International Journal of Applied Engineering Research ISSN 0973-4562 Volume 12, Number 11 (2017) pp. 2848-2854

Security Enhancement for the Wireless Sensor Networks

Dr. M. Anand Kumar
Associate Professor, Karpagam University, Karpagam Academy of Higher Education, Eachanari Post, Coimbatore, Tamil Nadu, India.

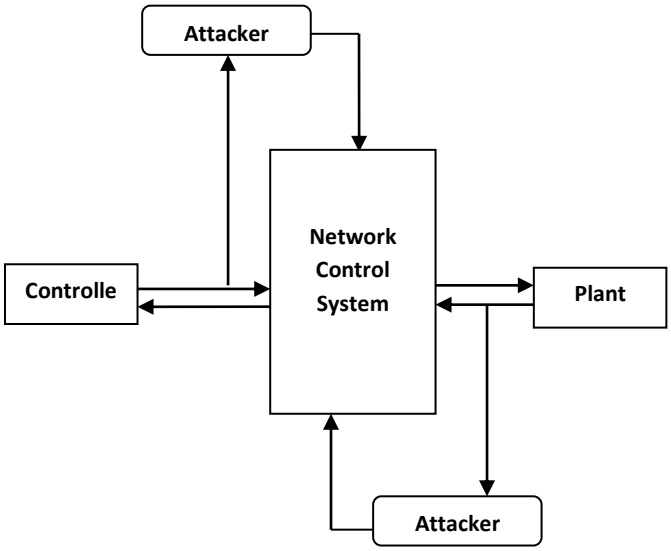
M. Jagadheeswari
Ph.D Research Scholar, Karpagam University, Karpagam Academy of Higher Education, Eachanari Post, Coimbatore, Tamil Nadu, India.

Abstract
This paper represents energy efficiency technique to find out the deception attack in wireless sensor network. NCS network provide many challenges to protect the packet delay and packet dropout. This methodology used to find out the attack and mitigate the effects and it improves the performance and protect from the damage. Protection against network attack consumes more energy. So the protection will be activated only when the attack persists in the network. In wireless network, deception attack will damage the network data and its integrity. Reduction of energy consumption, it leads to improve the network performance. Host will take more energy while its data transmission. It unnecessarily wastes its resources due to its delay of packet transmission and packets lose. If the system always monitors the network, its resource will be wasted. These problems will be overcome through TAM and CAR algorithm.

INTRODUCTION:
Now-a-days authentication is very mandatory to protect data and resources from unauthorized persons. Intrusion is a set of activity that compromise integrity, confidentiality, or availability, of a computing and networking resource. Intrusion Detection System is a software or hardware device that monitors the network activity and analyzes the activities for signs of possible violations of computer security policies. Intrusion detection provide three main types of security services i) Monitor the network activity ii) detect unauthorized access iii) Respond to any unauthorized access[1].

Deception attack is one of the major cyber attacks conveyes false information in any communication channel. Attacker misuses the information which is carrying out between the sender and receiver. Deception attack represented in both deceiver and target. This attack successfully done while the deceiver successfully misuses the target information. It can occur in any financial or economic interaction [3].

This deception attack represents in factory automation where the Network Control System works in the dangerous environment. The main problem of NCS is reduction of bandwidth required to each subsystem. To overcome this problem, Network Control System minimize overhead of data transfer. Plant and controller connected with packet based network. Plant carry out the command **c** to controller and the controller carry out output **o** to plant through the packet based network. Deception attack affects the data integrity of packet to modify their payload. Deception represents the interaction between the deceiver and target. Deceiver successfully modifies the target data to specify the incorrect version of reality. Deception can be represented in any financial or economical interaction [5].



The packet will be encrypted during the transmission over the network to protect the packet from the unauthorized person. The digital signature techniques add its signature along with the message for protection. Encryption of packet will take more energy consumption due to the increased size of packet. Digital signature will increase the battery consumption due to the increased size of transmission packet. Energy overhead will be increased when the attack is exists. If monitoring networks all the time, it leads to the unnecessary waste of resource. Intrusion detection system is used to optimize the system. It will monitor the network traffic and compare with predefined baseline threshold. If attack exists, it will activate the security check.

Attack mitigation is an another problem in this system. It will measure the performance when an attack is present. If performance of the current network load is higher the predefined threshold value, then it will send more data, otherwise it will decrease the network load [6].

LITERATURE SURVEY:

Zahra Rezaei , Shima Mobininejad [1] performed a work on energy saving in wireless sensor networks identified two main approaches ie duty-cycling and data-driven approaches to maximize the life time of node's battery by the minimizing consumption of energy. In duty-cycling method, sensor operates on four modes: transmission state, reception state, idle state and sleep state. Transceiver will be in an idle state if there is no more data to send or receive. It leads to reduce the energy consumption. The sensor should be resumed if the new packet becomes ready to send or receive. Alternatively nodes will be active or sleep depending on the network activity. In data-driven approach, mainly it aims to reduce the energy spent by the sensing subsystem. This technique follows two processes: in-network processing and data prediction. In-network processing, it performs data aggregation at the intermediate nodes from source to sink. Data rate will be reduced while traversing the network towards the sink. Data prediction predicts the values sensed by the sensor. If the accuracy is satisfied, queries can be evaluated at sink to reduce the power consumption.

Gurpreet Singh Sodhi and Sarabjit Singh [2] performed a work on Increasing the Performance of Wireless Sensor Networks using IM-LEACH. In this work using the clustering techniques to decrease battery consumption and to increase the scalability of WSN. IM-LEACH clustering algorithm used in this work to reduce the power consumption of battery. It has two phases a) Cluster formation b) deciding schedule for cluster head. In LEACH, every node has selected a random number that is compared with threshold value. Every node in the network acts as a cluster head whether it has a high energy or low energy. Low energy cluster head will end its life before forward the data to the base station. To solve this problem, each and every node will send their energy value to the initiator node. Initiator node will decide which node is eligible to elect to cluster head node. Initiator discards the low energy node and select high energy node as cluster head. It will forward the data to base station without compromising the performance.

Amit Sharma[3] performed a work on Energy Management for Wireless Sensor Network Nodes. This work represents the energy management and saving techniques in WSN. Data transmission takes much more energy consumption to transfer the data. This energy management technique reduced the data transmission rate by minimizing the amount of redundant data. It leads to minimize the cost of data transmission. LEACH is a cluster based algorithm used to reduce the data sensed by the sensor before forwards this data to the central base node. This technique helps to reduce the memory consumption.

R. S. Mangrulkar[4] performed a work on an improved cluster head selection approach for energy efficiency in the wireless sensor networks. This work keeps the entire network to stay alive for a long time and improves the performance of WSN network. Based on the energy, CH will be selected and the threshold value is calculated at base station to reduce the energy consumption. If the energy of node is higher than the threshold value, that node is selected as a cluster head. Minimum threshold value is rejected to select the cluster head to improve the lifetime of a node. Base station calculates the Energy Level Value and forward to cluster head; it seriously affects the bandwidth on network. It leads to prevent from filling the data packets in the network and decrease the usage of bandwidth.

D.Suresh and K.Selvakumar[5] performed a work on Network Lifetime and the Reducing Energy Consumption in Wireless Sensor Networks. CAR algorithm helps to reduce the energy consumption and increase the life span of the network. This technique reduces the data transmission distance of sensor node in WSN. CAFEE algorithm helps to the base stations to receive the information of location and residual energy of sensor node and energy of every node which is in the network. Residual energy of sensor node should be higher than the residual energy of average cluster head. CAFEE follows two phases: setup phase and steady state model. In setup phase, algorithm creates the cluster and find cluster head nodes. In this phase, base station collects information of location and energy level of each node. In steady state model, TDMA schedule is created to begin the data transmission process. Cluster head node will collect the data from non-cluster head node during their transmission slot. After receiving all the data, cluster head compress the data into single signal and send to the base station. It helps to reduce the amount of data reduced to decrease the energy consumption and used to increase the life time of the network.

Yingwei Yao, and Georgios B. Giannakis [6] performed a work on Energy-Efficient Scheduling for the Wireless Sensor Networks. This work minimizes the energy needed to the data fusion in sensor network among the different sensor nodes. Low complexity inverse log scheduling algorithm is used to achieve the near optimal energy efficiency. This work also used the centralized scheduling protocol to eliminate the communication over sensor network. Assigning a longer transmission time to each sensor channel leads to save the energy consumption required to the sensor network.

Subhash Dhar Dwivedi and Praveen Kaushik[7] performed a work on Energy Efficient Routing Algorithm with the sleep

scheduling in the Wireless Sensor Network. This work used sleep scheduling algorithm to save the energy of sensor network and increase the lifetime of the network. Cluster based routing protocol is used to achieve the energy efficiency. In this technique, all the nodes are collected as cluster and one node is selected as cluster head. Cluster head receives data from other node and forward to data sink. Each node in the network may be in sleep state in the probability of p or active state in the probability of 1-p. Sleep state node should not able to send or receive any packet until it get wake up. Sleeping node will be wake up after a period of time. This technique decides which node should be put into the sleep node to save energy consumed by the sensor node. It decides the active node list and sleep node list and constructs the tree structure using Breadth-First Search (BFS). Entire process will process for certain period of time. If any node takes long time or get down before time up, it affects the entire routing structure and leads to energy consumption takes much than as usual. So this technique should mantory consider that all the node should take equal consumption of energy and sharing of network load by the entire node. It leads the network to work long time without the power intervention.

Aly M. El-Semary[8] performed a work on Energy-Efficient Secure Routing Protocol Based on Roulette-Wheel and μTesla for Wireless Sensor Networks. This work performs as an energy efficient secure routing protocol. Roulette wheel selection algorithm used to select the next node to forward the data packet and μTesla protocol used to send the data securely through the symmetric encryption and hash the function algorithms. Next node selection is done based on the forwarding node information. μTesla protocol used symmetric encryption algorithm instead of using asymmetric algorithm to authenticating data over network. Symmetric algorithm is faster than asymmetric algorithm for encryption, it leads increase the performance.

Dhanunjayudu.K and Mahesh.B[9] performed a work on Trust-Based Secure And Energy Efficient Routing Framework For WSNS. This work found out deception and confirms the secure communication over wireless sensor network. WSN should have a secure communication with the base station. The deception attacks are not allowed over the network. Before sending data to the base station, sensor checks the trust value. If the trust value is higher than the threshold value, the data will be forwarded to base station. Otherwise data will be rejected. It obtains the greater throughput and used to protect the network from various deception attacks.

Amandeep Kaur and Kamaljit Kaur [10] performed a work on A Review of Different Energy Efficiency Techniques in Wireless Sensor Networks. This work performed a large comparison of two routing protocols used in the wireless sensor network. This work performed a comparison on LEACH and PEGASIS protocols and its strengths and weakness of these protocols using some metrics like usage of power, mobility. PEGASIS algorithm is better energy reduction algorithm than the LEACH protocol.

Sanghamitra Panda, Satyanarayana Gandi and Amarendra Kothalanka[11] performed a work on Secure and Efficient Data Transmission for Cluster-Based Wireless Sensor Networks. In this work security aspects, are increased, it follows two methods. One is Identity Based Signature used for authentication. Second is the secret key is XOR with the data and produce the cipher text and send to receiver. This binary level encryption technique encrypts the plain text to cipher text and split it into block. Receiver decrypts the data using reverse technique and gets the original plain text. This technique helps to improve efficiency of network, reduce the power consumption and reduce the security overhead.

Chih-Wei Shiou,Frank Yeong-SungLin, Hsu-Chen Cheng, and Yean Fu-Wen[12] performed a work on Optimal Energy Efficient Routing for the Wireless Sensor Networks. Increasing the number of nodes in network will reduce the power consumption. Error occurred in the network leads to retransmission of data again in the network. Retransmission of data takes more bandwidth energy and reduce lifetime of the network. This work used shortest path-based heuristic algorithm to reduce the energy and the increase network lifetime. It found out the shortest path to forward the data, and it leads to reduce the time to forward the data and reduce the energy taken for transmission.

PROBLEM DEFINITION:

NCS network faces deception attack problems; it will affect the network performance and leads to data damage. To increase the performance and to provide the data integrity, NCS network uses digital signature to encrypt the data. It add its digest with the message itself, and used to verify the data integrity whether the data is attacked by the attacker or not. Digital signature techniques will increase the size of the data and consume more energy to send the data. Data delay or data lose also affect the network performance, take unnecessary energy consumption. Two techniques are used to reduce the energy consumption and improve the network performance.

1. Protection will be done after the attack is on-going through finding the statistical approach.
2. Transmission rate will be adjusted according to the current performance of the network.

PROBLEM STATEMENT:

Network control system:

In NCS, plant pl(x) and controller cr(x) are connected with the packet based network. Here controller send the command **c** to plant and plant send the corresponding output **o** to controller. Wireless network used to communicate between the machines without additional cost for wiring. For the mobile environment, wireless medium is the only one solution. But it had more transmission issues like packet delay and packet loss. These transmission issues take more battery consumption. An energy efficient technique is used to increase the battery life for long time. Energy efficient technique follows two main tasks to increase life span of battery.

1. Minimize the overhead of encrypted packet

transmission.

2. Energy consumption will be reduced if control performance is the above threshold value.

Deception attack and protection:

Man-in-the-middle attack approach is tampered the network medium and make changes in the transmission packet. It leads severe damage in the NCS network. To attack countermeasure, digital signature is used for the message integrity. In digital signature, message signature created by the sender using sender's private key and inserted into message. Encrypted packet is transmitted over the network. At receiver side, receiver decrypt message by using sender's public key and compare it with locally computed digest. If both are same, message is not corrupted and receiver accepts the message. Otherwise the receiver decided that the attack is detected in that message.

Attacker strategy should be well known to handle the deception attack against the network. Attacker control system should work based on some strategy. i) damage system control ii) degrade performance of the network iii) undetected attacks in network for long time. These aspects of attacker will affect the network performance and leads to increase the attack activity in the network system.

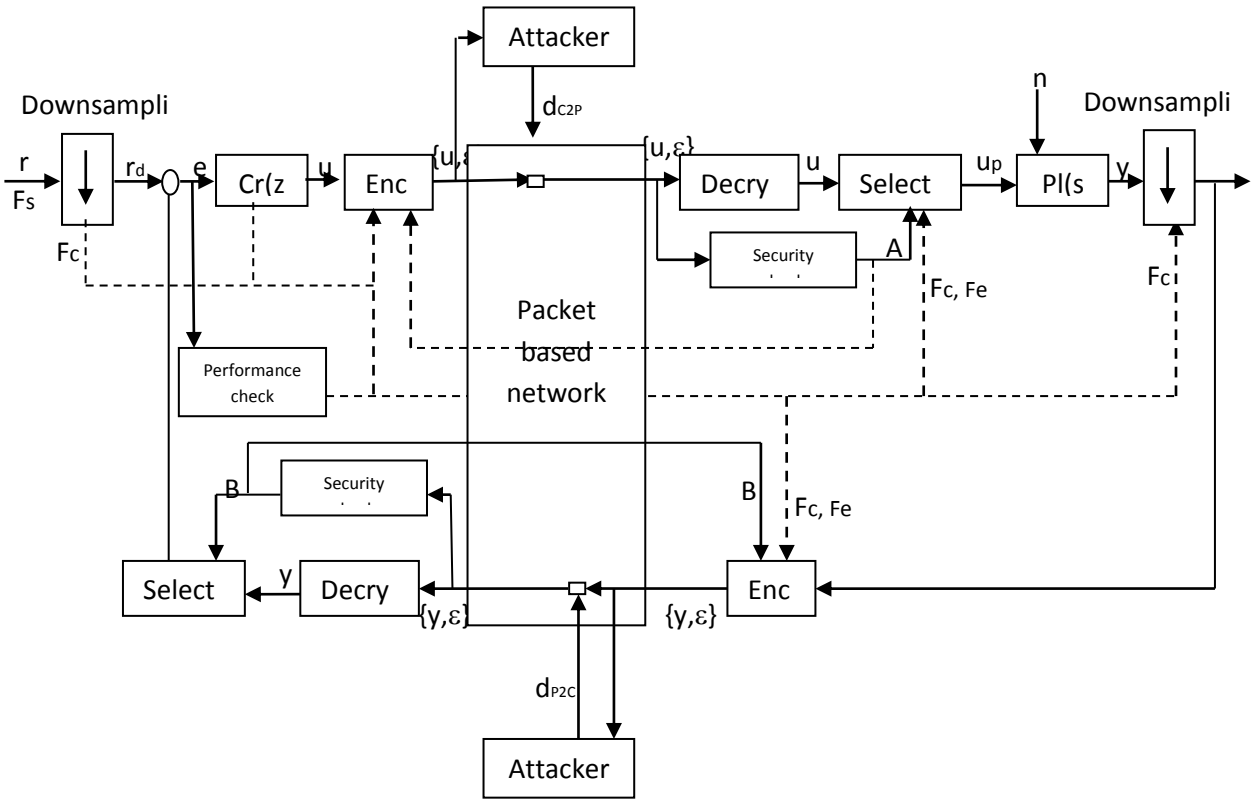
An encryption technique consumes more extra energy to transmit the data than sending the ordinary data. Digital signature increases the packet size and it requires more energy to be transmitted. Consumption of more energy leads to consume more computational and communication resources. Decreasing this resource overhead is not enough to increase the energy efficiency. It requires achieving two objectives to increase energy efficiency.

i) Activate the protection strategy only if the attack presents in the network.
ii) Adjust the transmission rate according to the network performance.

Proposed energy efficient control architecture used to i) detect the attacks ii) find out the end of the attack interval iii) save the transmission energy without compromising the performance.

PROPOSED ARCHITECTURE:

The proposed architecture used the security check block and performance check block to improve the energy efficiency. Security check block activates the security mechanism while attack occurs and performance check block enhance the performance of the network.



Controller:
Controller is a discrete time system to create command and send it to the plant through the packet based network. It receives the decrypted message from the plant.

Encryption block:
Encryption block encrypt the incoming packet and send it to the plant or controller. Encryption means insert the signature with its message. It uses the encryption bits either 0 or 1. If it is 1 means, packet is encrypted otherwise the packet is an unencrypted packet.

Decryption block:
Decryption block checks whether the packet is encrypted or not. If it is encrypted, that packet is decrypted and checks its data integrity. If any changes found, that corrupted packet will be discarded, otherwise it is accepted.

Plant:
A continuous time system with input and output.

Selector:
Selector mainly depends on the response of security check block. If any attack occurs, selector rejects the unencrypted packets from the network.

Attacker:
Attacker hacks the unencrypted packet either actively or passively from the network.

TAM ALGORITHM:
Energy overhead will be high when the attack persists on the network. Always monitoring the network leads unnecessary consumption of resources. To reduce the energy consumption, TAM algorithm is used to check whether the attack occurred on network or not. If the attack persists in the network, immediately take the security check action. To achieve this, TAM is used with the Multivariate Correlation Analysis.

Multivariate Correlation Analysis (MCA) is used with triangular area map to detect the attack. TAM is created and triangle attributes arranged and compared to find the attack. Mahalanobis Distance is used to find the dissimilarity between the network traffic records to identify the normal profile generation. Threshold value is calculated and checked with the statistical property to find the intrusion attacks. Multivariate Correlation Analysis follows two steps feature normalization and TAM generation. Feature normalization selects the normal attribute values and these features normally distributed to achieve the better detection rate and achieve desired results. In normal distribution, mean and standard deviation is calculated for every attributes.

The behavior of Deception attack traffic is reflected by its statistical property. It employs extracting correlative information from its observed objects. Triangular area is calculated for each and every combination of attributes objects. TAM^{i}_{lower} and mean of TAM^{i}_{lower} is calculated for each and every packet. These TAM values used to calculate the Euclidian Distance.

Euclidian Distance.is calculated in each and every packets in between the value of TAM^{i}_{lower} and mean of TAM^{i}_{lower} . Mean of all Euclidian Distance 'μ' and standard deviation 'σ' is calculated. Feature normalization uses 'μ', 'σ' and 'α' to define the threshold value. Threshold value define the normal profile range and falls in the range between '$\mu + \sigma * \alpha$' and '$\mu - \sigma * \alpha$'.

Euclidian Distance evaluates the normal threshold range. If it falls in the normal threshold range, then it is considered as normal traffic packet, otherwise it will be considered as an attack.

Generate TAM^{ob}_{lower} for all observed traffic record

Calculate $ED^{ob} = ED(TAM^{ob}_{lower}, TAM^{ob}_{lower})$

If $(\mu - \sigma * \alpha) \leq ED^{ob} \leq (\mu + \sigma * \alpha)$

Then return **Normal**

Else

Return **Attack**

End if

The below table represents the analysis part of TAM algorithm with existing algorithm for the wireless sensor network.

Table 1: Comparison of Scalability and transmission delay of TAM and existing algorithm

Algorithms	Scalability	Transmission delay
TAM	90%	84%
LEACH	93%	90%
CAFEE	95%	95%
PEGASIS	96%	97%

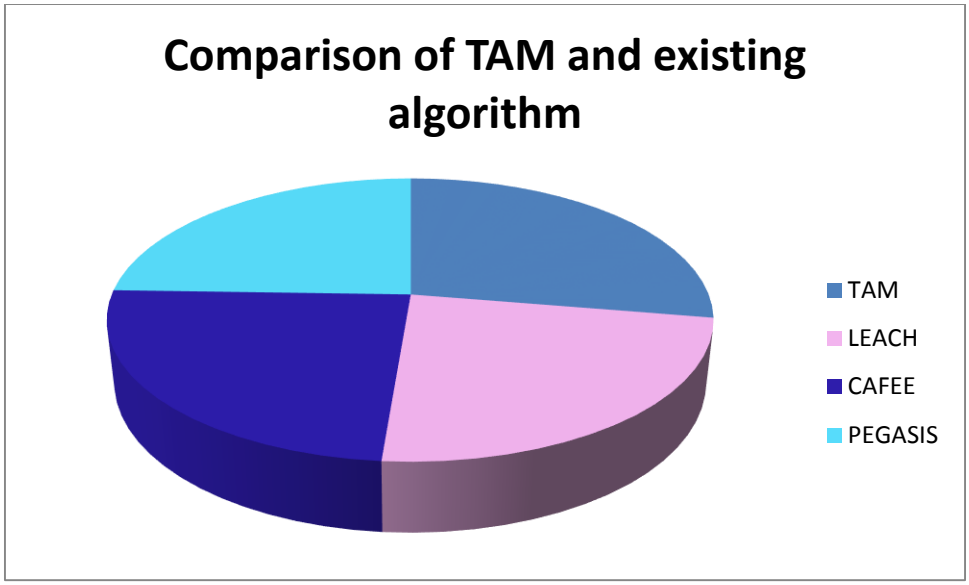
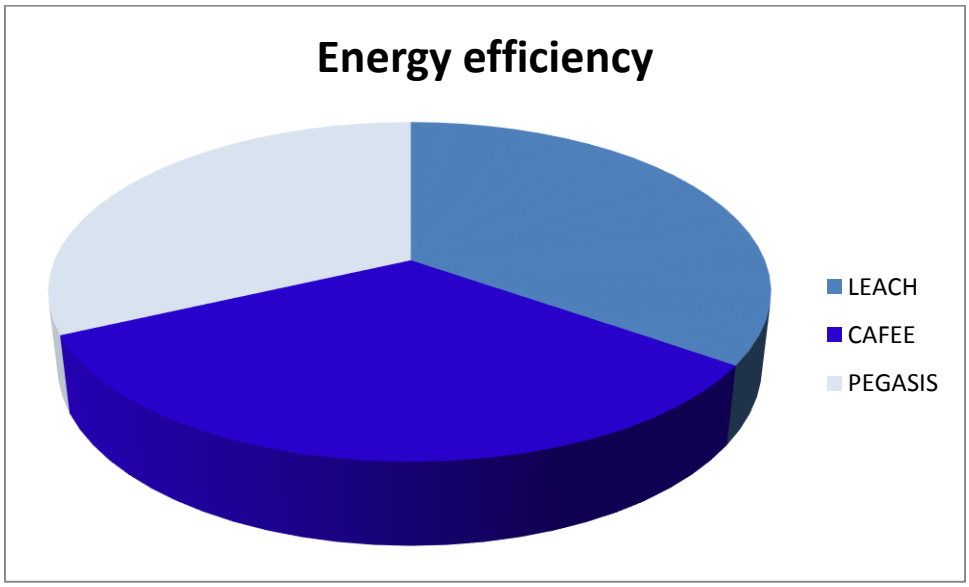


Table 1: Comparison of TAM algorithm and existing algorithm

Algorithms	Energy efficiency	Algorithm complexity	Uniform distribution of energy
LEACH	99%	Very Low	High
CAFEE	95%	Medium	Medium
PEGASIS	91%	High	Low



CAR Algorithm:

If the number of packets increases than the actual transmit capacity of network, it affect the performance of network. Performance degradation leads to the energy waste. Sometimes high important data will be dropped due to the network congestion and low important data will be delivered. This leads to degrade the performance of the network. To overcome this problem by Congestion Aware Routing protocol. It creates a conzone and enforces a differentiated routing based on the data priority. High priority nodes routed inside the conzone and low priority nodes routed outside conzone. Congestion Aware routing algorithm routes the high priority data delivery and decrease the data delay and data loss. So Congestion Aware Routing reduces energy consumption and increase the node's lifetime.

To achieve this goal, Congestion Aware Routing protocol

divides the network into two areas: congestion area and remaining part of the area. High priority data travels within the congestion zone to increase the performance and low priority data travels outside the congestion zone. After sensor node deployment, base station initiates to create high priority sensor network to carry high priority data.

CONCLUSION:

This paper presents the energy efficient technique for the wireless sensor network. Host takes more energy for the data transmission. It wastes its bandwidth due to packet delay and data lose. To avoid this problem, energy efficiency technique used to increase the performance of the wireless sensor network. This paper explains two algorithms to increase the performance of the network: Triangle Area Map and Congestion Aware Routing. This paper explains in detailed about TAM algorithm. If the attack frequently persists in the network, then the energy overhead will be high. It leads to unnecessary consumption of bandwidth. To avoid this problem, TAM algorithm checks whether attack the persists in the network or not. If the attack persists, it takes the security check mechanism. Encryption technique is used to detect the attack and save the battery power while the data transmission.

REFERENCES:

[1] M. Anand Kumar, Dr. S. Karthikeyan (2011), "Security Model for TCP/IP Protocol Suite", Journal of Advances in Information Technology, 2[2], 87-91.

[2] Zahra Rezaei , Shima Mobininejad, "Energy Saving in Wireless Sensor Networks", IJCSES, Vol . 3 No. 1, Feb 2012, DOI : 10.5121/ijcses.2012.3103. 23.

[3] M. Anand Kumar and Dr. S. Karthikeyan (2012)," Investigating the Efficiency of Blowfish and Rejindael (AES) Algorithms" International Journal of Computer Network and Information Security", 4[2] : 22-28.

[4] Gurpreet Singh Sodhi, Sarabjit Singh, "Increasing the performance of wireless sensor networks using IM-LEACH", IJESC, March 2015, DOI: 10.4010/2015.311.

[5] M. Anand Kumar and Dr. S. Karthikeyan 2012)," A New 512 Bit Cipher - SF Block Cipher" International. Journal of Computer Network and Information Security", 4[11]:55-61.

[6] Dr. M. Anand Kumar.and Dr. S. Karthikeyan (2013)," An Enhanced Security for TCP/IP Protocol Suite" International. Journal of Computer Science and Mobile Computing , 2[11]:331-338.

[7] Amit Sharma, Kshitij Shinghal, Neelam Srivastava, Raghuvir Singh, "Energy Management for Wireless Sensor Network Nodes", IJAET, Vol. 1, Mar 2011.

[8] Snehal P. Dongare, R. S. Mangrulkar, "An improved cluster head selection approach for energy efficiency in wireless sensor networks: A review", IEEE, Jan 2015, DOI: 10.1109/PERVASIVE.2015.7087190

[9] D.Suresh , K.Selvakumar, "Improving Network Lifetime and Reducing Energy Consumption in Wireless Sensor Networks", IJCSIT, Vol. 5 (2) , 2014.

[10] Yingwei Yao, and Georgios B. Giannakis, "Energy-Efficient Scheduling for Wireless Sensor Networks", IEEE, VOL. 53, NO. 8, AUGUST 2005, DOI: 10.1109/TCOMM.2005.852834.

[11] Subhash Dhar Dwivedi, Praveen Kaushik, "Energy Efficient Routing Algorithm with sleep scheduling in Wireless Sensor Network", IJCSIT, Vol. 3 (3), 2012.

[12] Aly M. El-Semary, "Energy-Efficient Secure Routing Protocol Based on Roulette-Wheel and μTesla forWireless Sensor Networks", International Journal of Sensor Networks and Data Communications, Vol. 1 (2012), Ashdin Publishing, doi:10.4303/ijsndc/X110201.

[13] Dhanunjayudu.K, Mahesh.B, "Trust-Based Secure And Energy Efficient Routing Framework For WSNS", IJCTT, volume 5, number 1, Nov 2013, DOI: 10.14445/22312803/IJCTT-V5N1P101

[14] Amandeep Kaur, Kamaljit Kaur, "A Review of Different Energy Efficiency Techniques in Wireless Sensor Networks", Volume 5, Issue 6, June 2015, Doi: 10.1007/s11276-015-1025-x.

[15] Sanghamitra Panda, Satyanarayana Gandi, Amarendra Kothalanka, "Secure and Efficient Data Transmission for Cluster-Based Wireless Sensor Networks",IJARCCE, Vol. 4, Issue 1, January 2015, DOI: 10.17148/IJARCCE.2015.4106. 27

[16] Chih-Wei Shiou,Frank Yeong-SungLin, Hsu-Chen Cheng, and Yean Fu-Wen, "OptimalEnergy-Efficient Routing for Wireless Sensor Networks", IEEE, 2005, DOI: 10.1109/AINA.2005.268.

[17] P. Samundiswary,Padma Priyadarshini and P. Dananjayan, "Detection of Sinkhole Attacks for Mobile Nodes in Heterogeneous Sensor Networks with Mobile Sinks", IJCEE, Vol. 2, No. 1, February, 2010

[18] Nidhi Chhajed and Mayank Sharma, "Detection and Prevention Techniques for Black hole Attack in Wireless Sensor Networks (WSN's): A Review", IJARCSSE, Volume 4, Issue 11, November 2014, DOI: 10.1002/wcm.v8:6. [14].

[19] Ira Nath and Dr. Rituparna Chaki, "BHAPSC: A New Black Hole Attack Prevention System in Clustered MANET", IJARCSSE, Volume 2, Issue 8, August 2012, DOI: 10.1002/sec.144. 11.