism for implementing to prevent a disconnected base station node.

With a lot of excessive research, literature usually covers the functionalities in terms of WSN By participating in a system of a base station. It is important to remember that with increase .The base station and its associated increase in the distance separating the sensor network Sensor nodes and may change after the increase in the distance:

- Packet to propagate through a long distance, they may be lost on the way Resulting in a decline in network performance.

- A large network data transmission between sensor nodes and a single base station Giving lifetime of nodes needed to reduce the high energy consumption is required.

- To a nearby base station nodes are located; their energy is worn out faster, which in turn very fast network lifetime shortens.

To overcome these problems, several base stations employing network shows potential Superior performance. However, the tradeoff between performance and there is of course Costs. Deploy multiple sink nodes in a network can be expensive, but the distance can be Sync between nodes and its associated sensor nodes will be reduced to provide more For successful data transmission path as well as eliminating high energy losses Consumption encountered otherwise.

For this research, many base stations will be considered a WSN. Under circumstances a base station and a sensor node are compromised, an assessment of the network Performance will be analyzed.

A wireless sensor network (providing the benefits of using a large number of nodes Cheap thousands of nodes communicating with each other) until hundred.One or more Base stations to process all of the network functions. Should be required to increase the number of Sink nodes, one has to consider an increase in spending. LEAP protocol offers plenty as previously mentioned a system with the installation of four keys, security. Protocols successfully or attempts to escape

and refresh mechanisms are key revocation Deal with compromised sensor nodes.

Separate agreement the methods used to detect nodes is through μTESLA and a key chain authentication hash functions [15]. However, this protocol lacks security against a base station, it is compromised, and the network should be strengthened. These are important A sink node is compromised, it can be severely affected because the aspects to consider All network functions such as network or system are dealt with these nodes. Flexibility Facility A leap protocol used is beneficial on many other security protocols, but improving firmly need. Therefore, to improve Leap protocol, a solution has been proposed Base stations and the add-on is only possible to overcome the limitations faced attacks In case of an agreement to recover from the base station network system more tightly As well as a compromise sensor nodes.

In theory, the majority of research papers, considered a reliable estimate of the base station and only for nodes of tampering measures. In different places, to stay alert is relevant In the case of a base station is compromised. High level protection against attacks against a base generally characterized by high computational power sources with which the station, a requirement [18] is.

In a wireless sensor network, will be three courses of actions:

- A sensor node is compromised

- A base station is compromised

- Sensor nodes and base stations are concurrent agreement Jump protocol deals only with the first scenario consists of the operations. Improving LEAP protocol, all three scenarios to be constructed with a network, thus, has to be dealt with A base station is over. So, Leap protocol that is able to handle all three by ensuring The aforementioned scenarios, Leap protocols for WSNs will be improved in terms of security.

I compromise to overcome the sensor system used is the same as the original jump protocol Nodes and base stations are to be any another similar mechanism to detect the Tampered with. The solution, I had to install another important key base station (KB) is called.

The key to the base station will be updated from time to time, and it is shared between the base Stations. Base stations are cut, it should be aware of the update session key, and use your old key will not continue to. In doing so, the base station is involved in data transmission, and will not be The other remaining base stations has reached an agreement that will recognize the base station.

Certified base stations administrator will send a message indicating that one of Base stations are cut. Remove, or change the system is up to the administrator with each other. However, the rival base station will act is always a case Node is like a certified and valid base stations being cut off one of the other accused.

Will consider any of base stations, at least one administrator to be greater than the cut the remaining three base stations declare otherwise.

VI. CONCLUSION& FUTURE SCOPE

Separate data aggregation algorithms or protocols by different researchers in wireless sensor networks are used for energy efficiency. Cluster-based and in-network algorithm used mostly for low energy consumption and prolonging the life of the network is to. WSN existing data aggregation protection, can threaten any secure aggregation plan has been proposed that an adversarial model. An aggregator model and the aggregator model: Consequently, these plans were classified into two groups. The classification and adversarial model, secure aggregation schemes leads to better assessment had also been proposed that on the basis of a conceptual framework. In the future, it is more secure schemes evaluate and if necessary to expand infrastructure plan.

REFERENCES

[1] Saraogi, M. (n.d.). Security in wireless sensor networks. University of Tennessee,

[2] Burgner, D. E., &Wahsheh, L. A. (2011). Security of wireless sensor networks. Eighth International Conference on Information Technology: New Generations,

[3] Madden, S. R., Franklin, M. J., Hellerstein, J. M., and Hong, W., TAG: A tiny aggregation service for ad-hoc sensor networks. In The Fifth Symposium on Operating Systems Design and Implementation (OSDI 2002), 2002,

[4] Madden, S. R., Szewczyk, R., Franklin, M. J., and Culler, D. Supporting aggregate queries over ad-hoc wireless sensor networks. In Workshop on Mobile Computing and Systems Applications, 2002,

[5] Zhu, S., Setia, S., Jajodia S., LEAP: Efficient Security Mechanisms for Large-Scale Distributed Sensor Networks. In The Proceedings of the 10th ACM conference on Computer and communications security, 2003.

[6] Jang, J., Kwon, T., &Jooseok, S. (2007). A time-based key management protocol for wireless sensor networks. E. Dawson and D.S. Wong (Eds.): ISPEC 2007, LNCS 4464, pp. 314–328, 2007.,

[7] Pathan, A. K. (2011). Security of self-organizing networks. (1 ed., pp. 318-344). Florida: CRC Press.

[8] Saraogi, M. (n.d.). Security in wireless sensor networks. University of Tennessee,

[9] Jang, J., Kwon, T., &Jooseok, S. (2007). A time-based key management protocol for wireless sensor networks. E. Dawson and D.S. Wong (Eds.): ISPEC 2007, LNCS 4464, pp. 314–328, 2007.,

[10] Zhu, S., Setia, S., Jajodia S., LEAP: Efficient Security Mechanisms for Large-Scale Distributed Sensor Networks. In The Proceedings of the 10th ACM conference on Computer and communications security, 2003.

[11] Modares, H., Salleh, R., &Moravejosharieh, A. (2011). Overview of security issues in wireless sensor networks. Third International Conference on Computational Intelligence, Modelling& Simulation, IEEE,

[12] Abuhelaleh, M. A., &Elleithy, K. M. (2010). Security in wireless sensor networks: Key management module in sooawsn. International Journal of Network Security & Its Applications (IJNSA), 2(No. 4),

[13] Mohanty, P., Panigrahi, S., Sarma, N., &Satapathy, S. S. (2010). Security issues in wireless sensor network data gathering protocols: A survey. Journal of Theoretical and Applied Information Technology,

[14] Perrig, A., Szewczyk, R., Wen, V., Culler, D., &Tygar, J. D. (2001). Spins: Security protocols for sensor networks. Mobile Computing and Networking 2001,

[15] Wang, Y., Ramamurthy, B., &Xue, Y. (2008). A key management protocol for wireless sensor networks with multiple base stations. CSE Conference and Workshop Papers. Paper 111.,

[16] Wang, Y., Ramamurthy, B., &Xue, Y. (2008, January 1).Digitalcommons@university of nebraska - lincoln. Retrievedfrom http://digitalcommons.unl.edu/cseconfwork/111

[17] Xue, Y., Lee, H. S., Yang, M., &Kumarawadu,, P. (2007). Performance evaluation of ns-2 simulator for wireless sensor networks. 0840-7789/07 ©2007 IEEE,

[18] Söderlund, R. (2006). Energy efficient authentication in wireless sensor networks. LITHIDA/ DS-EX--06/012--SE,

[19] Perillo, M. A., &Heinzelman, W. B. (n.d.). Wireless sensor network protocols. Department of

[20] Electrical and Computer Engineering University of Rochester, Leandro Villas, Azzedine Boukerche1, Heitor S. Ramos "DRINA: A Lightweight and Reliable Routing Approach for in-Network Aggregation in Wireless Sensor Networks" , IEEE 2013

[21] Erfan. Arbab, Vahe. Aghazarian, Alireza. Hedayati, and Nima. GhazanfariMotlagh, "A LEACH-Based Clustering Algorithm for Optimizing Energy Consumption in Wireless Sensor Networks", ICCSIT'2012

[22] Samuel Madden, Michael J. Franklin, and Joseph M. Hellerstein, "TAG: a Tiny AGgregation Service for Ad-Hoc Sensor Networks",OSDI, December, 2002.

[23] VaibhavPandey, AmarjeetKaur, Narottam Chand, "A review on data aggregation techniques in wireless sensor",JEEE, 2010

[24] Geetu, Sonia Juneja, " Performance Analysis of SPIN and LEACH Routing Protocol in WSN", IJCER,2012

[25] ParulBakaraniya, Shital Mehta, "Features of WSN and Various Routing Techniques For WSn: A survey", IJRET,2012