Key Management and Reducing the Hop Count Using IBS Algorithm in Heterogeneous Wireless Network

M. Suganya[1] Mr. M. Premanand[2]
[1]M.E Student (Applied Electronics) [2]Assistant Professor
[1,2]Department of Electronics & Communication Engineering
[1,2]Kalaignar Karunanidhi Institute of Technology, Coimbatore, India

Abstract— An efficient hop count route finding approach for heterogeneous wireless sensor network is Presented .It is an routing protocol that has a tradeoff between transmission power and hop count for heterogeneous wireless networks. The nodes can dynamically assigning transmission power to each node along the route, and then the node will receive the request message. After receiving its request message the node compares its power with the threshold power value and select a particular route. The IBS algorithm is an effective solution to heterogeneous wireless networks for secured data sending through reasonably selected path to reduce the delay using the key management technique. Simulation results indicate that can deliver better performance with respect to data privacy.

Key words: heterogeneous WSN, IBS algorithm, key management, hop-count, threshold power

I. INTRODUCTION

In terms of wireless sensor networks, resources such as bandwidth, power, computing ability for nodes are limited by the environments and hardware. Make it difficult to establish and maintain the communications through the multiple intermediate nodes which are mobile devices Transmission range of nodes will change over time in real wireless networks. In this network, there is no regular infrastructure such as base stations or mobile switching centers, each node only has a limited radio propagation distance, limited power of battery, and nodes can move freely.

Researchers generally assume that the nodes in wireless sensor networks are homogeneous, but in reality, homogeneous sensor networks hardly exist. Even homogeneous sensors have different capabilities like different levels of initial energy, depletion rate, etc. In heterogeneous sensor networks, typically, a large number of inexpensive nodes perform sensing, while a few nodes having more energy perform data filtering, fusion and transport. In general, routing in WSNs can be divided into flat-based routing, hierarchical-based routing, and location-based routing depending on the network structure. In hierarchical-based routing, however, nodes will play different roles in the network. In location-based routing, sensor nodes' positions are exploited to route data in the network.

A routing protocol is considered adaptive if certain system parameters can be controlled in order to adapt to the current network conditions and available energy levels. Furthermore, these protocols can be classified into multipath-based, query-based, negotiation-based, QoS-based, or coherent-based routing techniques depending on the protocol operation. Fig.1 illustrates that the number of hops which passing from one router to the other. In computer networking, a hop is one portion of the path between source and destination. Data packets pass through routers and gateways on the way. Each time packets are passed to the next device, a hop occurs.

II. RELATED WORK

The hop count refers to the intermediate devices like routers through which data must pass between source and destination, rather than flowing directly over a single wire. Each router along the data path constitutes a hop, as the data is moved from one network to another. Hop count is therefore a basic measurement of distance in a network. Hop count is a rough measure of distance between two hosts.

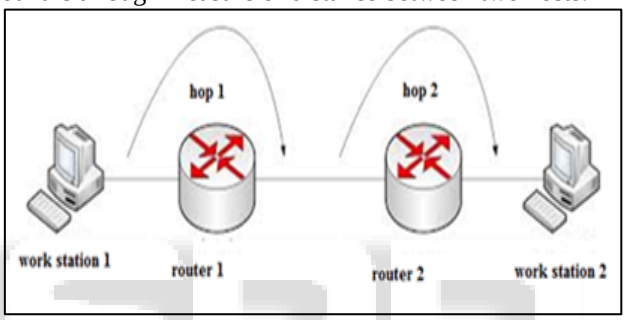

Fig. 1: Image of hop count

A. *RREQ Extension:*

A source node broadcasts a RREQ packet. When an intermediate node receives the first RREQ packet, it records a reverse route in its routing table and re-broadcasts the packet. On the other hand, when the intermediate node receives a delayed RREQ packet from other neighbors, it firstly checks a source route list in the packet and discards the packet when a routing loop is detected If this address check is passed, the intermediate node then checks reverse routes already stored in its routing table.

B. *RREP Extension:*

A destination node receiving RREQ packets generates multiple RREP packets toward a source node. The first arriving RREQ packet is unconditionally accepted and a RREP packet is immediately generated to create a primary route. Delayed RREQ packets are conditionally accepted and limit the number of RREP packets. Operation of an intermediate node is slightly complicated. In principle, the intermediate node receiving a RREP packet forwards it to any neighboring nodes over the reverse routes. When the intermediate node receives a delayed RREP packet, it checks a specified metric condition and decides acceptance of the packet.

III. PROPOSED METHOD

In wireless heterogeneous networks may have nodes with different power and their transmission range is not same that is nothing but the communication radius Through the use of

long-range links, the number of hops on the path will be reduced. They consider the use of long range transport may increase energy consumption and reduce overall network throughput, which can solve the problem of asymmetric links, and make rational and effective use of heterogeneous nodes. sometimes high-power node can send information to low-power node, when the node transmission range of the low-power cannot reach the distance between two nodes, the feedback information cannot be sent back to high-power node.

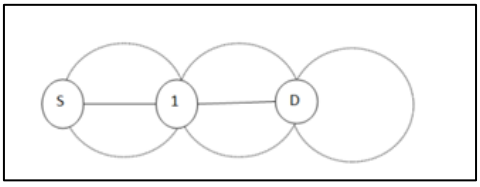

Fig. 2: High transmission power versus minimum hop counts

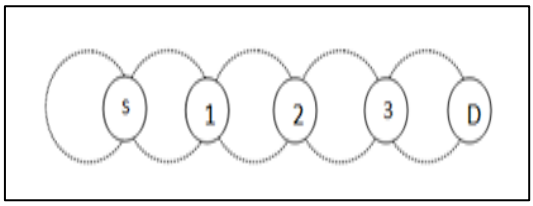

Fig. 3: Low Transmission power versus maximum hop counts

Fig.2 representing the transmission power versus hop counts. which determine the high transmission power reducing the number of hop counts and reducing the overhead and Fig.3 representing the lower transmission power which increases the number of hop counts and its take long time to reach the destination.

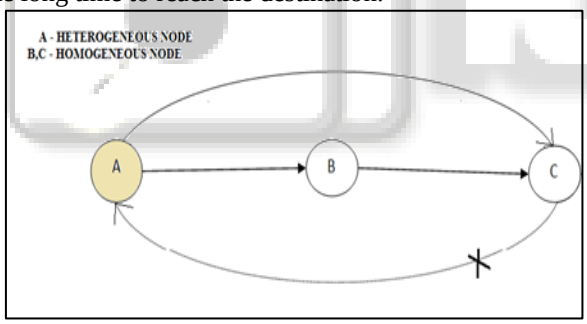

Fig. 4: Heterogeneous nodes in wireless sensor network

Fig.4 shows the heterogeneous nodes in wireless sensor network. In the homogeneous network, the routing protocol will choose the path A-B-C. But in the heterogeneous network, node A sends RREQ to node C directly. suppose the protocol is based on symmetric network, the heterogeneous network will not work properly. That is the RREP message from Node C cannot be received by node A. Therefore, the path discovery process fails.

Key management is used for security purpose for sending the data. They are having the pool of key for security and so they are having very good authentication, confidentiality. Key distribution are more suitable for large groups. Key establishment is the key issue of the secure communication, reducing the computational overhead and so delay reduced.

Key generation is the process of generating keys for cryptography. A key is used to encrypt and decrypt whatever data is being encrypted/decrypted. Modern cryptographic systems include symmetric-key algorithms and public-key algorithms . Symmetric-key algorithms use a single shared key; keeping data secret requires keeping this key secret. Public-key algorithms use a public key and a private key. The public key is made available to anyone . A sender encrypts data with the public key; only the holder of the private key can decrypt this data. Computer cryptography uses integers for keys. In some cases keys are randomly generated using a random number generator (RNG) or pseudorandom number generator (PRNG).A computer algorithm that produces data that appears random under analysis. PRNG that use system entropy to seed data generally produce better results, since this makes the initial conditions of the PRNG much more difficult for an attacker to guess.

The key management method is security for the data and it contains the pool of keys , which having lots of key and so the authentication is very high. compare to RSA algorithm the IBS method contains different key size that is 32 bit to 64 bit key length.

Key management method which additionally add the numbers or symbols for high security because of this the intruders will not hack the data easily.

IV. FLOWCHART FOR PROPOSED METHOD

The flow diagram fig.5 illustrates the proposed system and the steps are explained below:

1) STEP 1: Starting the process.
2) STEP 2: Creating the nodes.
3) STEP 3: Initialize the sequence number for each node.
4) STEP 4: Sink node send the Route Request (RREQ) to other node for transmitting the data.
5) STEP 5: The receiving node check the sequence number whether it is correct or not. If the number is correct that means YES, then accept the RREQ and send Route Reply (RPLY) to the sink node.
6) STEP 6: If the sequence number is incorrect that means NO, then the receiving node will discard the RREQ.
7) STEP 7: Stop the process.

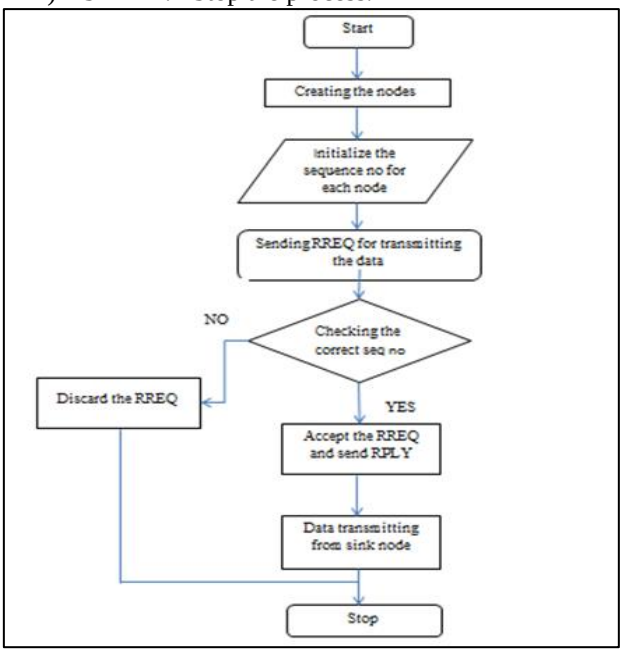

Fig. 5: Flow diagram of proposed system

V. PROPOSED ALGORITHM

IBS-Identity Based Digital Signature Algorithm which having 16 bit and 32 bit usage.IBOOS-Identity Based Online/Offline Digital Signature Pool will contain all the key .It can give the key when it is needed and send the data quickly, which is crucial for wireless sensor network while it security relies on the hardness of discrete problem and security analyses against various attacks.

1) Setup: The BS as a trust authority generates a master key msk and public parameters for the private key generator and gives them to all sensor nodes.
2) Extraction: Given an ID string, a sensor node generates a private key sek ID associated with the ID using msk.
3) Signature signing: Given a message M, time-stamp t and a signing key θ, the sending node generates a signature.
4) Verification: Given the ID, M and SIG, the receiving node outputs "accept" if signature is valid, and outputs "reject" otherwise.

VI. SIMULATION RESULT AND DISCUSSION

In this section the simulation results are taken using NS2 tool. The node which assign the sink node according to the variation of time and then taken the output results of pairwise key generation between the nodes and finally, the output result of distance calculation between the nodes are shown below.

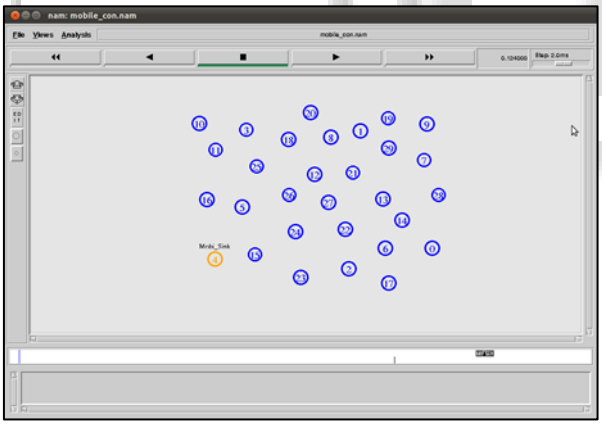

Fig. 6: Arrangement of nodes

Fig. 6 shows the arrangement of nodes .There are 30 nodes are presented in the figure, that is numbered as (0 to 29). The node 4 can be considered as sink node is called mobi-sink and each node having the unique address.

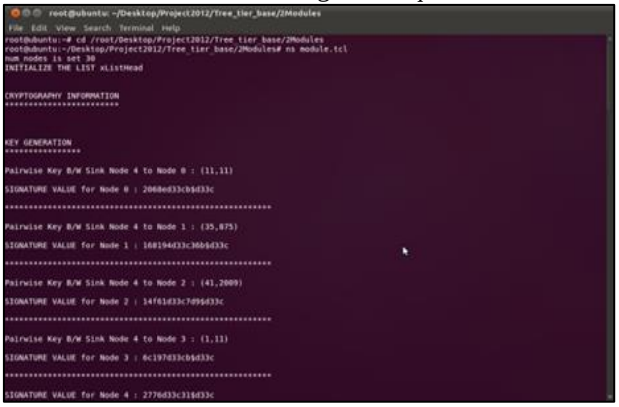

Fig. 7: pair-wise key between the nodes

Fig.7 shows a pair-wise key between the nodes. This means that each mobile device and access point needs to store one pair-wise key. The Fig.7 shows the pair-wise key between the sink node (mobile node) and the access point; here the sink node is 4.

Signature value is used for privacy purpose, the pair-wise key can match each node from the network, whether the signature value is correct are not, by comparing the value which already stored from the sink node, if not the node will not accept the request.

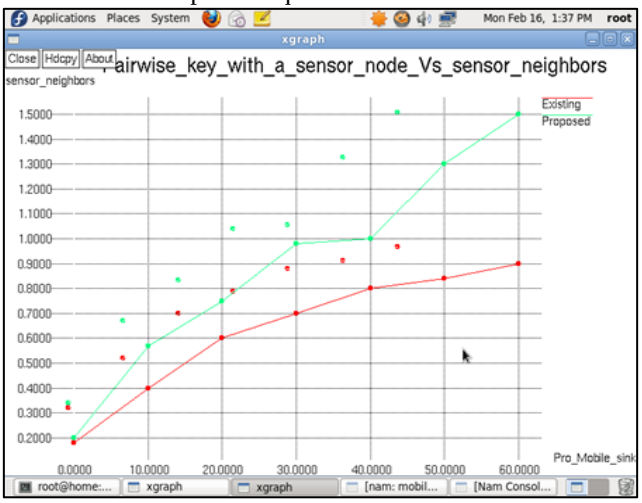

Fig. 8: graph for sensor nodes Vs sensor neighbors

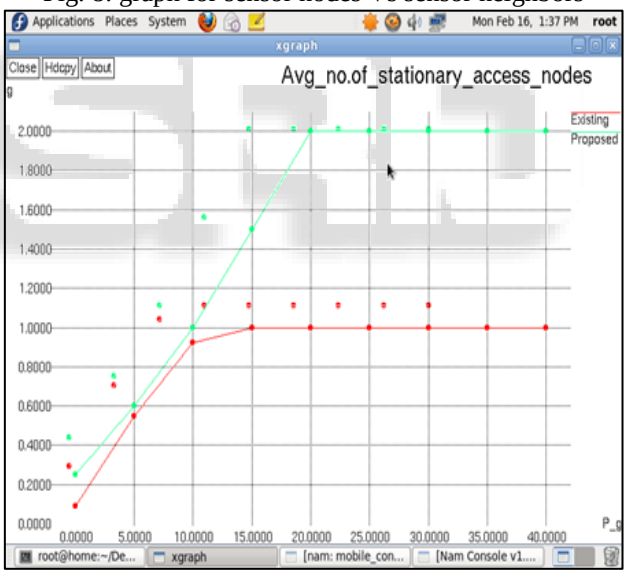

Fig. 9: Number of access nodes

Using the key management technique for security purpose with the help of IBS protocols they improved the access nodes and so the failure of data can be reduced In future work, the sink node can dynamically assign transmission power to nodes along the route.

Through the use of long-range links, the number of hops on the path will be reduced. They consider the use of long range transport may increase energy consumption and reduce overall network throughput, which can solve the problem of asymmetric links, and make rational and effective use of heterogeneous nodes.

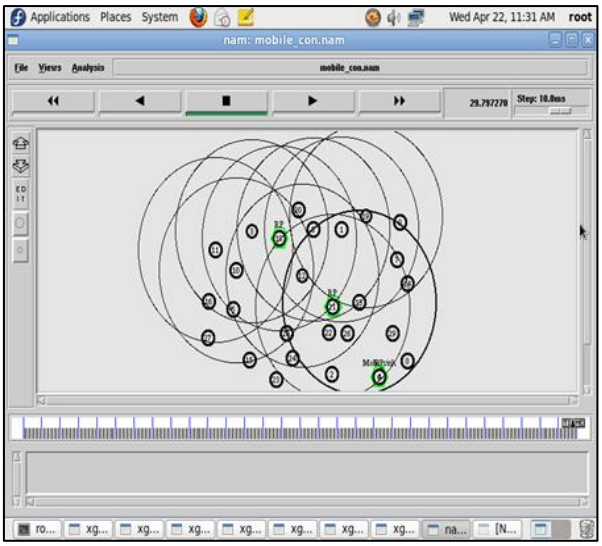

Fig. 10: Rendezvous point in wireless sensor network

The node who has received route request message compares its power with the threshold power value, and then selects a reasonable route according to IBS algorithms.

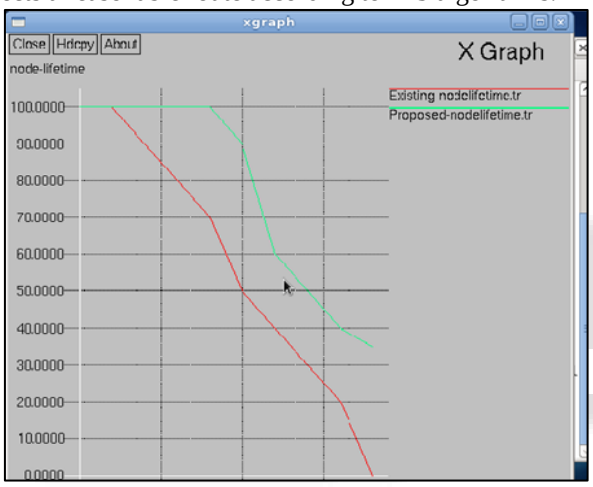

Fig. 10: comparison graph of lifetime node

The figure 10 shows the comparison graph of lifetime node. This algorithm is an effective solution scheme to wireless heterogeneous networks through reasonably selected path to reduce network consumption. Which reduce the traffic overhead and reach the destination point quickly and reduce the end to end delay.

In future work, plan to enhance our approach to include data with different delay requirements. This means a mobile sink is required to visit some sensor nodes or parts of a WSN more frequently than others while ensuring that energy usage is minimized, and all data are collected within a given deadline. Moreover, plan to extend WRP to the multiple mobile sinks/rovers case. This case, however, is nontrivial as it involves sub problems such as interference and coordination between rovers. Having said that, note that WRP remains applicable if a large WSN is partitioned into smaller areas where each area is assigned a mobile sink. WRP can be thus run in each area. Defer the evaluation of such an approach to a future paper.

REFERENCES

[1] Abusaimeh H and Yang S.H. (2009) 'Dynamic cluster head for lifetime efficiency in WSN', Journal of Automation and Computing, Vol. 6, No. 1, pp. 48–54.
[2] Choudhary S and Qureshi S. (2012) 'Performance evaluation of meshbasedNoCs: Implementation of a new architecture and routing algorithm',Journal of Automation and Computing,Vol. 9, No. 4, pp. 403–413.
[3] Hasan M.S , Harding C et-al (2005) 'Modeling delay and packet drop in networked control systems using network simulator NS2',Journal of Automation and Computing, Vol. 2, No. 2, pp. 187–194, 2005.
[4] Hekmat R and Mieghem P.V. (2003) 'Degree distribution and hopcount in wireless ad-hoc networks',Sydney, NSW, Australia, pp. 603–609.
[5] Johnson D.B and Maltz D.A. (1996) 'Dynamic source routing in ad hoc wireless networks' Mobile Computing,Vol. 353, pp. 153–181.
[6] Marina M.K and Das S.R. (2002) 'Routing performance in the presence of unidirectional links in multihop wireless networks', USA, pp. 12–23.
[7] Meghanathan N. (2010) 'Impact of the Gauss-Markov mobility model on network connectivity, lifetime and hop count of routes for mobile ad hoc networks',Journal of Networks,Vol. 5, No. 5, pp. 509–516.

