IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.-7, Special Issue, 4, Feb 2019 E-ISSN: 2347-2693

Self Organzied Wireless Sensor Network Model for Military Decentralized Applications

T. Manivannan

Dept. of Computer Science, E.G.S. Pillay Arts and Science College, Nagappatinam,Tamilnadu, India.

Corresponding Author: manibcommca@gmail.com

Available online at: www.ijcseonline.org

***Abstract*—** Developments in integrated circuit design technology are expected to make the mass production of sensor devices relatively inexpensive, and hence such large sensor networks are likely to be common.A cluster-based scheme is proposed as a solution for this problem. The proposed scheme extends First Input High Energy (FIHE) clustering algorithm and enables multi-hop transmissions among the clusters by incorporating the selection of cooperative sending and receiving nodes. We propose a sensor network architecture based on the cluster-tree based multi-hop model with optimized cluster head election and the corresponding node design method to meet the tactical requirements. In the earlier system, such types of networks for transmission of information are available but there is no security mechanisms for providing the security for that transmitted information. Because several attackers may enter into the network without any authentication and they can attack the network and they can access the data or service they require. With the proposed WSN architecture, one can easily design the sensor network for military usage in remote large scale environments.

***Keywords*—**Military sensor networks, Architecture, Design, Self-organization, Cluster head election.

I. INTRODUCTION

Networks of wireless sensor devices are being deployed to collectively monitor and disseminate information about a variety of phenomena of interest. A wireless sensor device is a battery-operated device, capable of sensing physical quantities. In addition to sensing, it is capable of wireless communication, data storage, and a limited amount of computation and signal processing. Advances in integrated circuit design are continually shrinking the size, weight and cost of sensor devices, while simultaneously improving their resolution and accuracy.Robust: Sensor nodes may fail, and the failures should not have significant effect on the time synchronization error. If sensor nodes depend on a specific master to synchronize their clocks, a failure or anomaly of the master's clock may create a cascade effect that nodes in the network may become unsynchronized. So, a time synchronization protocol has to handle the unexpected or periodic failures of the sensor nodes. If failures do occur, the errors caused by these failures should not be propagated throughout the network.Energy aware: Since each node is power/energy limited, the use of resources should be evenly spread and controlled. A time synchronization protocol should use the minimum number of messages to synchronize the nodes in the earliest time. In addition, the load for time synchronization should be shared, so some nodes in the network do not fail earlier than others. If some parts of the network fail earlier than others, the partitioned networks may drift apart from each other and become unsynchronized. While some sensor network applications involve a small number of sensors (10-20), most exciting applications require a large number of sensor nodes (100-1000) [1]. The networks are also expected to have a high node density in most cases.Since sensor networks contains an outsized range of nodes, it's clear that we want distributed protocols for gathering knowledge, and arbitrating the access to the wireless channel, and these protocols ought to scale well because the range of nodes within the network will increase. a way to realize this is often to prepare the network into smaller sub-networks referred to as clusters. every cluster may be then managed autonomously. Such a hierarchy ends up in lower routing overheads, and will even be used for in-network aggregation of the measured knowledge. The clusters themselves may contains nodes with completely different hardware capabilities. Within every cluster, the responsibilities of co-ordinating MAC and routing, similarly as knowledge aggregation can be assigned to nodes with special hardware [2].MAC protocols may be divided into 2 main classes [3, 4]: scheduled primarily based protocols and contention-based protocols. Scheduled- based protocols are primarily Time Division Multiple Access (TDMA) protocols. In TDMA protocols a centralized (master) node distributes the transmission schedule among alternative nodes within the network throughout the initialization amount. once the initialization amount, no overhead management packets (RTS or CTS) are needed. TDMA protocols are collision free

and perform best in single-hop networks. They need strict synchronization among nodes so as to coordinate node transmission slots. TDMA primarily based protocols don't seem to be adaptive. Once the transmission schedule is distributed, it can't be changed to accommodate newly added nodes. TDMA protocols don't seem to be scalable. They can not support an outsized range of nodes as a result of latency will increase considerably with the quantity of nodes. Contention-based protocols are primarily Carrier Sense Multiple Access (CSMA) protocols [5]. In CSMA, wireless nodes are able to sense the communication medium and defer their transmission whereas the channel is busy. CSMA protocols will simply accommodate newly added nodes (adaptive), don't need strict synchronization among nodes, and may support an outsized range of sensor nodes (scalable). Multi-hop communication is less complicated to handle in CSMA protocols than in TDMA ones.

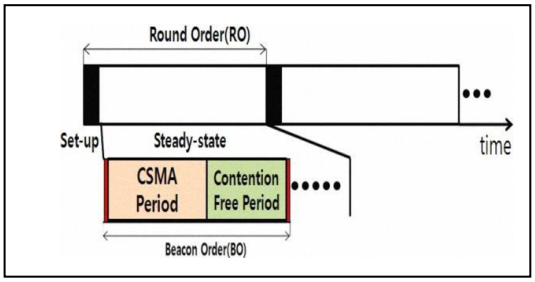


Figure 1. Time-line showing the tactical sensor network operation

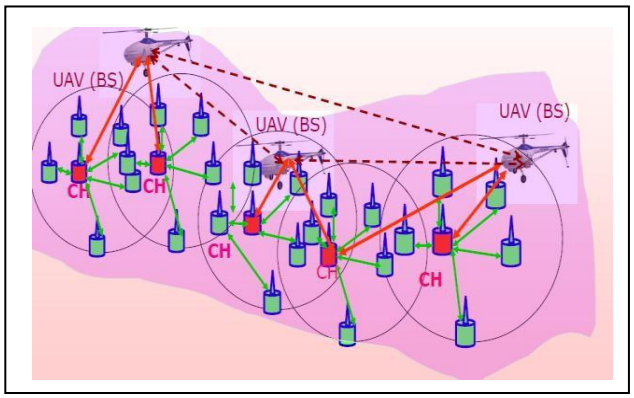


Figure.2. Clustering

In LEACH [6], the network topology contains one sink node and lots of sensor nodes that sample the surroundings at a relentless rate and send their knowledge to the sink. The network includes a hierarchical organization. The network is split into clusters, and every cluster has associated a cluster head node. every node within the cluster sends its sensed knowledge to the cluster head where it belongs. The cluster head aggregates the info packets received into one packet that is transmitted to the sink. For this operation, an ideal correlation among the received knowledge packets is assumed. In reactive (on demand) protocols, a path discovery mechanism is initiated solely when a supply node tries to seek out a route to a destination node that's on the move. thetrailinfo is maintained as long because it is required by the supply. Generally, reactive protocols consume fewer overheads than proactive protocols. When there's no vital movement, there's neither a requirement to periodically send advertisements, nor to receive them. However, the delay caused by looking out a brand new route is inevitable. the placement Aided Routing proposal [7], as an example, proposes the utilization of position info to boost the route discovery part of reactive routing approaches. A supply broadcasts a route request message to all or any its neighbours, sorting out the destination. Neighbours that are inside the request zone can forward them more. Once the destination node, that ought to be inside the zone, receives such a question, it'll send back a route reply message moreover as its current location. Such protocol works because the read-some/write-one theme. Nodes don't ought to update their location to others immediately once the movements. They reply solely when requests are received.An application faces the matter of power management if the active lifetime of the sensor nodes comprising a WSN is a smaller amount than the required lifetime of the network. In such a case, we'd like to seek out ways in which to increase the lifetime of the network.

The principles of ancient network style cannot be directly applied to the look of communication protocols for the WSNs we have a tendency to think about. this can be as a result of ancient communication networks aim to support a various set of users, every with their individual objectives. Hence, there's a requirement to style the network during a modular, interoperable and generic fashion, resulting in layered protocol design. This approach yields a platform which will support any new application on prime of the prevailing network. This multi-service paradigm has been substantially at the core of networking analysis within the Nineteen Eighties and Nineteen Nineties. Such an approach is unsuitable for the WSNs thought-about during this chapter due to the subsequent characteristic options that differentiate them from ancient communication networks:

The large density of nodes, that begs for sensors that are low cost to manufacture and prepared to deploy.
The application diversity, which needs totally different sorts of application specific sensor devices.
The tight limitations in energy, processing power and memory, that decision for highly optimized and light-weight protocols.The collaborative objective that all the sensor nodes cooperate with each other.
In order to account for all of the on top of factors, it's necessary to optimize the communication protocols, to best satisfy the applying level objectives. The other style issues, like protocol layering, are secondary.

II. EXISTING SISTEM

secret data must be transmitted from one place to a different place through an outsized scale wireless network therefore one wants a secure, scalable, and reliable wireless sensor network for military applications, that covers an outsized scale wireless setting. restricted battery power is employed to work the sensor nodes and is extremely tough to exchange or recharge it, when the nodes die. Among others knowledge transmission consumes most of the energy, and it heavily depends on the transmission distance and also the transmitted knowledge quantity.

Scalable Self-Organization

Since thousands of sensor nodes in remote areas cannot be managed by military personnel, they must identify neighbours within communication range and configure the network autonomously. In addition, the network should cope with self- healing and self-reconfiguring. Several papers proposed self- organization self- configuration algorithms for the WSNs [8]- [9]. However, the proposed algorithms are on the assumption that the sensor nodes have a long transmission range which is possible to reach from all nodes to the sink. This assumption is not suitable for the design of scalable networks in large- scale areas since the distance between a sink node and sensor nodes becomes longer. We should design a suitable self organization algorithm considering network scalability.

LEACH: Low-Energy Adaptive Clustering Hierarchy

In standard clustering algorithms, cluster heads are chosen a priori and glued throughout the system lifetime. it's obvious that sensors chosen to be cluster heads would consume a lot of energy, as a result of they need a lot of communication load. Thus, these cluster heads can die quickly and therefore the overall system lifetime is also reduced. LEACH [10] addressed this downside by using randomized rotation of the ―cluster heads‖ and therefore the corresponding clusters, which may distribute the work load evenly among sensors within the network.

The operation of LEACH is shifting into rounds. Every spherical includes 2 phases, a set-up part, throughout that the clusters are fashioned, and a steady state part, throughout that knowledge is transmitted to the bottom stations. Initially, every sensor node decides whether or not to become a cluster head or not primarily based on the instructed proportion of clusterheads within the sensor network, and therefore the variety of times the node has been a cluster head to this point. Every node randomly chooses variety between zero and one. If the quantity is a smaller amount than the edge T (n), the node becomes a cluster head for the present spherical. The edge is computed as

Wh ds given as an input, r is t that the set of nodes

$$T(n) = \begin{cases} \frac{P}{1-P\times(r \bmod \frac{1}{P})} & \text{if } n \in G, \\ 0 & \text{otherwise.} \end{cases}$$

that haven't been cluster heads within the last 1/p rounds. every node that has elected itself a cluster head for the present spherical can broadcast a poster message to the remainder of the nodes. Every non cluster head node decides that node to be its cluster head for this spherical based mostly on the received signal strength of the advertisements. It then informs the cluster head that it'll be a part of the cluster. When the cluster head receives all the messages, it'll broadcast a schedule telling every node within the cluster when to transmit information. Solely throughout information transmission part will nodes send information to the cluster head. When all the information has been received, the cluster head can compress the information into one stream and send it to the bottom station. After a specified amount of your time, ensuing spherical begins with the set-up part and goes on as described on top of. This theme has comparatively low message overhead, and is energy economical as we'll see within the simulation. However, it solely includes a loose management over then share of cluster heads: it guarantees that among each 1/p rounds, each node includes a probability to be a cluster head, however it's no tight management over the amount of cluster heads and therefore the distance from a sensor to its head in every spherical.

Figure 3 shows that because the variety of nodes will increase, the energy dissipation is increased in all 3 schemes. However, the variations among them are important. Max-Min encompasses a sharp increase because the variety of nodes will increase. Forest is that the most energy economical among all 3 schemes. LEACH consumes twice the maximum amount energy as Forest will when the network size is a hundred nodes, and gradually gets near Forest because the network size will increase.

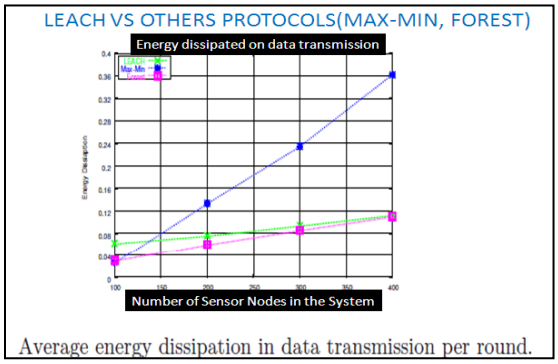


Figure 3:Energy Dissipation

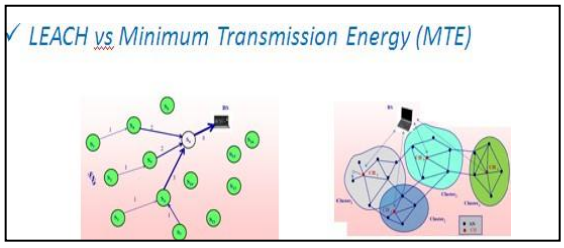


Figure.4: Minimum Transmission Energy

1. Energy Hole Problem in MTE: If nodes use the minimum transmission energy (MTE) routing protocol [11] to forward packets to their closest neighbor, nodes nearer to the sink can handle a lot of traffic than nodes farther off from the sink, and thus can deplete their energy quicker. LEACH eliminates these issues by choosing some nodes that are the cluster heads, to send packets to the sink directly, and let alternative nodes solely send packets to the cluster heads. However, if the cluster heads are mounted, they'll consume a lot of energy than alternative nodes and die quickly as a result of they need to participate in all communications. thus LEACH randomly selects completely different nodes as cluster heads in every spherical to avoid this downside.

2. Improvement for LEACH: In our simulation, so as to reinforce the performance, a doable improvement is additionally implemented here to match with the originality. a vital disadvantage in LEACH is that if clusters cannot be well divided within the clustering part, every cluster size is large totally different, which can end in vital uneven energy consumption among sensors. It may worsen the potency of usage of energy. Therefore, so as to well divide all sensors into clusters, we have a tendency to attempt to divide the realm into many grids. Every grid are often treated as a cluster. Evenly clustering is able to do energy dissipation over all nodes a lot of obvious. The simulation result is shownbelow in Figure.

III. PROPOSED SYSTEM

A design approach for the military WSN in remote large-scale environments based mostly on the military necessities is proposed. Since WSNs in remote large-scale environments cannot be managed manually, when being distributed, sensor nodes got to organize and heal themselves in an energy economical manner whereas guaranteeing the network connectivity. To satisfy the tactical WSN desires, the varied necessities are outlined, and eventually propose the cluster-tree based mostly multi-hop sensor network with the optimized cluster head election. Cluster heads are selected in step with the chance of optimal cluster heads determined by the networks (LEACH). when the choice of cluster heads, the clusters are made and also the cluster heads communicate information with base station. initial Input High Energy (FIHE) algorithm is proven to be an optimal cluster head choice algorithm that maximizes the network lifetime.

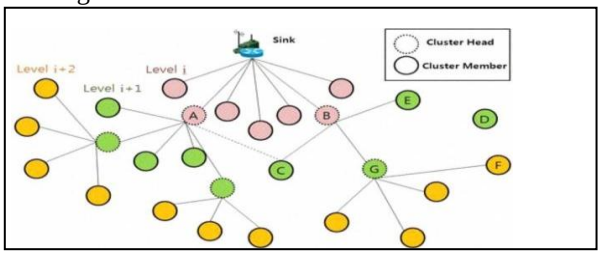


Figure.5. Multi-hop based on clustering

Cluster-Tree Creation

After being distributed, sensor nodes should self-organize cluster tree topology as illustrated in Fig. 3. First, the sink or cluster head sends beacon messages with (i) level to neighbor nodes within its transmission range. After receiving beacons, the node sends association request messages to the sink or cluster head to join the network. After receiving all association request and confirm messages, the cluster head election algorithm is performed by individual member nodes or by cluster head. In Fig. 5, the sensor node A or B which was elected as a cluster head sends a beacon message to neighbour nodes within its transmission range with the increased (i+1) level like the sink's role, and the other nodes act as members of the sink. In case of the node C which received more than two beacons from different cluster heads, the lower level and higher received strength signal indicator could be a criterion to select its cluster head for making a shortest path from a sensor node to the sink and saving energy as well.

A)Modules

Cluster head selection.

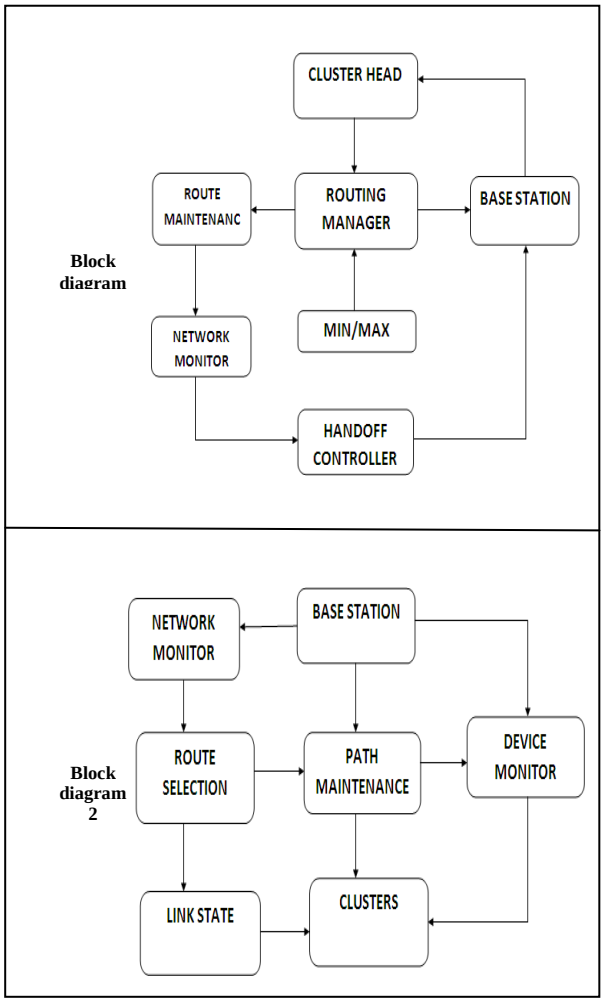


Fig. 6

Cluster Head Selection: The cluster heads may be special nodes with higher energy or normal node depending on the algorithm and application. Here base station is a cluster head performs computational functions such as data aggregation and data compression in order to reduce the number of transmission to the base station (or sink) thereby saving energy. One of the basic advantages of clustering is that the latency is minimized compared to flat base routing and also in flat based routing nodes that are far from the base station lacks the power to reach it. Clustering based algorithms are believed to be the most efficient routing algorithm for the WSNs. The basic principle of its efficiency is that it operates on the rule of divide and conquers. Clustering along with reduction in energy consumption improves bandwidth utilization by reducing collision. Work is currently underway on the energy efficiency in WSNs which will result from the selection of cluster heads.

Energy Consumption: Transmission in WSNs is additional energy consuming compared to sensing, so the cluster heads that performs the operate of transmitting the information to the bottom station consume additional energy compared to the remainder of the nodes. Clustering schemes ought to make sure that energy dissipation across the network to be balanced and also the cluster head ought to be rotated so as to balance the network energy consumption. The communication model that wireless sensor network uses is either single hop or multi hop. Since energy consumption in wireless systems is directly proportional to the sq. of the space, single hop communication is pricey in terms of energy consumption.

Energy Efficient Routing: In distinction to easily establishing correct and economical routes between combine of nodes, one necessary goal of a routing protocol is to stay the network functioning as long as doable. As mentioned within the Introduction, this goal is accomplished by minimizing mobile nodes' energy not solely throughout active communication however conjointly after they are inactive. Transmission power management and cargo distribution are 2 approaches to reduce the active communication energy, and sleep/power-down mode is employed to reduce energy throughout inactivity. Energy consumed/packet,

- time to network partition,
- variance in node power levels,
- cost/packet, and
- Maximum node cost.

RESULTS

Step 1: After starting the network, the wireless sensor nodes will be divided into several clusters in the WSN. (Snapshot1)
Step 2: One node will be chosen as the cluster head in each cluster area. This cluster head will use a negotiation system to send joining messages to the nodes near the cluster head. (Snapshot 2)

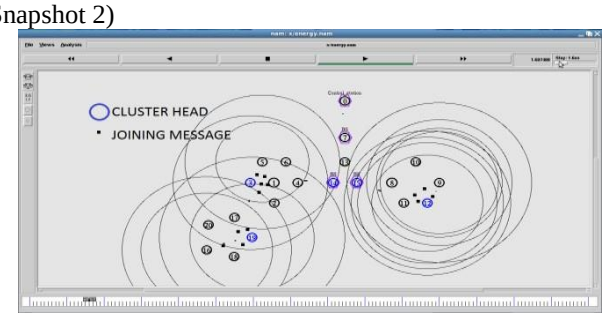


Fig. 7

Step 3: After that, the cluster-heads will send invitations to the wireless sensor nodes in each cluster asking them to join the cluster-heads to form the clusters. The second phase includes the \transferring data process" and the \distributing the role of cluster head process" including the following three steps. The AODV routing protocol is responsible for sending the data from the source to the destination nodes. The role of distribution is determined by regularly selecting a set of new cluster)

The first metric is helpful to produce the min-power path through that the general energy consumption for delivering a packet is minimized. Here, every wireless link is annotated with the link value in terms of transmission energy over the link and also the min-power path is that the one that minimizes the total of the link prices along the trail. However, a routing algorithm using this metric could lead to unbalanced energy spending among mobile nodes.

Step 4: When any wireless sensor node must send a message, it's to see its routing table and appearance for a path to the destination node. Therefore, if the route is on the market within the routing table, it'll forward the message to succeeding node. Otherwise, the message are saved during a queue, and therefore the supply node can send the RREQ packet to its neighbor's to begin the invention method.

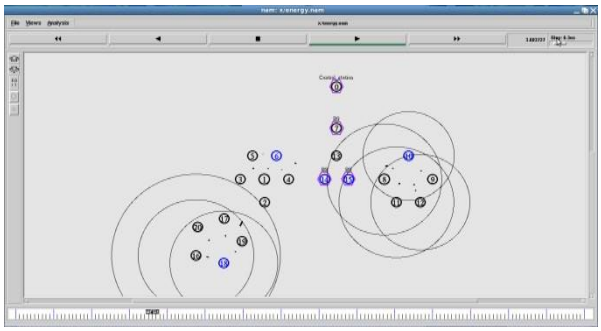


Fig. 8

Step 5: During the forwarding of the message to the destination, the rate at which power is consumed by the

cluster head will be calculated based on the energy model. If the energy consumption speed is high, then the procedure will choose another node to act as the cluster head based on the value.(snapshot - 4)

Step 6: Then, the procedure will remove the route from the routing table of the source, which will lead the source node to initiate the discovery process in phase 2 again and a new path to the destination node through the new cluster head.(snapshot5,6)

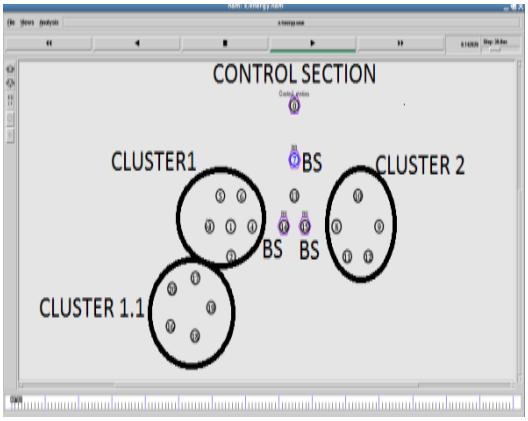


Fig. 9

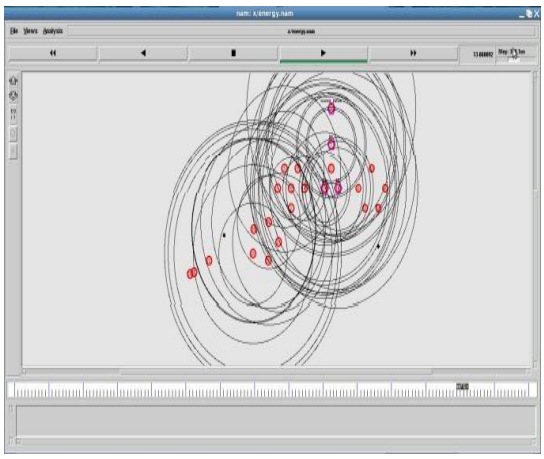
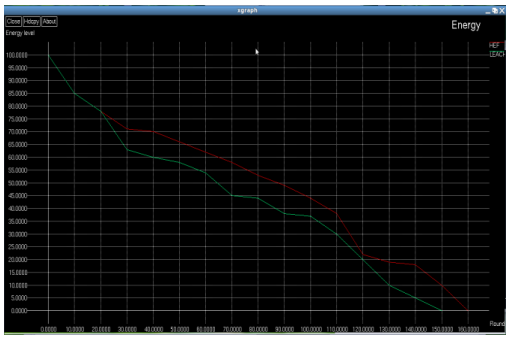


Fig. 10

As the graph shows in the same situation from mentioned proposed algorithm the rounds reached to 1600000 (red) from 1500000(green). However logically it's obvious to understand that if there isn't too much sending and receiving packet or network traffic, the existing system will be more efficient though experiences show it happens rarely.
(snapshot 7)



IV. HYBRID KEYING SENSOR AUTHENTICATION

To allow for more flexibility, existing keying models can be combined by using a different keying model for different communication types. Because of storage limitation it's not possible to use asymmetric keying authentication for sensors in large scale; more over each symmetric key has its own limitation though by hybrid symmetric keys their weaknesses could be improved. Here there are three enemy sensors that they want to authenticate themselves to our network. (snapshot8)

In the specific times base station requests all sensors to authenticate themselves by sending global key.(snapshot 9)
Two enemy sensors are recognized because of wrong global key, but the third enemy sensor catch the global key by monitoring or by other means. In the next level each cluster head (internal base station) request to cluster members to authenticate themselves to related cluster head by sending group key. Here optimistically the third enemy will be recognized, but if not, it can't authenticate itself to other clusters because of different group keys for each cluster. In addition to this, each cluster head and base station can use a pair wise key to authenticate each other against of a-man-in-the-middle attack (reset pair wise key after cluster headchanged).(snapshot 10)

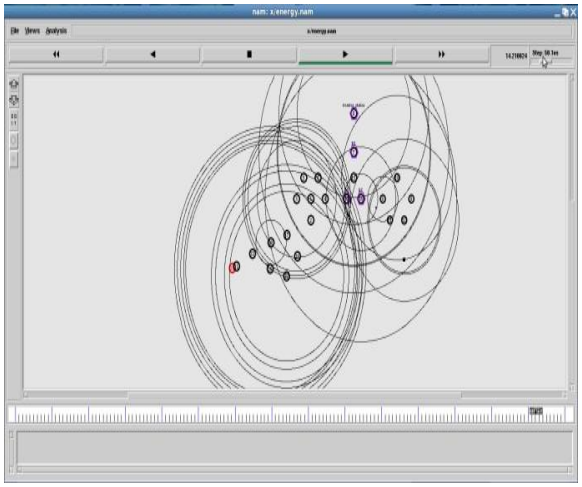


Fig. 11

IV.CONCLUSION

In this paper, we discussed a tactical WSN architecture with sensor nodes in remote large-scale environments. To satisfy the tactical WSN needs, we defined the various requirements, and finally proposed the cluster-tree based multi-hop sensor network with the optimized cluster head election. The prediction and recovery mechanisms for maintenance of the network are also designed. Studies satisfying other tactical requirements (e.g., security, QoS, inter-working with tactical backbone) are being conducted in order to design more useful tactical.

WSN system, providing a trustworthy system behaviour with a guaranteed hard network lifetime is a challenging task to safety-critical and highly-reliable WSN applications. For mission critical WSN applications, it is important to be aware of whether all sensors can meet their mandatory network lifetime requirements. In this paper, we have addressed the issue of the predictability of collective timeliness for WSNs of interests. First, the First Input High Energy (FIHE) algorithm is proven to be an optimal cluster head selection algorithm that maximizes a hard N-of-N lifetime for HC-WSNs under the ICOH condition. Then, we provide theoretical bounds on the feasibility test for the hard network lifetime for the FIHEalgorithm. Our experiment results show that the FIHE algorithm achieves significant performance improvement over LEACH, and FIHE's lifetime can be bounded. We have also developed formulas to derive the A lifetime quickly and easily (including both loose, and sharp bounds). In particular, the feasibility test analysis performed in this paper presented a solution that would guide the system administrator to ensure that the system lifetime is predictable.

REFERENCES

[1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci. Wireless sensor networks: A survey. Computer Networks (Elsevier) Journal, pages 393–422,March 2002.

[2] V. Mhatre, C. Rosenberg, D. Kofman, R. Mazumdar, and N. Shroff. A minimum cost surveillance sensor network with a lifetime constraint. IEEE Transactions on Mobile Computing, 4(1):4–15, January 2005.

[3] W. Ye, J. Heidemann, and D. Estrin, An Energy-efficient MAC Protocol for Wireless Sensor Networks, Proc. IEEE INFOCOM 2002, (Jun. 2002), pp. 15671576.

[4] W. Ye, J. Heidemann and D. Estrin, Medium Access Control with Coordinated Adaptive Sleeping for Wireless Sensor Networks, IEEE, ACM Transactions on, Networking, Vol 12, No 3, (Jun. 2004), pp. 493–506

[5] A. Tanenbaum, Computer Networks, 4th ed., Prentice Hall, 2003.

[6] W. Heinzelman, A. Chandrakasan, and H. Balakrishnan, Energy-Efficient Com- M. Miller and N. Vaidya, Minimizing Energy Consumption in Sensor Networksmunication Protocols for Wireless Microsensor Networks, Proc. of the Hawaii International Conference on Systems Sciences (HICCS 2000), (Jan. 2000).

[7] Y.-B. Ko and N. H. Vaidya, Location-aided routing (LAR) in mobile ad hoc networks, ACM/Baltzer WINET J., vol. 6, no. 4, 2000, pp. 307– 21

[8] A. Manjeshwar and D. P. Agrawal, "TEEN: A Routing Protocol for Enhanced efficiency in Wireless Sensor Networks," in Proc. 15th Int. Parallel and Distributed Processing Symp. (IPDPS 2001), San Francisco, CA, April 2001.

[9] W. R. Heinzelman, A. P. Chandrakasan, and H. Balakrishnan, "An application-specific protocol architecturefor wireless microsensor networks," IEEE Trans. Wireless Commun., Vol. I, No.4, pp. 660-670, Oct. 2002.

[10] W. R. Heinzelman, A. Chandrakasan, and H. Balakrishnan,―Energyefficient communication protocol for wireless microsensor networks,‖ in Proceedings of the 33rd Annual Hawaii International Conference on System Sciences(HICSS), January 2000, pp. 3005–3014. [Online].Available:citeseer.ist.psu.edu/rabinerheinzelman00energyefficient.html

[11] Timothy J. Shepard, A channel access scheme for large dense packet radio networks (SIG COMM 96) pp 219-230.

