isrjournals

International Journal of Advanced Research in Computer Science Engineering and Information Technology

Volume: 4, Issue: 3,Special Issue: 1 ,Mar,2016 ,ISSN_NO: 2321-3337

Reliable And Secure Data Transfer For Wireless Sensor Network

Mrs.Jeyaselvi.M[1],Akshara K P[2], Cyrene Mary A[3]
Sr.Asst. Professor, Dept. of Computer Science and Engineering,
Agni College of Technology, Chennai.
Student, Dept. of Computer Science and Engineering,
Agni College of Technology, Chennai.

Abstract**- A traditional setting, investigations on group communication focus on system reliability in the face of network failures or group member changes. However, sensor networks face serious obstacles like limited energy resources and high vulnerability to harsh environmental conditions that have to be considered carefully. In our concept, sink selects the nodes to create a cluster head based on node received signal strength. Cluster head assigns digital signature to each node for transmits sensed data to sink through cluster head using RCS (Resource Conscious Secure Routing) protocols. The protocol is used to authenticate the digital signature of that authorized node, which are efficient for communication and applying the key management for security. After packet transmission sink conduct recycling process to select new cluster head based on node threshold value. Although all sub nodes id and cluster head changed based on RCS. We are using localization algorithm to detect the attack in cluster head. Sink to detect the active attack based on checking the new node arrival using localization algorithm. After identification of attacker, that attacker node goes to inactive state. For security purposes, the content of each message can also be encoded by using pattern encoding method and decoded at the sink node by knowing the swapping bit position. So, unauthenticated person cannot access the original data. By this way, the protocol provides a secure message delivery option to maximize the message delivery ratio under adversarial attacks.**

Keywords— routing, message delivery ratio, energy balance, pattern

encoding, random walking.

I. INTRODUCTION

A wireless sensor network consists of a collection of many unbound and unattached randomly placed sensor nodes with non-replenishable energy resources. Because of this, routing in wireless sensor networks is a tremendous challenge. Routing is challenging in wireless sensor networks since it cannot provide soaring message delivery ratio and little energy consumption for message delivery. Routing should also ensure energy balance and security among the sensor nodes thereby extending the sensor network lifetime. Along with aforesaid issues, wireless sensor networks rely on wireless communication and can be easily attacked by several adversaries due to missing physical boundary. The adversaries can be well equipped and hence they can act upon the network from a distance and extract the messages. They can also cause jamming and traceback attacks. Propelled by the reality that WSNs routing is often geography based, we propose geography based secure and efficient Resource Conscious Secure routing (RCS) protocol for WSNs without relying on flooding. RCS allows messages to be transmitted using two routing strategies, Random Walking and Deterministic Routing, in the same framework. In the Random walking method, there is a chance of choosing low energy node as a relay node. To avoid this, the data is transmitted via energy aware route only, the MES scheme on Elliptic curve algorithm used to provide authentication. For security purposes, the content of each message can also be encoded by using pattern encoding method and decoded at the sink node by knowing the swapping bit position. So, unauthenticated person cannot access the original data. By this way, the protocol provides a secure message delivery option to maximize the message delivery ratio under adversarial attacks. RCS protocol has two major preferences: (1) Balanced energy consumption can be ensured. (ii) Manifold routing strategies can be used to ensure security. Also, routing traceback attacks and hostile traffic jamming attacks can be detected and prevented.

II. SYSTEM ANALYSIS

2.1 EXISTING SYSTEM:

Lifetime optimization and security are two conflicting design issues for multi-hop wireless sensor networks (WSNs) with non-renewable energy resources. In this paper, they proposed a novel secure and efficient Cost-Aware Secure Routing protocol to address these two conflicting issues through two adjustable parameters: energy balance control and probabilistic-based random walking. They then discovered that the energy consumption is severely disproportional to the uniform energy deployment for the given network topology, which greatly reduces the lifetime of the sensor networks. To solve this problem, they proposed an efficient non-uniform energy deployment strategy to optimize the lifetime and message delivery ratio under the same energy resource and security requirement.

2.2 PROPOSED SYSTEM:

In our paper, the network is equally divided into little grids. Each grid has a relative location based on the grid information. The node in each grid with the greater energy level is selected as the head node for message forwarding. The head node can be re-elected if the energy level becomes low than other nodes in the grid. In addition, each node in the grid will maintain its own attributes, including location information, remaining energy level of its grid, as well as the attributes of its adjacent neighbouring grids.

The information maintained by each sensor node will be updated periodically. In this project, we will focus on two routing strategies for message forwarding: shortest path message forwarding, and secure message forwarding through random walking to create routing path unpredictability for source privacy and jamming prevention. To avoid the storage of secret keys we are going to use pattern encoding for encoding and decoding purpose.

III. IMPLEMENTATION

3.1 Node construction

- First we have to construct a base station which consists of ‘n’ number of Nodes. So that nodes can request data from other nodes in the network. We can assume that

  the nodes are moving across the base station. All nodes in the cluster head connect through the base station. Base station is used to store all the Nodes information like Node Id, Energy Initialized, Public key,

  private key and Digital Signature and also node location with Time stamp details are updated to the Sink from the all sensor nodes.

- Also base station will monitor all the Nodes Communication for security purpose.

3.2 Cluster head formation

- In this module, base station assigns energy, public and private key for each node and it selects the cluster head based on node distance. Then the cluster head selects

  sub nodes based on coverage area.

- Then cluster head 1 selects the cluster head 2 similarly cluster head are selected and it forms the group using clustering algorithm. Once we created node group in the cluster head, any of the node in cluster head can send the data to reach the base station via another cluster head. Here randomly cluster head are selected for each recycling once completed.

3.3 Authentication process for cluster communication

- In this module, each node transmits encrypted data with appended digital signature to base station through cluster head using RCS protocols.

- The encrypted sensed data is authenticated by applying digital signature to message

  packets, which are efficient for communication and applying the key management

  for security based on energy aware route placed.

- Here shortest path message forwarding and secure message forwarding scheme are done using localization algorithm.

3.4 Data Transmission and Recycling using localization algorithm

- Source node in cluster head sends encrypted data to base station via cluster head. For example ch2 transmit data to base station via ch1. After data transmission in cluster head, the base station conducts recycling process. In that process, it checks sub node and cluster head energy level.

- Also passive and active attacks are verified from the Inter or Intra cluster communication. Then base station selects alternate cluster head in that group based on threshold value if genuine node occurred. So old cluster head act as sub node in that group. Then these new cluster head selects it neighbors cluster heads and sub nodes id also changed based on time stamp followed. After cluster head selection data transmission is continued packet transmission on the base station.

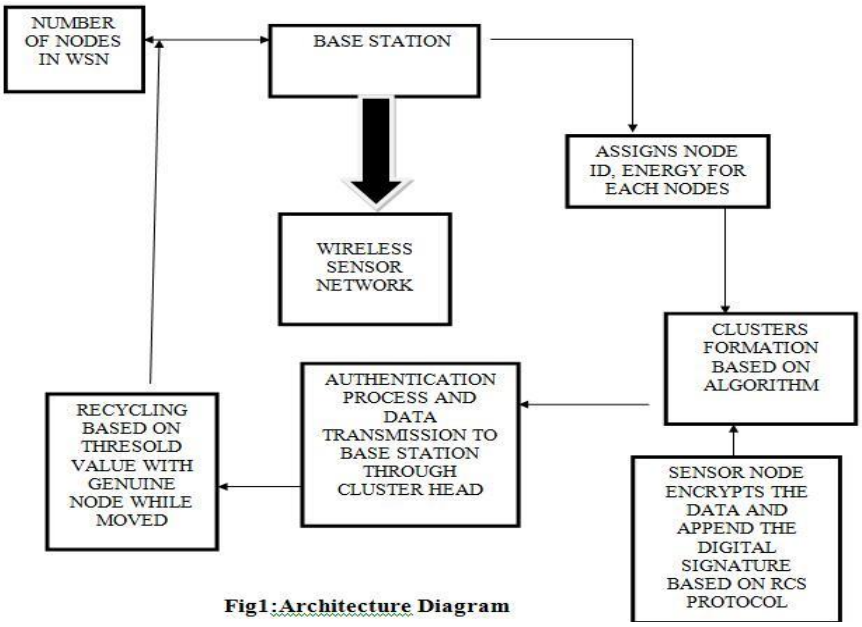

NUMBER OF NODES IN WSN
BASE STATION
ASSIGNS NODE ID, ENERGY FOR EACH NODES
WIRELESS SENSOR NETWORK
CLUSTERS FORMATION BASED ON ALGORITHM
AUTHENTICATION PROCESS AND DATA TRANSMISSION TO BASE STATION THROUGH CLUSTER HEAD
RECYCLING BASED ON THRESOLD VALUE WITH GENUINE NODE WHILE MOVED
SENSOR NODE ENCRYPTS THE DATA AND APPEND THE DIGITAL SIGNATURE BASED ON RCS PROTOCOL

Fig1:Architecture Diagram

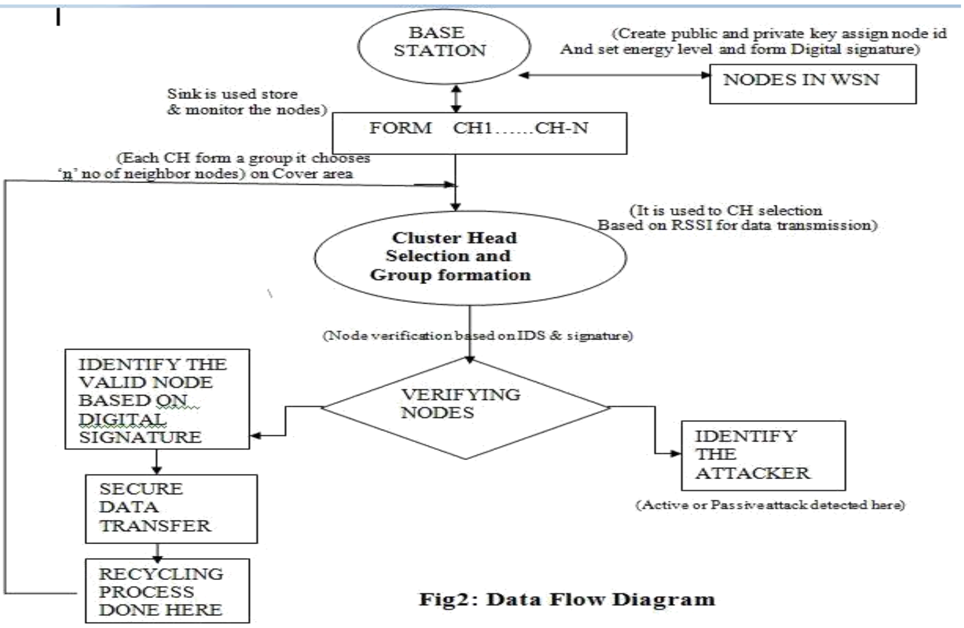

BASE STATION
(Create public and private key assign node id And set energy level and form Digital signature)
NODES IN WSN
Sink is used store & monitor the nodes)
FORM CH1……CH-N
(Each CH form a group it chooses 'n' no of neighbor nodes) on Cover area
(It is used to CH selection Based on RSSI for data transmission)
Cluster Head Selection and Group formation
(Node verification based on IDS & signature)
IDENTIFY THE VALID NODE BASED ON DIGITAL SIGNATURE
VERIFYING NODES
IDENTIFY THE ATTACKER
(Active or Passive attack detected here)
SECURE DATA TRANSFER
RECYCLING PROCESS DONE HERE

Fig2: Data Flow Diagram

IV. TABLE

Simulation Parameters:

Parameter	Value
Network Size	200m x 200m
Number of Nodes	99
Node Distribution	Uniformly Distributed
Sink Position	At (100m,100m)
Initial Energy	100J
Data Rate	250kbps
Packet Size	46Bytes
Transmission Interval	1000 seconds
Transmission Range	Upto 50 meter
Transmit Power	0dbm

V. PERFORMANCE EVALUATION

In this section, we evaluate the performance of simulation. We are using the graph for evaluate the performance. We choose the four evaluation metrics:

1.**Energy consumption-** the energy consumption rate for sensors in a wireless sensor network varies greatly based on the protocols the sensors use for communication.

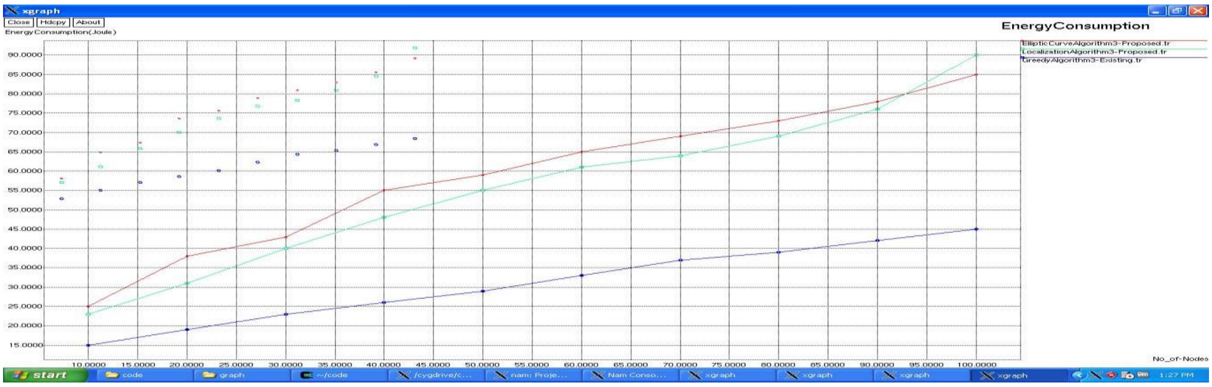
2.Packet delivery ratio – it is the ratio of the number of packet received at destination and number of packet sent by the source.

3.End-to-End delay – the average time taken for a packet to be transmitted from the source to destination,

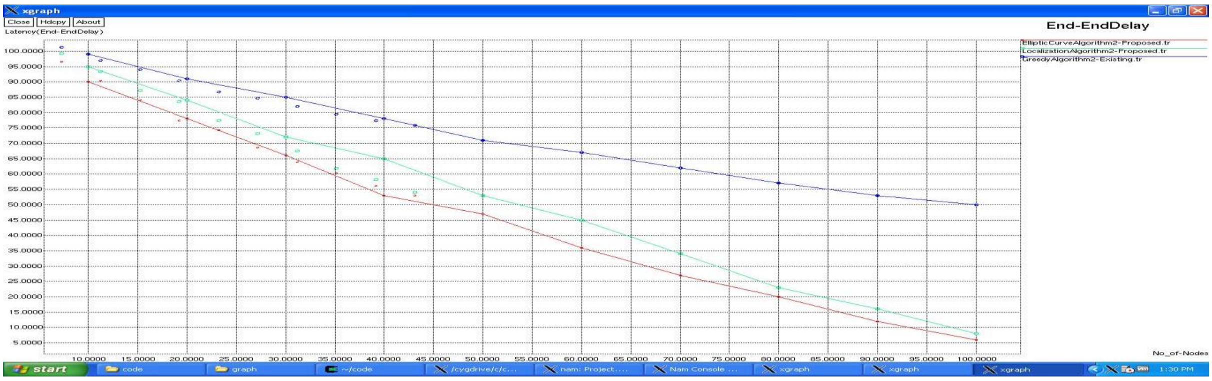
4. Throughput – number of data received by the destination without any losses.

5.1 COMPARATIVE GRAPH FOR EXISTING AND PROPOSED SYSTEM:

A.FOR ENERGY CONSUMPTION

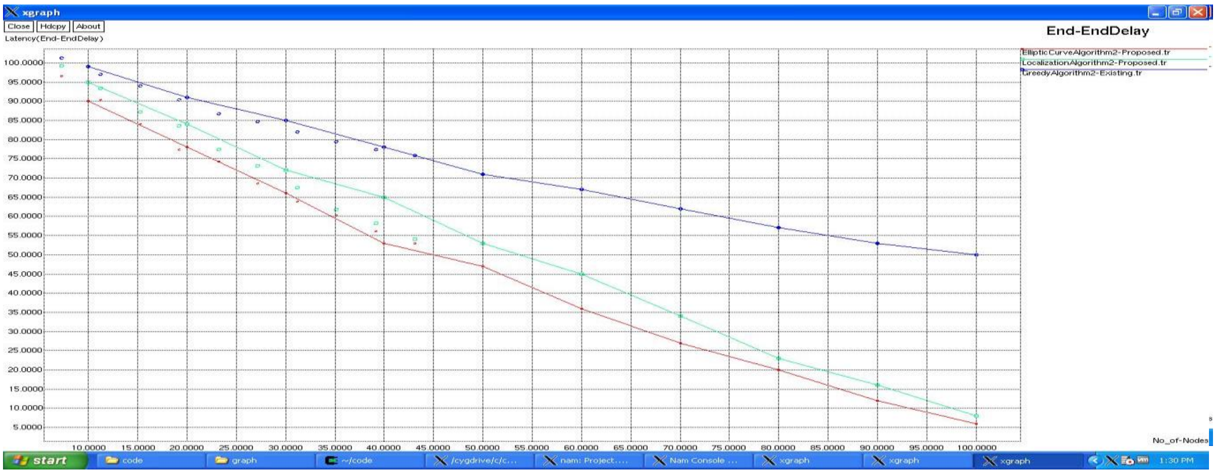


B. FOR END -TO-END DELAY:



C. FOR PACKET DELIVERY RATIO:

D. FOR THROUGHPUT:



VI. CONCLUSION AND FUTURE WORK

6.1 CONCLUSION:

Thus, the proposed system of combining the deterministic shortest path algorithm with high energy balance and MES Elliptic curve cryptographic algorithm can provide 80% highly secure message transfer from source to node and also the pattern encoding method ensures authentication of the message.

6.2 FUTURE WORK:

The future goal of the project is to provide source location privacy. Many new techniques have been devised to enhance source-location privacy in sensor network routing. One of our strategies, called phantom routing, has proven flexible and capable of protecting the source's location, while not a sustainable noticeable increase in energy overhead. Phantom routing techniques yield improved source-location privacy relative to other routing protocols. The basic idea of this method is that once a node decides to become a fake source, it will keep generating fake messages regularly so that attacker may be misled .The main goal behind the phantom techniques is to entice the hunter away from the source towards a phantom source.

REFERENCES

[1] G. J. Pottie and W. J. Kaiser, "Wireless integrated network sensors," Commun. ACM, vol. 43, no. 5, pp. 51–58, May 2000.

[2] W. R. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "Energyefficient communication protocol for wireless micro sensor networks," in Proc. 33rd Annu. Hawaii Int. Conf. Syst. Sci., Jan. 2000, p. 8020.

[3] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless sensor networks: A survey," Comput. Netw., vol. 38, no. 12, pp. 393–422, Aug. 2002.

[4] Hung, C.C., K.J. Lin, C.C. Hsu, C.F. Chou and C.J. Tu, 2010. "On enhancing network-lifetime using opportunistic routing in wireless sensor networks," in Computer Communications and Networks (ICCCN), 2010 Proceedings of 19th International Conference on, Aug.

[5] Li, Y., Y. Yang and X. Lu, 2010. "Rules of designing routing metrics for greedy, face, and combined greedy-face routing," Mobile Computing, IEEE Transactions on, 9(4): 582–595.

[6] Liu, F., C.Y. Tsui and Y.J. Zhang, 2010. "Joint routing and sleep scheduling for lifetime maximization of wireless sensor networks," Wireless communications, IEEE Transactions on, 9(7): 2258– 2267.