Journal of Engineering Science and Technology
Vol. 10, No. 9 (2015) 1224 - 1238

ENERGY EFFICIENT IMPROVEMENT GEOCAST FORWARDING IN MANET BASED ON A CLUSTERED STRUCTURE

PRASANTH K., SIVAKUMAR P.*

Department of Electronics and communication, SKP Engineering College,
Anna university- Chennai, Tiruvannamalai, India
*Corresponding Author: sivakumar.poruran@gmail.com

Abstract

Mobile sinks (MSs) are very important in many wireless sensor network (WSN) applications for efficient data gathering, restricted sensor reprogramming, and for characteristic and revoking compromised sensors. This paper presents a secure and energy-efficient geocast forwarding for MANET based on a hierarchical clustered structure with reduction of packet dropping from the base station (BS) and access Point (AP) all nodes placed in one or more geocast regions. Our protocol is composed of two major parts which are protects from attackers and allow over all energy savings. First of all the hierarchical formation based on cliques and a concept of data aggregation allows us to build a robust, fast and secure foundation for routing of information. Next geocast diffusion itself provides data forwarding and reduced a research phase in the network that is a step of sending data(s). Our protocol performs better in terms of less broadcast rounds overhead. For security a three-tier general framework is used, that permit utilize of any pair wise key pre distribution plan as its indispensable component. The innovative framework requires two disconnect key pools, solitary for to access the network, and one for pair wise key establishment between the sensors. To decrease the compensation caused by reproduction attacks we encompass strengthened the authentication device between the sensor nodes and the stationary access node (AP) in the planned framework. Through in depth analysis, we show that our security framework has top network flexibility to a mobile sink reproduction attack as compared to the two-tier general frame work. The analysis is done using network simulator 2 (NS2) and it is a packet level simulator with trace level analysis.

Keywords: Energy consumption, Geocast, Hierarchical clustering, Security, MANET, Three-tire, Access point.

1. Introduction

The wireless sensor networks (WSN) are beginning the family of mobile ad-hoc (MANET), other than have extra features and constraints: characteristically, they consist of a wide range of sensors with limited energy capacity. Each sensor is powered from a battery non-rechargeable and non-replaceable [1] and has a low capacity in terms of memory, calculation (CPU), and transmission range. Each sensor is able to harvest a set of data in a certain environment, and transmit it in multi-hop way to a base station (BS) or sink, which may act as instructor of the network. The use of such networks is widespread in many applications. For example we can mention the monitoring of forests, health monitoring [2], critical infrastructure, habitat monitoring [1], or the detection of biochemical agents and in the military industries, data acquisition in hazardous environments. Some examples of work can be found through [3-6]. The sensed information often requires to be sent back to the base station for investigation. but, while the sensing meadow is too far since the base station, transmit the information over stretched distances via multi hop could deteriorate the protection strength (e.g., a few intermediary might alter the information passing by, capture sensor nodes, introduction a Sybil attack [7], wormhole attack [8], selective forwarding [9, 10], sinkhole [11]), and rising the energy spending at nodes close to the base station, dropping the lifetime of the system.

In such a system, the security is a critical position to we require revising and putting onward. In detail, WSN contain numerous constraints such as the communication standard, which is wireless: at the present time it is extremely straightforward to understand, catch and smooth adapt the information transmitted, in addition to concession an entire system. Permit us insert to these inconveniences the sensors submission framework, which are frequently deployed in aggressive environments. Thus in attendance is a want to secure the protocols, in categorize to assurance authentication, interactions privacy [12, 13], data reliability and network accessibility. Established schemes in ad hoc networks with asymmetric keys are costly due to their computation cost and storage. These boundaries build key predistribution scheme [14-19] the tools of alternative to tender low cost, protected communication stuck between movable sensor sinks.

Objective of this paper is to solve some of above problem. We initially refined a common three-tier security framework for pair wise key establishment and authentication, based on the polynomial pool-based key predistribution format [16]. The stationary access point, act as authentication access points to the network, to trigger the sensor nodes to transmit their aggregated data to movable sensor sinks. A movable sensor sink sends information demand messages to another movable sensor node via a stationary access point. These information demand messages from the movable sensor sink will initiate the stationary access point to trigger sensor nodes, which transmit their data to the requested movable sensor sink. The system use separate polynomial pools for movable sensor. Figure 1 shows the wireless sensor network with three-tire security. The access point changes the polynomial pool-based key predistribution format with in a fraction of second.

The expertise associated to sensor networks advance day by day, it is ordinary to see WSN collected of numerous thousand units [20, 21]. In huge networks, the sensors know how to be grouped into cluster based on their closeness to tender a enhanced administration and information transmissions in sort to considerably

amplify the scalability, financial system of energy, routing, and accordingly the lifetime of the system, e.g.,. [22-24]). To preserve steadiness, minimal hierarchy is formed in each cluster, everywhere the members agree on a head: a cluster-head (CH for small), which is in charge for organization all members of its cluster and to hold away from cluster outwards function.

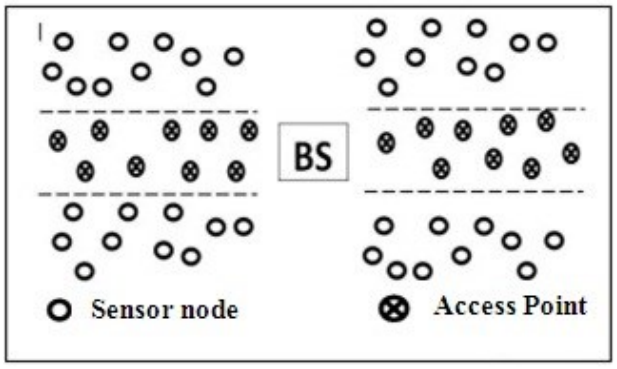


Fig. 1. The three-tire security scheme architecture.

In this article we examine a process of transmitting information, the geocasting (or geographical forwarding) that guarantees the information deliverance to every sensor positioned at one or more than a few exact location of a network(geocast regions). To reach this objective we superpose to data aggregation clustered architectures. The cluster is formed based on energy in the cluster structure used as the cluster of Level 1 [1] and clusters of Level 2 [1] and superior. The arrangement provided by the employ of clusters allows the use of dissimilar approach compared to what is normally optional in the literature. The protocol that we present takes the main lines of [25], but is protected and intelligent to shun a preponderance of attacks [26]. Certainly, in adding together to combining the indispensable feature of security, our protocol is energy-efficient. The multi cluster arrangement in which is based our protocol helps to reduce the broadcast overhead to the local structures move toward with positive geocast regions proposed in [27] that yield gigantic broadcast rounds overhead.

This paper is prepared as follows. Section 2 presents geocast forwarding performed in base station, access point and within a cluster. Section 3 presents the cluster structure formation with selection of cluster head, with algorithms. Section 4 describes three-tire security scheme. Section 5 discussed about the stimulations. Section 6 shows about the performance measure using X-graph.

2. Geocast Forwarding

The geocast forwarding is initializing in the source node to the access point then access point will examine the authentication to particular information then it passed to the base station then base station will distribute to other access point. which in twist spread the information to their hold neighbors and so on, pending all sensors in the geocast regions are reached and include knowledge of the information. Imielinski and Navas [28] and Ko and Vaidya [29] try to decrease

the on the whole costs caused by flooding, which are very important, besides the obvious aspect of flooding. We used two geocast forwarding protocol to reduce the information overhead. We use geographic routing to resource fully distribute the geocast packet to the region. In adding up, our definite delivery algorithm is based on geographic features (as well call perimeter) routing. Consequently we offer next a brief overview about geographic routing protocols. Geographic routing consists of greedy forwarding, where nodes move the packet closer to the destination at each hop by forwarding to the neighbor closest to the destination. Greedy forwarding fails when reaching a dead-end (local maximum), a node that has no neighbors closer to the destination. A face routing algorithm [30] that guarantees unicast information save on a geometric graph by traversing the limits of planar faces intersect the line stuck between the source and the destination.

For geocasting we provided an algorithm for enumerating every one of edges, faces and vertices of a associated planar graph intersecting a area. The geographic routing protocol for wireless Networks that mechanism in two modes: greedy mode and perimeter mode. In greedy mode every node forwards the packet to the neighbour adjoining to the destination. When greedy forwarding is not possible, the packet switches to perimeter mode, where perimeter routing is worn to route approximately dead-ends until closer nodes to the destination are found. In perimeter mode a packet is forwarded using the Right-hand rule in a planar embedding of the network.

We present two narrative algorithms for geocasting in wireless networks. The initial algorithm Geographic-Forwarding-Geocast (GFG) [30] has roughly finest minimum overhead and is idyllic for opaque networks. The second algorithm Geographic Forwarding-Perimeter-Geocast (GFPG) [31] provides assured delivery in associated networks level at low concentration or asymmetrical distributions through gaps or obstacles.

2.1. Geographic-forwarding-geocast (GFG)

In geocast application, nodes are probable to be responsive of their geographic area. Geographic-Forwarding-Geocast utilizes this geographic information to frontward packets professionally in the direction of the geocast region. A geographic routing protocol consisting of greedy forwarding with perimeter routing such as GPSR [30] is used by nodes outer surface the area to certification the forwarding of the packet to the section. Nodes within the section broadcast the packet to flood the section.

In supplementary factor, a node wishing to throw a geocast creates a packet and puts the coordinates of the section in the frame header. Then it forwards the packet to the neighbour adjoining to the target. The target of geographic routing in this container is the section centre. Apiece node sequentially forwards the information to the neighbour closest to the target using greedy forwarding. When greedy forwarding fails, perimeter routing is worn to direction roughly dull trimmings until quicker nodes to the target are found. Eventually (in holder present are nodes surrounded by the region) the information will enter the region. The primary node to accept the geocast packet within the area starts flooding the region by broadcasting to all neighbour (otherwise we can use elegant flooding [30]). All nodes within the area that receives the information for the first time broadcasts it to

its neighbour and nodes outer surface the section remove the packet. Figure 2 shows the format of geocast forwarding in geographic region (S-source).

In opaque networks lacking obstacles or gaps, GFG is enough to convey the packet to all nodes in the area. In totalling, because in opaque networks geographic routes are close to optimal routes (shortest path), GFG has roughly the lowest amount overhead a geocast algorithm can have which largely consists of the lowly numeral of hops to reach the area plus the number of nodes within the area itself. In regulate for GFG to supply just right delivery (i.e. every one of nodes in the area receive the geocast packet), the nodes in an area need to be associated mutually such that every node can attain all supplementary nodes without going out of the area. In dense networks normally this requirement is satisfied, but in sparse networks or due to obstacles, regions may have gaps such that a path between two nodes inside the region may have to go through other nodes outside the region as shown in Fig. 3. In case of region gaps, GFG will fail to provide perfect delivery.

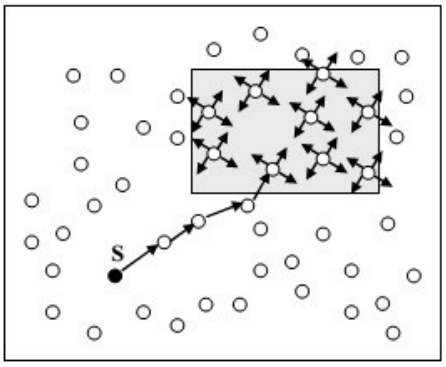


Fig. 2. Geographic forwarding is used to deliver the packet to the region.

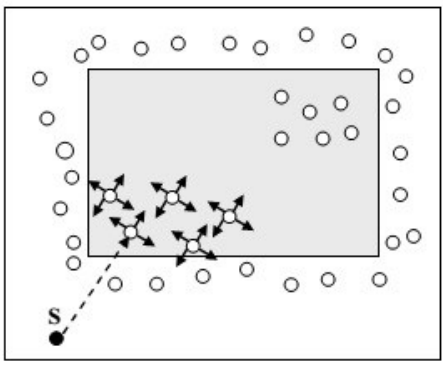


Fig. 3. Disconnection in the geocast region.

2.2. Geographic-forwarding-perimeter-geocast (GFPG)

We here an algorithm that guarantees the deliverance of a geocast packet to all nodes within the geocast region, have known that the network as a whole is

connected. The algorithm solves the region gap trouble in thin networks, except it causes unnecessary overhead in opaque networks. The algorithm provides ideal delivery at all densities and keeps the overhead low in dense networks. This algorithm uses a combine of geocast and perimeter routing to assurance the delivery of the geocast packet to all nodes in the region. Thus if a packet is sent in perimeter mode by a node on the gap edging, it will go roughly the gap and traverse the nodes on the other side of the gap. Figure 4 shows the method of perimeter connection.

Initially, similar to GFG, nodes outer surface of the geocast region use geographic forwarding to forward the packet toward the area. As the packet enters the area, nodes flood it within the area. All nodes in the region broadcast the packet to their nearby nodes similar to GFG, in accumulation, nodes on the edge of the area sends perimeter mode packets to their neighbour that are outer surface of the area. A node is an area border node if it has neighbour outside of the region. By sending perimeter packets to neighbour outside the region in Fig. 5 (observe that perimeter mode packets are sent only to nearby in the planar graph not to all physical neighbour), the faces intersecting the area border are traversed. The node outer surface the area, receiving the perimeter mode packet, forwards the packet using the right-hand rule to its neighbour in the planar graph and that neighbour forwards it to its neighbour and so on. The packet goes around the face until it enters the region again. The first node inside the region to receive the perimeter packet floods it inside the region or ignores it if that packet was already received and flooded before. This way if the region consists of separated clusters of nodes, a geocast packet will start at one cluster, perimeter routes will connect these clusters together through nodes outside the region, and each cluster will be flooded as the geocast packet enters it for the first time. This guarantees that all nodes in the region receive the packet, since perimeter packets going out of the region will have to enter the region again from the opposite side of the face and accordingly all faces intersecting the region will be covered.

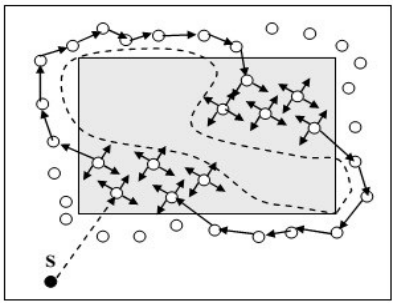


Fig. 4. Perimeter routing connects separated clusters.

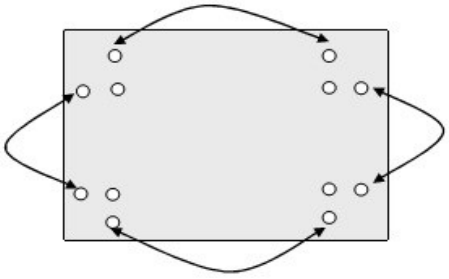


Fig. 5. Mix of region flooding and perimeter routing.

3. Cluster Structure

Investigate on WSNs has developed quickly and fresh techniques have been improved for the data-gathering and finding nearest path. Multihopping scheme is chosen between these techniques, which the data is routed in a cluster level manner. All nodes with the sensor in WSNs are separated into various clusters in which CHs (cluster heads) receive, information, and forward the traffic originated by cluster

members to the destination. This sort of hierarchy clustering topology is simply managed and has fine scalability. Aspire is to extend the network's duration by minimizing the transmission control. However, numerous clustering protocols primarily center on stationary sensor nodes or prohibited movable for hop-count reduction in data gathering. Mobile sensor nodes are required in applications where sensors are deployed on erratically moving stuff for monitoring, tracking, and other purposes [32]. For example, wireless sensor strategies have been fixed to bikes, vehicles, and animals. Additional applications connecting humans as participants can be flu-virus tracking or air-quality monitoring.

The cluster structure is formed based on the data aggregation. The Aggregated data like energy, next hop, location, ID. Formation of the cluster contains of two steps, the first election of cluster head and second within a range of CH are cluster members. Cluster head is selected based on two parameters, namely the counts and location of the sensor node. There are two algorithms to election of cluster head, Cluster-head election by counting and Cluster-head election with location.

3.1. Cluster-head election by counting

This part describes the algorithm of cluster-head election by counting. Suppose that the amount of sensor nodes in a dynamic sensor network is M and we give the sensor nodes from the count of 0 to M−1. Every sensor node therefore can use the assigned number as a single identifier (ID) in the sensor network. We suppose that there are C clusters in each movement with the ID's, algorithm elect the sensor nodes as the cluster-heads in a round-robin method. In additional words, in the first change, the sensor nodes through ID's from 0 to C−1 are the cluster-heads. In the second change, the sensor nodes with ID's from C to 2C−1 are the cluster-heads. The algorithm continues for the next changes.

Algorithm

BEGIN:

C: the number of**CH** (Cluster Head) in an area.

M: total number of nodes.

M_{CH}=0 /* cluster head count */

WhileM_{CH}<C **do**

(Sensor ID)t_{ID} = (t_{ID}+1) mod M

if (t_{ID}=0) **then**

Now t is a cluster head.

Advertisement is given in network.

Increase in M_{CH} by 1.

End if

Wait for change in network.

If(change in network) **then**

Increase M_{CH} by 1.

End if

End while

End if

3.2. Cluster head election with location

We here describe a distributed algorithm of cluster-head election with location, which is particularly for dynamic sensor nodes. The necessary plan is to use the node mobility to have all sensor nodes be a cluster-head in turns. Known some fixed reference points in the location of the mobile sensor network, the sensor nodes nearby to these reference points will be the cluster-heads, correspondingly, when electing the cluster-heads. To reach this, we regard as to set the remoteness of a sensor node to a reference point (rp) as the metric of the delay time, which is worn when a sensor node contends a channel. The decision is hence also a product of the channel contention among sensor nodes. Figure 6 shows the simple cluster location with group of movable sensor nodes with cluster head (CH), reference point (rp) and distance (d).

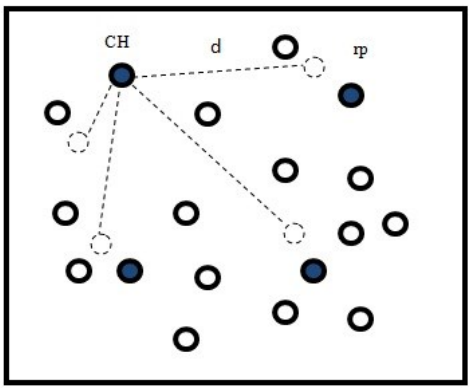


Fig. 6. Cluster head election based on reference point.

4. Security Scheme

For security scheme the three tire security scheme is applied. Which contains of base station, access point (AP) and finally group of dynamic sensor nodes (MANET), Dynamic sensor nodes form the cluster structure. The connection is established by AP and cluster head, which provide the authentication between these nodes. The subset of polynomials from the polynomial pool is picked by each cluster head. The randomly selected sensor nodes called access point carry a polynomial from the polynomial pool. These nodes acts as the authentication point for the network which triggers the sensor node to transmit the data. The data request is transmitted to cluster head from the sensor node through stationary access point. This data request will initiate the sensor node to transmit the collected data. Every stationary access point may share a polynomial with a mobile sensor destination. The main benefit to use pools is the mobile sensor authentication is autonomous of the key distribution scheme used to unite the sensor network. We divide our scheme into two stages: polynomial predistribution and key discovery among mobile sensor nodes.

4.1. Polynomial predistribution

Stage 1 is performed earlier than the nodes are deployed. A polynomial pool P of size mod-P is generated along with the polynomial identifiers. All cluster head and

stationary access point randomly given K_p and one polynomial (K_p>1) from P. The amount of polynomials in every cluster head is extra than the quantity of polynomials in every stationary access point. This assures that a cluster head shares a widespread polynomial with a stationary access point with high probability and reduces the number of compromised cluster head polynomials when the stationary access point shares captured. All sensor nodes and the preselected stationary access point randomly pick a subset of K_s and Ks1 polynomials from P.

Blundo's Scheme [33] is the main scheme used for finding the polynomial share of each node. Every node is assigned with an id. And the steps of this scheme are given below.(finite field- Zp, unique ID – rU, rV, polynomial share-gu(x)).

1. Each node has an id rU which is unique and is a member of finite field Zp.
2. Three elements a,b,c are chosen from Zp.
3. Polynomial f(x,y) = (a + b(x + y) + cxy) mod p is generated, where P is a prime.
4. For each node, polynomial share gu(x) = (an+ bnx) mod p Where an= (a+brU) mod p and bn= (b + crU) mod p is formed and pre-distributed .
5. In order for node U to be able to communicate with node
6. V the following computations have to be performed:
7. Ku,v= Kv,u= f(ru,rv) = (a + b(ru+rv) + crurv)mod p.
8. U computes Ku,v= gu(rv).
9. V computes Kv,u= gv(ru)
10. If Ku,v=Kv,u , then the nodes share the same polynomial and then they can establish communication.

4.2. Key discovery

To set up a direct pair wise key [34] beginning one cluster head (CH1) to an extra cluster head (CH2). A cluster head (CH) want to discover a stationary access point (AP) within its range, such that AP can launch pair wise key with sensor nodes (CH). Figure 7 shows a direct secure path establishment among sensor nodes sends the pair wise key; AP betweenCH1 and AP. if AP receives the over message and it shares a pair wise key with CH1 it sends the pair wise key to CH2 in a message encrypted and authenticated with pair wise key; CH2 between AP and CH2.

Figure 8 illustrates that the CH1 and the CH2 will have to establish a pair wise key with help of intermediate [34] AP using indirect key discovery. To establish pair wise key with cluster head CH2 has to find a stationary access point AP in its neighbourhoods such that AP1 can establish a pair wise key with both nodes CH2 and CH1. If AP1 establishes a pair wise key with only CH1 and not with CH2. As the probability is high that the AP1 can discover a common polynomial with CH1, CH2 need to find an intermediate AP2 along the path CH2-AP2-AP1-CH1, such that intermediate AP2 can establish a direct pair wise key with AP1.

Figure 9 shows that the cluster head and member of the cluster sensor node (n) will have to establish a pair wise key with the help of CH using indirect key discovery [34].To establish a pair wise key with sensor node within a range of cluster head (CH2), a cluster head (CH1) has to find a stationary AP in its neighbourhoods such that AP can establish a pair wise key with both CH1 and CH2. If AP establishes a pair wise key with only CH1 and not with CH2. As the probability is high that the AP can discover a common polynomial with CH1,

sensor need to find an intermediate CH2 along the path n-CH2-AP-CH1,such that intermediate CH2 can establish a direct pair wise key with AP.

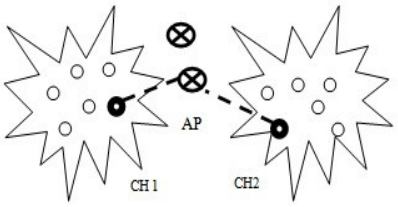


Fig.7. Direct secure path establishment.

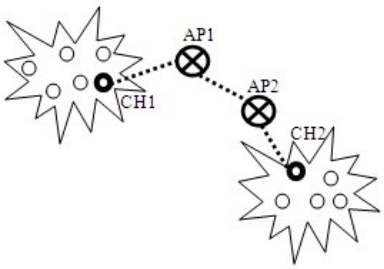


Fig. 8. Establish a pair wise key with help of intermediate point.

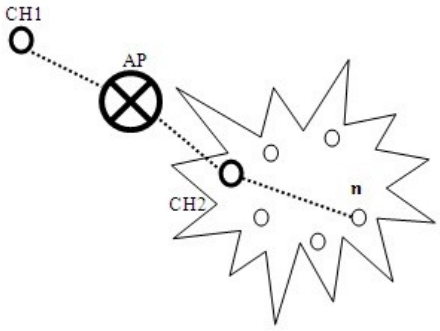


Fig. 9. Indirect key discovery.

5. Simulation

Network Simulator (Version 2), extensively recognized as NS2 [35, 36], is just an event determined simulation tool that has proved use full in study the dynamic environment of communication networks. Performance is measured using the trace files. In NS2 contains two types of trace files, there are text level trace file contains the delay, time of arrival, ID of source and destination. This text trace file contains trace frame formats, above mentioned parameters will be in that frame [36]. The second trace file is NAM (network animator) this used for visualize the network as per the coding.

5.1. Performance measure

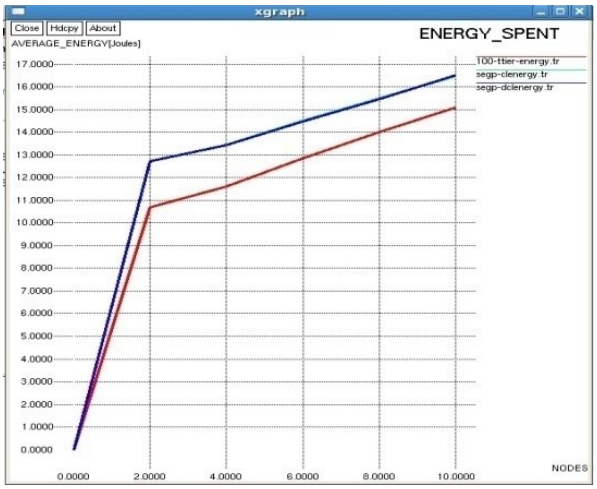
Performance measure is done in NS2 using awk file. AWK is an interpreted programming language designed for text processing and typically used as a data extraction and reporting tool. Awk in NS-2 takes the trace file for analysis, handles complex task such as calculation, database handling, report creation. Awk programming can be used to analyze the metrics of any network connection. They are throughput, end to end delay, packet delivery ratio and energy.

5.2. X-Graph

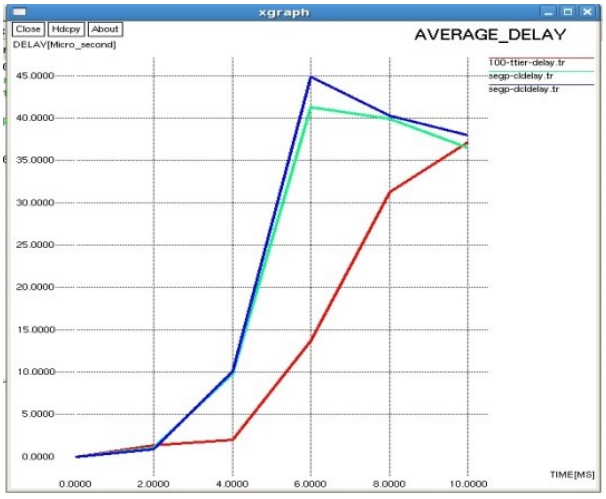
The X-graph is generated using NS2 packages from the trace files a value has been plotted as graph. In this graph we examine the comparison of the three tier system with static and dynamic two tier system.

6. Results and Discussion

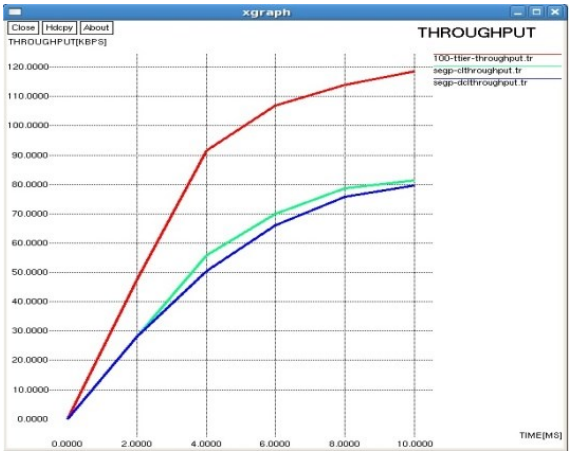
Comparing three-tier with the two-tier the throughput is increased is shown in Fig. 10. Average delay of each node is decreased from source to destination comparing with two tier system. The delivery of packets is outperformed compared with two-tier system. Energy spent is also reduced for mobile sensor node by this clustering algorithm when this algorithm is included with Sybil Attack [37].



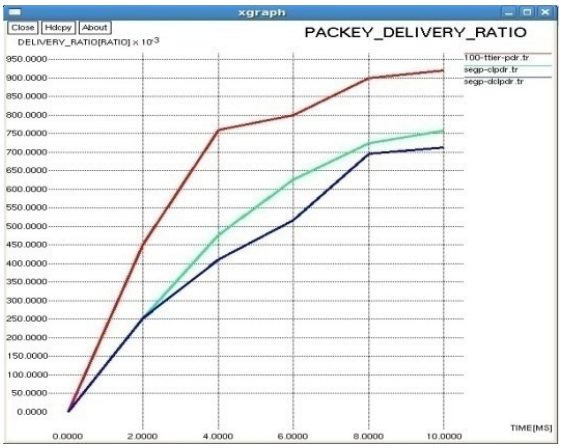
(a) Average delay.



(b) Energy spent.



(c) Packet delivery ratio.



(d) Throughput.

Fig. 10. Comparisons of three-tier system with static and dynamic two-tier system.

7. Conclusion

In this document, the security scheme move towards making it promising to carry out in trouble-free and hasty manner in geocast forwarding in Base station, Access point, and in final single sensor node. The hierarchical cluster structure on which our protocol is based allows a distributed use of the network, and especially efficient use, for a control always ensured by BS, AP and cluster head. We provide distributed clustering algorithms which lead less energy dissipation for data-gathering in a cluster-based mobile sensor network. Based on the polynomial pool-based key Pre distribution scheme substantially improves network throughput to protract from attacks compared to the two tire security scheme. Using separate key pools and having few stationary access point carrying polynomials from the cluster head in the network may hinder an attacker from gathering sensor data, by deploying a replicated mobile sink.

References

1. Akyildiz, I.F.; Su, W.; Sankara subramaniam, Y.; and Cayirci, E. (2002). Wireless sensor networks: a Survey. *Computer Networks,* 38(4), 393-422.
2. Gao, T.; Greenspan, D.; Welesh, M.; Juang, R.R.; and Alm. A. (2005). Vital signs monitoring and patient tracking over a wireless network. *Proceedings of IEEE 27th annual International Conference of Engineering Medicine and Biology Society*. (EMBS).
3. Agre, J.; and Clare, L. (2002). An integrated architecture for cooperative sensing networks. *IEEE Computer*, 33(5), 106-108.
4. Akyildiz, I.F.; Su, W.; Sankarasubramaniam, Y.; and Cayirci. E. (2002). Wireless sensor networks: A survey. *Computer Networks,* 38(4), 393-422.
5. Intanagonwiwat, C.; Govindan R.; and Estrin, D. (2000). Directed diffusion: A scalable and robust communication paradigm for sensor networks. *In proceedings of MOBICOM'*, 56-67.
6. Shen, C.C.; Srisathapornphat, C.; and Jaikaeo, C. (2000). Sensor information networking architecture and applications. *IEEE Personal Communications*, 52-59.
7. Douceur, J.R. (2002). The Sybil attack. *Proceedings of First International Workshop Peer-to Peer Systems* (IPTPS '02).
8. Hu, L.; and Evans, D. (2004). Using directional antenna to prevent wormhole attacks. *Proceedings of network and distributed system security symposium*.
9. Culpepper, B.J.; and Tseng, H.C. (2004). Sinkhole intrusion indicators in DSR MANETs. *Proceedings of First International Conference on Broadband Networks (BroadNets '04)*, 681-688.
10. Deng, H.; Li, W.; and Agrawal, D.P. (2002). Routing security in wireless Ad hoc networks. *Proceedings of IEEE Communication Magazine*, 70-75.
11. Intanagonwiwat, C.; Govindan, R.; and Estrin, D. (2000). Directed diffusion: a scalable and robust communication paradigm for sensor networks. *Proceedings of Mobile Computing and Networking,* 56-67.
12. Li, C.; Wang, Z.; and Yang, C. (2011). Secure routing for wireless mesh networks. *International Journal of Network Security*, 13(2), 109-120.
13. Saroit, I.A.; El-Zoghdy, S.F.; and Matar, M. (2011). A scalable and distributed security protocol for multicast communications. *International Journal of Network Security*, 12(2), 61-74.
14. Eschenauer, L.; and Gligor, V.D. (2002). A key-management scheme for distributed sensor networks, *Proceedings of ACM Conference on Computer and Communications Security (CCS'02),* 41-47.
15. Chan, H.; Perrig, A.; and Song, D. (2003). Random key pre-distribution schemes for sensor networks, *Proceedings of IEEE Symposium on Research in Security and Privacy*.
16. Chan, H.; Perrig, A.; and Song. D. (2004). Kluwer academic key distribution techniques for sensor networks. *Wireless Sensor Networks*, 277-303.
17. Liu, D.; and Ning, P. (2003). Location-based pair wise key establishments for static sensor networks. *Proceedings of First ACM Workshop Security AD HOC and Sensor Networks.*

18. Zhu, S.; Setia, S.; and Jajodia, S. (2003). LEAP: Efficient security mechanisms for large-scale distributed sensor networks. *Proceedings of 10th ACM Conference on Computers and Communications Security (CCS '03),* 62-72.
19. Rasheed, A.; and Mahapatra, R. (2008). An efficient key distribution scheme for establishing pair wise keys with a mobile sink in distributed sensor networks. *Proceedings of IEEE 27th International Performance Computing and Communications Conference (IPCCC '08)*, 264-270.
20. Kahn, J.M.; Katz, R.H.; and Pister, K.S.J. (1999). Mobile networking for smart dust. *In Proceedings of MOBICOM'* 99, 17-19.
21. Warneke, B.; Last, M.; Leibowitz, B.; and Pister, K. (2001). Smart dust: communicating with a cubic-millimeter computer. *IEEE Computers,* 34, 44-51.
22. Manjeshwar, A.; and Agrawal, D.; TEEN (2001). A protocol for enhanced efficiency in WSN. I*n Proceedings of the 15th International Parallel & Distributed Processing Symposium*, 23-27.
23. Tirta, Y.; Li, Z.; Lu, Y.; and Bagchi, S. (2004). Efficient collection of sensor data in remote fields using mobile collectors, *Proceedings of 13th International Conference on Computer Communications and Networks (ICCCN '04)*.
24. Heinzelman, W.R.; Chandrakasan, A.; and Balakrishnan, H. (2000). Energy efficient communication protocol for wireless micro sensor networks. *In Proceedings of the 33th IEEE Hawaii International Conference on Systems*, 3005-3014.
25. Bomgni, A.B.; and Myoupo, J.F. (2010). An energy-efficient clique-based geocast algorithm for dense sensor networks. *Communications and Network*, 2, 125-13.
26. Schoch, E.; Kargl, F.; Leinmuller, T.; and Weber, M. (2007). Vulnerabilities of geocast message distribution, *2nd IEEE* W*orkshop on Automotive Networking and Applications*, 1-8.
27. Shim, Y.C. (2009). Secure and energy efficient geo cast protocol for sensor networks with misbehaving nodes, *International Journal of Communications*, 2, 222-229.
28. Imielinski, T.; and Navas, J. (1996). GPS-based addressing and routing. *RFC 2009 Computer Science, Rutgers University Press, Rutgers*.
29. Ko, Y.B.; and Vaidya, N.H. (2002). Flooding-based geo casting protocols for mobile ad hoc networks. *MANET*, 7(6), 471-480.
30. Seada, K.; and Helmy, A. (2004). Efficient geo casting with perfect delivery in wireless networks, *IEEE Wireless Communications and Networking Conference*, 2551-2556.
31. Stojmenovic, I. (2004). Geo casting with guaranteed delivery in sensor networks. *IEEE Wireless Communications*, 11(6), 29-37.
32. Ma, C.; Liu, N.; and Ruan, Y. (2013). A dynamic and energy-efficient clustering algorithm in large-scale mobile sensor networks. *International Journal of Distributed Sensor Networks*, Article ID 909243, 8 pages.
33. Blundo, C.; De Santis, A.; Herzberg, A.; Kutt-en, S.; Vaccaro, U.; and Yung, M. (1993). Perfectly secure key distribution for dynamic conferences.

Proceedings of 12th Annual International Cryptology Conference on Advances in Cryptology (CRYPTO'92), 471-486.

34. Rasheed, A.; and Mahapatra, R.N. (2012). The three-tier security scheme in wireless sensor networks with mobile sinks. *IEEE parallel and distributed system*, 23(5), 958-965.
35. Ke, Z.; Cheng, R.; and Deng, D. (2008). NS2 simulation experiment. *Electronic Industry Press*, Beijing, China.
36. Fang, L.; Liu, S.; and Chen, P. (2008). Basis and applications of NS-2 network simulation, *National Defense Industry Press,* Beijing, China
37. Douceur, J.R. (2002). The Sybil attack. *Proceedings of First International Workshop Peer-to Peer Systems* (*IPTPS '02*).