Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 11, November 2014, pg.367 – 376

RESEARCH ARTICLE

EFFICIENT PRIVACY PRESERVING AND ACO BASED ROUTING TO IMPROVE THE LIFETIME EFFICIENCY OF GRID WIRELESS COMMUNICATION

Miss. T. Sahana*, Mrs. A. Sankareswari, M.C.A., M.Phil.******

*M.Phil(Computer Science), Research Scholar
Vivekanandha College for Women, Unjanai, Tiruchengode, India
******Assistant Professor in Computer Science
Vivekanandha College for Women, Unjanai, Tiruchengode, India

ABSTRACT: ***Wireless Sensor Networks consisting of nodes with limited power are deployed to gather useful information from the field. It is applied in routing and difficult power supply area that cannot be reached and some temporary situations, which do not need fixed network supporting and it can fast deploy with strong anti-damage. In order to avoid the problem proposed a new technique called Bio-Inspired mechanism for routing. Modified Hash-Message Authentication Code (HMAC) algorithm is used to increase the security in the network. By finding the shortest path during the process of communication between the nodes the delay is reduced and the Energy Efficiency is greatly increased. Modified and colored ACO is one of the Bio-inspired mechanisms. By using the Modified Ant Colony Optimization Algorithm the shortest path between the nodes are identified. Then applying the nodes in that shortest path, the energy of the individual nodes is saved and the life time of that node is increased. The main goal is to maintain the maximum lifetime of network, during data transmission in the efficient manner. This paper defines implementation of WSN and comparison of its performance with Ad-hoc On Demand distance Vector (AODV) routing protocol based on ANT algorithm is done in terms of packet delivery ratio, throughput and energy level.***

Keywords: HMAC, ACO, WSN, AODV, ANT Algorithm

1. INTRODUCTION

A Wireless network is any type of computer network that uses wireless data connections for connecting network nodes. Wireless telecommunications networks are generally implemented and administered using radio communication. This implementation takes place at the physical level (layer) of the OSI model network structure. Wireless sensor networks (WSN) are composed of independent sensor nodes deployed in an area working collectively in order to monitor different environmental and physical conditions such as motion, temperature, pressure, vibration sound or pollutants. The main reason in the advancement of wireless sensor network was military applications in battlefields in the beginning but now the application area is extended to other fields including industrial monitoring, controlling of traffic and health monitoring.

1.1 Sensor Node Components

There are various sensor nodes having capabilities regarding power of microcontroller, radio and capacity of memory. Despite of the variances it can be said that there are four basic sub- systems of sensor nodes: computing subsystem, sensing subsystem, power subsystem and communication subsystem.

Controlling Component: In order to control the components of the sensor nodes and perform the required computations this subsystem is responsible for it. There are two sub-units, storage unit and processor unit. There are different operational modes of processors in sensor nodes. They are either Idle, Active or in Sleep modes. In order to preserve power this is important, so processor operates when required.

Communication Component: The sensor nodes due to this component interact with the base station and to the other nodes. Usually this subsystem is a radio of short range but other fields has also been explored like ultrasound, infrared communication and inductive fields.

Power Component: Power is supplied to sensor nodes by this sub-system in which a battery is contained. Every aspect of the network regarding communication algorithms, sensing devices, localization algorithms should be efficient in terms of energy usage because replacement or recharging of battery is unfeasible in case where large numbers of sensor nodes are deployed. For recharging of battery onsite a power generator should be included.

Sensing Component: In this sub-system the physical phenomena is converted to electrical signals by sensor transducers. So the outside world is linked to this subsystem. Sensors may have analog or digital output. There should be an Analog to Digital Converter (ADC) in case if output is analog.

1.2 Wireless Sensor Network Applications

Monitoring of Area: The common application of WSNs is monitoring of area. The events occurring in the environment are monitored by the sensor nodes deployed in the region. Monitoring of area involves detecting enemy intrusion by a large number of sensor nodes deployed over a battlefield.

Monitoring of Environment: A large scale wireless sensor networks are deployed for environmental monitoring including forest fire/flood detection, monitoring of the condition of soil and space exploration.

Applications in Commercial Area: Wireless Sensor Networks have a lot of applications concerning commercial are such as office/home smart environments, health applications, controlling of environment in buildings, monitoring of industrial plants.

Tracking Applications: In tracking area, WSN applications include targeting in intelligent ammunition and tracing of doctors and patients inside a hospital.

2. LITERATURE SURVEY

Tiago Camilo, Carlos Carreto, Jorge Silva, and Fernando Boavida. ACO is one of the Bio-inspired mechanisms. ACO is a dynamic and reliable protocol. It can avoid network congestion and fast consumption of energy of individual node. ACO algorithm reduces the energy consumption, the main goal is to maintain the maximum lifetime of network, during data transmission in an efficient manner. Dorigo, M., Maniezzo, V., Colorni Comparing their performance with respect to the original ACO and other commercial routing algorithms like RIP and OSPF. The simulation results indicate a better throughput. S. Singh and Meenaxi. Ant colony optimization is a technique for optimization that was introduced in the early 1990's. The

inspiring source of ant colony optimization is the foraging behaviour of real ant colonies. I. D. Chakeres and E. M. Belding-Royer. ACO is an innovative algorithm for packet routing in communication networks. Comparing their performance with respect to the original ACO and other commercial routing algorithms like RIP and OSPF. The simulation results indicate a better throughput. Many routing protocols in mobile ad-hoc networks have been developed by many researchers. One of ad-hoc routing protocol types is the on-demand routing that establishes a route to a destination node only when required. Ant Colony Optimization (ACO) is a class of optimization algorithms modelled on the actions of an ant colony in a swarm intelligence approach. ACO methods are useful in problems that need to find paths to some goals. In nature ants leave pheromones trails on the path they took to find food and back again to colony. First ACO algorithms aimed to solve the travelling salesman problem and the goal was to find the shortest round trip between series of cities.

3. PROTOCOLS AND ALGORITHM

3.1 AODV Routing Protocol

There are two types of routing protocols which are reactive and proactive. In reactive routing protocols the routes are created only when source wants to send data to destination whereas proactive routing protocols are table driven. Being a reactive routing protocol AODV uses traditional routing tables, one entry per destination and sequence numbers are used to determine whether routing information is up-to-date and to prevent routing loops. Control messages used for the discovery and breakage of route are as follows

- Route Request Message (RREQ)
- Route Reply Message (RREP)
- Route Error Message (RERR)
- HELLO Messages.

Route Request (RREQ) A route request packet is flooded through the network when a route is not available for the destination from source

Route Reply (RREP) On having a valid route to the destination or if the node is destination, a RREP message is sent to the source by the node.

Route Error Message (RERR) The neighbourhood nodes are monitored. When a route that is active is lost, the neighbourhood nodes are notified by Route Error Message (RERR) on both sides of link.

HELLO Messages The HELLO messages are broadcasted in order to know neighbourhood nodes. The neighbourhood nodes are directly communicated.

3.2 Bio-Inspired Algorithm

ANT COLONY OPTIMIZATION (ACO) Swarm Intelligence (SI) is the local interaction of many simple agents to achieve a global goal. SI is based on social insect metaphor for solving different types of problems. The basic idea of the ant colony optimization (ACO) meta-heuristic is taken from the food searching behaviour of real ants. The basic idea of the ant colony optimization (ACO) meta-heuristic is taken from the food searching behaviour of real ants. Ant agents can be divided into two sections: FANT (Forward Ants) and BANT (Backward Ants). The main purpose of this subdivision of these agents is to allow the BANTs to utilize the useful information gathered by FANTs on their trip time from source to destination Based on this principle; no node routing information updates are performed by FANT, whose only purpose in life is to report network delay conditions to BANT. The various steps how these agents are passing routing information to each other are as follows

1. Each network node launches FANT to all destinations at regular time intervals.

2. Ants find a path to destination randomly based on current routing tables.

Ant Algorithm:

```
Loop
   Randomly position m artificial ants on n cities
   For city=1 to n
      For ant=1 to m
        {Each ant builds a solution by adding one city after
        the other}
         Select probabilistically the next city according to
                        exploration and exploitation mechanism
         Apply the local trail updating rule
      End for
  End for
  Apply the global trail updating rule using the best ant
Until End_condition
```

3.3 Modified HMAC Algorithm

The Access control Mechanism is based on the process of network security. The Modified HMAC algorithm is used to increase the network security. It is one of the cryptography based algorithm. The performance Analysis is done after the compilation. That shows, that the proposed method performed well when it compared to the existing method. In cryptography, a Keyed-Hash Message Authentication Code (HMAC) is a specific construction for calculating a message authentication code (MAC) involving a cryptographic hash function in combination with a secret cryptographic key.

Design Principle: The design of the HMAC specification was motivated by the existence of attacks on more trivial mechanisms for combining a key with a hash function. One might assume the same security that HMAC provides could be achieved with MAC = H(key ‖ message).

Security: The cryptographic strength of the HMAC depends upon the size of the secret key that is used. The most common attack against HMACs is brute force to uncover the secret key. HMACs are substantially less affected by collisions than their underlying hashing algorithms alone.

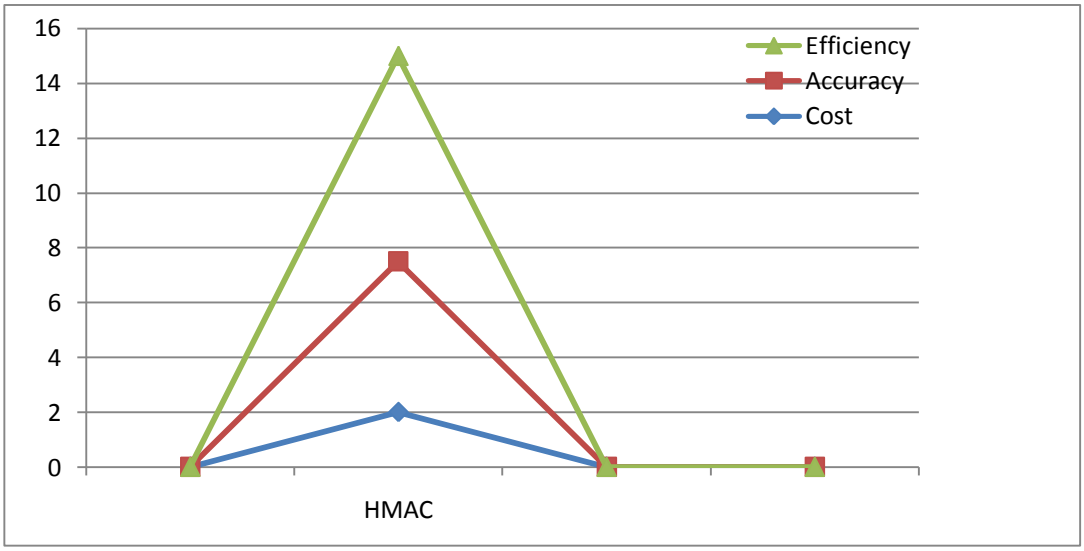

```
function hmac (key, message)
   if (length(key) > blocksize) then
      key = hash(key) // keys longer than blocksize are shortened
   end if
   if (length(key) < blocksize) then
      key = key ∥ [0x00 * (blocksize - length(key))] // keys shorter than blocksize are
                                                        zero-padded
                                  (where ∥ is concatenation)
   end if

   o_key_pad = [0x5c * blocksize] ⊕ key // Where blocksize is that of the underlying
                                           hash function
   i_key_pad = [0x36 * blocksize] ⊕ key // Where ⊕ is exclusive or (XOR)

   return hash(o_key_pad ∥ hash(i_key_pad ∥ message)) // Where ∥ is concatenation
end function
```

4. EXPERIMENTS AND RESULT

MRMS topology discovery is partially based on the three colour algorithm used in Top Disc, which is derived from the simple greedy log (n)-approximation algorithm for finding the set cover. At the end of the Top Disc topology discovery process, the sensor network is divided into n clusters and each cluster is represented by one node, which is called the cluster head. The cluster head is able to reach all the nodes in the cluster directly because they are all within its communicate on range. Each cluster head knows its sink, but they cannot communicate with each other directly. Instead a delivery node (the grey node) acts as an intermediary which delivers messages between each pair of head node. In the MRMS topology discovery mechanism, unlike Top Disc, the cluster is stateless because the cluster head will not maintain any children. Instead every sensor will not previous hop and corresponding sink in its routing table, this approach reduces the complexity of cluster reconstruction described in the next section. Thus each cluster can be considered a virtual node as far as the topology is concerned. A sensor node may keep information for more than one cluster heads and sinks in the routing table, as it can keep track of different paths from different sink nodes. However only one of these paths

can be designated the primary path in the table, and this is the path with the minimum path cost, hence ensuring the topology will be an energy efficient one.

Comparison in terms of cost, Accuracy and Security in the proposed methods



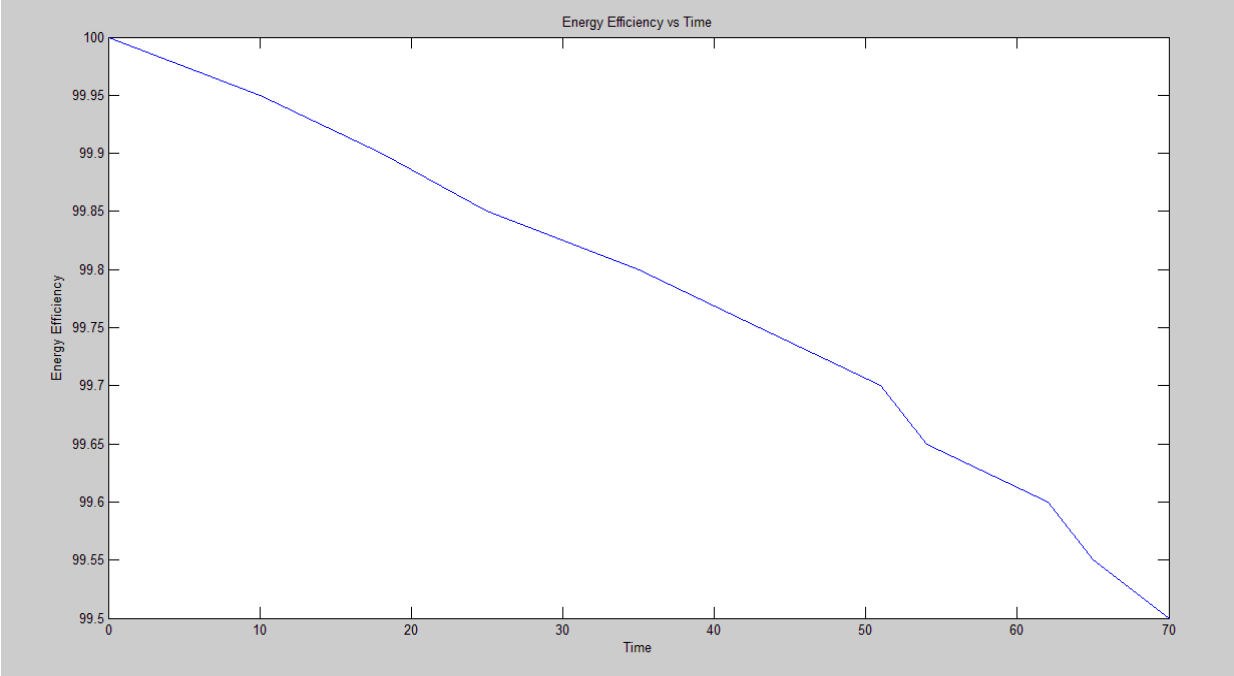
The Graph represents the Cost, Accuracy and the Efficiency of the HMAC algorithm.

Bandwidth calculation in BAR graph

The Bar chart represents the Bandwidth calculation when compared with the existing and the proposed method. Here the proposed method performed much better in terms of bandwidth with several time periods.

Energy Calculation in BAR graph

The Bar chart represents the Energy calculation when compared with the existing and the proposed method. Here the proposed method performed much better in terms of Energy efficiency with several time periods.



5. CONCLUSION AND FUTURE ENHANCEMENT

The protocol is achieved by using ACO algorithm to optimize routing paths, providing an effective multi-path with Multi-sink and clustering concept for data transmission to obtain reliable communications in the case of node faults. Aimed to maintain network life time in maximum, while data transmission is achieved efficiently. This study was concluded to evaluate the performance of ant based algorithm and AODV routing protocol in terms of Packet Delivery Ratio and Normalized Routing Load. From the comparison it is concluded that overall performance of ant based algorithm is better than AODV. The proposed algorithm can control the overhead generated by ants and improved packet delivery ratio. The future work could be to investigate different methods to further limit the traffic or load and compare the ant based algorithm for other proactive and reactive routing protocols.

REFERENCES

1. Ahmed A Ahmed, Hongchi Shi, and Yi Shang, **"A Survey On Network Protocols For Wireless Sensor Networks"** In Information Technology: Research and Education, 2013. Proceedings. ITRE2003. International Conference on, pages 301–305. IEEE, 2013.

2. Tiago Camilo, Carlos Carreto, Jorge Silva, and Fernando Boavida, **"An Energy-Efficient Ant-Based Routing Algorithm For Wireless Sensor Networks"** Ant Colony Optimization and Swarm Intelligence, pages 49–59, 2011.

3. Enan A Khalil and Baraa A Attea, **"Energy-Aware Evolutionary Routing Protocol For Dynamic Clustering Of Wireless Sensor Networks"** Swarm and Evolutionary Computation, 1(4):195–203, 2011.

4. Yingqi Lu, Du Zhang, Ya Chen, Xiao Liu, and Ping Zong, **"Improvement Of Leach In Wireless Sensor Networks Based On Balanced Energy Strategy"** In Information and Automation (ICIA), 2012 International Conference on, pages 111–115. IEEE, 2012.

5. Song MAO and Cheng-lin ZHAO, **"Unequal Clustering Algorithm For WSN Based On Fuzzy Logic And Improved ACO"** The Journal of China Universities of Posts and Telecommunications, 18(6):89–97, 2011.

6. Basma M Mohammad El-Basioni, Sherine M Abd Elkader, Hussein S Eissa, and Mohammed M Zahra, **"An Optimized Energy-Aware Routing Protocol For Wireless Sensor Network"** Egyptian Informatics Journal, 12(2):61–72, 2011.

