# Multi-Chain Oriented Logical Topology for Wireless Sensor Networks

Quazi Ehsanul Kabir Mamun, Sita Ramakrishnan and Bala Srinivashan
*Clayton School of IT, Monash University, VIC 3800, Australia*
*{Quazi.Mamun, Sita.Ramakrishnan, srini}@infotech.monash.edu.au*

**Abstract.** Intrinsic restrictions of sensor nodes and unreliable nature of wireless communication direct the designers to develop power efficient and resource utilizing protocols for wireless sensor networks(WSNs). Different types of energy-efficient protocols have been proposed based on different topologies. In this paper we address the issue of logical topology of WSNs in conserving energy and efficient utilization of constraint resources. We discuss how topology may play vital role in conserving energy, establishing reliable communication as well as decreasing the response time and propose a multi-chain oriented logical topology for wireless sensor networks. Moreover, we develop two different protocols, one for data collection from the target are and another for data dissemination among the sensor nodes, to run on the top of the proposed topology. Analytical and simulation results show that the proposed topology facilitates both protocols to save noticeable amount of energy, reduce latency and also uses minimum resources.

**Keywords:** *Wireless sensor networks, Topology, chain oriented topology.*

## 1. Introduction

Wireless sensor networks (WSNs) consist of a large number of small, low-cost and low-power nodes (called motes) that coordinate with one another for environmental sensing. The sensor nodes are severely restricted in power, memory and computational resources. The nodes can be densely deployed in close proximity to the phenomenon to be observed [1]. They can be deployed in hostile environments where the nodes may not be physically accessible and are subject to tampering. Also nodes can be added to and deleted from the network at any time, resulting in unpredictable changes to the physical topology of the network. This presents new challenges in the design of routing protocols for sensor networks.

Since in WSNs sensors are deployed in unattended or hostile place, it is not possible in most of the cases to arrange them in some physical topology. Thus we have to depend on the logical topology only. In this paper, we discuss about the effect of different logical

topologies on the performance of different protocols for WSNs. We propose a multi-chain oriented topology. We develop a data collection protocol and a key distribution protocol and run the both protocol on the top of the proposed topology to find out the effect of topology in conserving energy, minimizing resource usage and reducing latency.

The rest of the paper is organized as follows: in section 2 we discuss about the influences of topology in WSN with two elaborations. Section 3 discusses about different logical topologies being proposed or used by different types of communication protocol. We propose the multi-chain oriented logical topology in section 4. Two protocols that run on the top of the proposed protocol are briefly described in section 5. In section 6 we discuss about the evaluations of our protocols and we draw the conclusion in section 7.

## 2. Topology Influences on WSN

In this section we describe the influences of logical topology on the constraints of WSN such as energy conservation, low quality communication, resource-constraint computation, scalability etc. We claim that topology plays a vital role for wireless sensor networks. Energy consumption is proportional to the number of packets sent or received. The receiving cost depends on packet size while the transmission energy depends on the distance between the nodes. As topology inherently defines the type of routing path, whether to use broadcast or unicast, size and type of packets and other overheads, choosing a right topology can help us reduce the amount of communication needed for a particular problem. Thus energy can be saved. An efficient topology which ensures neighbors are in minimal distance can reduce the probability of message lost between sensors. A topology can also reduce the radio interference, thus reduce the waiting time for sensors to transmit data. Moreover, topology facilitates data aggregation which greatly reduces the amount of processing cycles, also energy – thus gives long life time. Topology inherently defines the size of a group, how to manage new members in a group or how to deal with left members. With the awareness of the underlying network topology, more efficient routing or broadcasting schemes could be achieved. Furthermore, the network topology in WSNs can be changed by varying the nodes' transmitting range and adjusting the wake/sleep schedule of all nodes. Therefore, more energy can be saved if the network topology can be maintained in an optimal manner. Below we give two elaborations which have motivated us to study the realm of topology.

***Topology and Energy Consumption***

Suppose node $u$ must send a packet to node $v$, which is at distance $d$ (see figure 1). Node $v$ is within $u$'s transmitting range at maximum power, so direct communication between $u$ and $v$ is possible. However, there exists also a node $w$ in the region $C$ circumscribed by the circle of diameter $d$ that intersects both $u$ and $v$. Since $\delta(u,w) = d_1 < d$ and $\delta(v,w) = d_2 < d$, sending the packet using $w$ as a relay is also possible. Which of the two alternatives is more convenient from the energy-consumption point of view? To answer this question,

we must refer to specific wireless channel and energy consumption models. For simplicity, assume the radio signal propagates according to the free space model and that we are interested in minimizing the transmit power only. For these assumptions, the power needed to send the message directly from $u$ to $v$ is proportional to $d^2$; in case the packet is relayed by node $w$, the total power consumption is proportional to $d_1^2 + d_2^2$. Consider the triangle $\Delta uwv$, and let $\gamma$ be the angle opposite to side $uv$. By elementary geometry, we have

$$d^2 = d_1^2 + d_2^2 - 2d_1 d_2 \cos\gamma$$

Since circle $C$ contains the point $w$, $\cos\gamma \leq 0$ and thus we have that $d^2 \geq d_1^2 + d_2^2$. It follows that, from the energy-consumption point of view, it is better to communicate using short, multi-hop paths between the sender and the receiver.

The observation above gives the first argument in favor of topology: instead of using a long, energy-efficient edge, communication can take place along a multi-hop path composed of short edges that connects the two endpoints of the long edge.

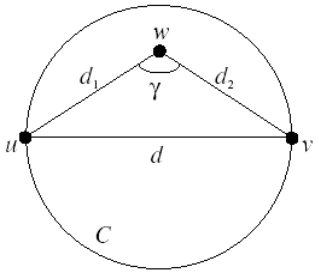


**Fig. 1.** Topology and energy consumption

***Topology and network capacity***

Contrary to the case of wired point-to-point channels, wireless communications use a shared medium, the radio channel. The use of a shared communication medium implies that particular care must be paid to avoid that concurrent wireless transmissions corrupt each other. A typical conflicting scenario is depicted in figure 2: node $u$ is transmitting a packet to node $v$ using certain transmit-power $P$; at the same time, node $w$ is sending a packet to node $z$ using the same power $P$. Since $\delta(v,w) = d_2 < \delta(v,u) = d_1$, the power of the interfering signal received by $v$ is higher than that of the intended transmission from $u$, and the reception of the packet sent by $u$ is corrupted.

Note that the amount of interference between concurrent transmissions is strictly related to the power used to transmit the messages. We clarify this important point with an example. Assume that node $u$ must send a message to node $v$, which is experiencing a certain interference level $\lambda$ from other concurrent radio communications. For simplicity, we treat $\lambda$ as a received power level, and we assume that a packet sent to $v$ can be

correctly received only if the intensity of the received signal is at least $(1 + \eta)^{\lambda}$ , for some positive η. If the current transmit power *P* used by *u* is such that the received power at *v* is below $(1 + \eta)^{\lambda}$ , we can ensure correct message reception by increasing the transmit power to a certain value $P' > P$ such that the received power at *v* is above $(1 + \eta)^{\lambda}$ . This seems to indicate that increasing transmit power is a good choice to avoid packet drops due to interference.

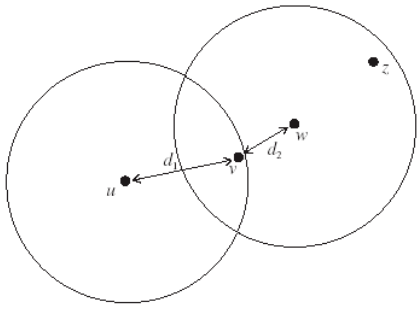


**Fig. 2.** Conflicting wireless transmission

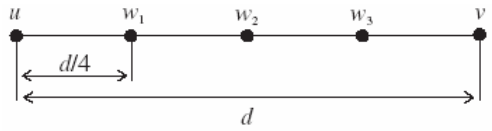


**Fig. 3.** Topology and network capacity

On the other hand, increasing the transmit power at *u* increases the level of interference experienced by the other nodes in *u*'s surrounding. So, there is a trade-off between the 'local view' (*u* sending a packet to *v*) and the 'network view' (reduce the interference level in the whole network): in the former case, a high transmit power is desirable, while in the latter case, the transmit power should be as low as possible. The following question then arises: how should the transmit power is set, if the designer's goal is to maximize the network traffic carrying capacity?

In order to answer this question, we need an appropriate interference model. Maybe the simplest such model is the Protocol Model used in [14] by Gupta *et al.* to derive upper and lower bounds on the capacity of ad hoc networks. In this model, the packet transmitted by a certain node *u* to node *v* is correctly received if $\delta(v,w) \geq (1 + \eta)\delta(u, v)$ for any other node *w* that is transmitting simultaneously, where $\eta > 0$ is a constant that depends on the features of the wireless transceiver. Thus, when a certain node is receiving a packet, all the nodes in its *interference region* must remain silent in order for the packet to be correctly received. The interference region is a circle of radius $(1 + \eta)\delta(u, v)$ (the *interference range*) centered at the receiver. In a sense, the area of the interference region

measures the amount of wireless medium consumed by a certain communication; since concurrent non conflicting communications occur only outside each other interference region, this is also a measure of the overall network capacity.

Suppose node $u$ must transmit a packet to node $v$, which is at distance $d$. Furthermore, assume there are intermediate nodes $w_1, \ldots, w_k$ between $u$ and $v$ and that (see figure 3)

$$\delta(w_1, w_2) = \cdots = \delta(w_k, v) = \frac{d}{k+1} .$$

From the network capacity point of view, is it preferable to send the packet directly from $u$ to $v$ or to use the multi-hop path $w_1, w_2, \ldots, v$? This question can be easily answered by considering the interference range(s) in the two scenarios. In case of direct transmission, the interference range of node $v$ is $(1 + \eta)d$, corresponding to an interference region of area $\pi d^2(1 + \eta)^2$. In case of multi-hop transmission, we have to sum the area of the interference regions of each short, single-hop transmission. The interference region for any such transmission is

$$\pi\left(\frac{d}{k+1}\right)^2 (1+\eta)^2$$

There are $(k + 1)$ regions to consider overall. Hence, by Holder's inequality, we have

$$\sum_{i=1}^{k+1}\left(\frac{d}{k+1}\right)^2 = (k+1)\left(\frac{d}{k+1}\right)^2 < \left(\sum_{i=1}^{k+1}\frac{d}{k+1}\right)^2 = d^2$$

Thus we can conclude that, from the network capacity point of view, it is better to communicate using short, multi-hop paths between the sender and the destination.

The observation above is the other motivating reason for a careful design of the network topology: instead of using long edges in the communication graph, we can use a multi-hop path composed of shorter edges that connects the endpoints of the long edge. Thus, the max-power communication graph, that is, the graph obtained when the nodes transmit at maximum power, can be properly pruned in order to maintain only 'capacity-efficient' edges.

## 3. Logical Topologies in WSNs

In this section we discuss about how topology influences different constraints of wireless sensor network. Here we briefly describe different characteristics only, analytical and simulation results are given in section 6. Figure 4 depicts different types of logical topologies found in wireless sensor networks.

Common topologies found in wireless sensor networks are flat/unstructured topology, cluster oriented topology and chain oriented topology.

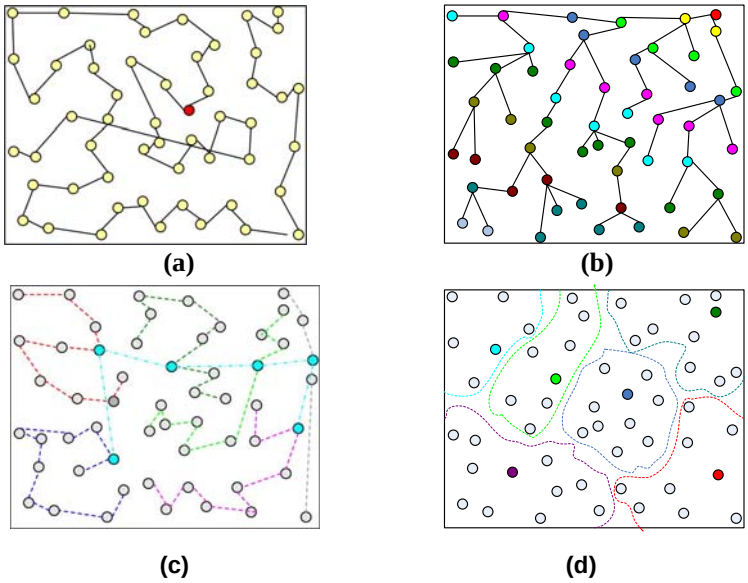


**Fig. 4.** Different types of topologies for WSNs. (a) Single chain topology; (b) Tree based topology; (c) Multi-chain topology; (d) Cluster based topology

The first topology is the flat or unstructured topology. In this topology each sensor node plays equal role in network formation. Routing protocols based on flat topology attempt to find good-quality routes from source nodes to sink nodes by some form of *flooding*. Since flooding is a very costly operation in resource starved networks, smart routing algorithms restrict the flooding to localized regions. Some algorithms use probabilistic techniques based on certain heuristics to establish routing paths. However, flooding is an expensive operation that is normally avoided by sensor network routing protocols. Moreover, a large number of redundant messages are present in the protocols of this topology. Also sensors are not aware of new members or died members. Thus connectedness cannot be guaranteed. On the other hand, most of the flat routing protocols that have been proposed for sensor networks incorporate distance vector routing algorithms. In distance vector routing [6], nodes maintain estimates of their distances from the destination nodes. Each node transmits its distance estimates to its neighbors. Each node updates its distance vector so as to minimize the distance to each destination by examining the cost to that destination reported by each of its neighbors and then adding its distance to that neighbor. The problem with the straightforward distance vector algorithm is that it takes a long time to converge.

The second topology we discuss about is the cluster based topology. In this topology clusters are formed with the sensors deployed and cluster heads are selected. Non uniform clustering is the main problem of cluster based WSNs. Consider the LEACH [20]

protocol, where each of the deployed sensor will choose a random between 0 and 1 and if the random number is greater than some threshold value, they will broadcast themselves as cluster heads and broadcast advertisement. Receiving advertisements rest of the sensors will join at the cluster under a particular cluster head. This protocol cannot guarantee even clustering. Due to non uniform clustering following problems occur - energy dissipation rate is highly different from one sensor to another sensor, even after they are in the same cluster., total energy dissipation is higher, network lifetime decreases as well as connectivity problem

In tree based topology a logical tree is formed. Sensor data are passed from the child node to its parent node. An example protocol that use tree based protocol is TBDCS. This topology is not resilient to node failures. If a parent node fails, then its entire sub-tree is cut off from the base station during the current epoch. In the tree based topology uneven power consumption across network nodes is another substantial problem. The nodes nearer to the base station consume a lot of power in forwarding packets from all the nodes in their sub-tree, whereas the leaf nodes in the spanning tree do not have to perform any forwarding at all and consume the least power. Also long delay occurs for sending sensor data from leaf node to the root node or sink.

In PEGASIS [21], we find single chain topology (figure 4a) where a single logical chain is formed along with all the sensors deployed. A node is elected as the leader of the chain. PEGASIS tries to distributed energy consumption evenly by reselecting new leader in each round. It has been found that utilizing the single chain, PEGASIS is able to save up to 50% more energy compared with LEACH protocol. As broadcast is not used in this topology, it also reduces the redundancy in communication. Moreover, unlike cluster-based topologies, chain leader in this topology is not chocked with communication messages from other sensors of the network. The main problem of this single chain topology is the very long delay for sensor data propagation. Other problems of this single chain topology are scalability, node failure resilience as a single node failure divides the chain into two parts. Although node failure detection protocol can be run, it takes long time for the recovery.

After finding all logical topologies, we find the chain oriented topology more promising than any other topologies. We try to alleviate the major problems of single chain topology at the same time retaining the advantages of that. Our proposed topology, a multi-chain oriented logical topology is discussed in the following section.

## 4. A Multi-Chain Oriented Logical Topology

We propose a multi-chain topology where multiple chains are formed using the deployed sensors. We propose all the chain length to be of same size. A chain length denotes the number of sensor present in a chain. A sensor is selected as local leader of the

chain. In turns all the local-leader form a higher level chain where one of the local-leaders is chosen as higher level leader.

For chain formation to take place, sensor node at the furthest position from base station (BS) takes initiative to start the process. We also assumed that sensor nodes have dynamic power adjustment capability so that while transmitting, they can modify the amplifier power in such a way that it can be heard only by the closest neighbor in the chain. This ensures the avoidance of collision in large extent. Chain formation starts from the furthest node in the network that gives itself the initial chain and member id. Then it finds out the next alive node that is not included in any other chain. The next node's chain id is same as previous but member id is incremented by one. In this way chain formation continues until the member id reaches some maximum number. In our present experiment we took this maximum number to be 20. This choice of maximum number of nodes in a chain depends on several factors such as energy consumption, tolerable delay etc. those we discuss more elaborately in last part of this section. Whenever member id in a chain reaches its maximum number, the next node increments its chain id by one and assigns itself the initial member id for that chain. This way chain formation continues until all the live sensors in the network are included in several chains. These are the chains which we refer as lower-level chains. These lower-level chains remain fixed for long duration of time and chain formation takes place again whenever 20% of member nodes of the previous chain formation die. This is to maintain optimal length of a chain and thus efficiently balance the energy dissipation.

After fixing the chains, next target is to locate the lower-level chain leader at each chain. Instead of leaders being chosen randomly in every round, we propose to select leaders for every chain based on the remaining energy in each sensor of the chain. In addition, we suggest not changing these lower-level chain leaders at every round but after an optimal number of rounds. We tried to find out this optimal number of rounds R, after that these local leaders are reselected based on criteria like energy expenditure and time required completing hundred rounds of data transfer cycle etc.

The benefits of using a slight larger duration for selecting leaders rather than selecting leaders at every round are i) less communication overhead ii) reduced required time for leader selection at every round and iii) maximum utilization of higher level chain. Once these lower-level leaders are selected, a higher-level chain is formed again including all the lower-level leaders using the same greedy way as used in the formation of lower-level chain. After that a higher-level leader is selected based on some criteria among those lower-level leaders that gathers all the information from other leaders and sends this information to the BS for further processing.

For the higher-level leader selection the criteria our protocol considers are i) distance from BS ii) remaining energy of the node. This ensures that nodes closer to BS take turn to transmit frequently than the nodes those are far from the BS. As nodes at far from BS station require more energy to the nodes those are nearer to the BS. We tried to evenly distribute the load of long distance transmission and our protocol can use the energy of the network optimally.

It is important to reconstruct the chains whenever a notable number of sensors die in the network. Otherwise, there may be possibilities that one chain contains higher number of sensors while other contains lower number of sensors.

The lower-level leaders should be changed after some period of time to distribute the energy load. Next we have to decide the optimal number of rounds R, after that the lower-level leaders need to be changed. If the lower-level leaders are changed at every round it causes extra energy expenditure for negotiations as well as causes delay. Also the higher-level chain would be utilized fully if we change these leaders after some number of rounds. On the contrary, if we do not change these leaders for long time they will quickly drain out energy because of excessive long transmissions. Therefore we consider to change the lower-level leaders based on the criteria like total energy dissipation in the network, maximum number of round when first node dies and delay introduced in the network against the different values of number of rounds.

## 5. Applied Protocols on Proposed Topology

We apply two different protocols on the proposed topology – one for collecting data from the sensor network and sending the information to outside world and the other one for inserting information from outside into the sensor network – key distribution in sensor networks. Both protocols come across with worthy results. The first protocol is a data collection protocol on multi-chain oriented sensor networks named as COSEN. The second one is the key distribution protocol for secured sensor network named SecCOSEN.

### 5.1 Data Collection Protocol (COSEN)

The detailed description of this protocol is available in [3]. In this protocol the similar data transmission mechanism takes place both in the lower-level as well as in higher-level chains. Each chain leader is responsible for collecting data from its associated chain. Lower-level leaders collect information from lower-level chains. All lower-level leaders then transfer data to the higher-level leader and finally higher-level leader transmits this information to the remote BS to complete a round. At the beginning of a round, each leader in a lower-level chain sends a token towards the one end indicating the beginning of data transmission phase. The node at one end of a chain sends its data toward the leader node through intermediate nodes as shown in Figure 5. In this Figure leader n3 sends token toward node n1 through intermediate node n2. After getting this initiation message node n1 sends its data to node n2 which then fuses its own data with n1's data and send the final data packet to the leader node n3. After receiving message from one end, n3 sends token similarly toward node n5 and collect n5 and n4's data in the same way as described before. As the size of the token is small so cost associated to it is

negligible. It is noticeable that data get fused at the time of traveling toward the leader node therefore leader only receives the aggregated information from its chain. As stated in [11, 18, 19], this kind of data fusion can save a lot of energy which yields longer network lifetime. Therefore all the lower-level leaders collect data from their own chains using similar token and data passing approach in parallel. This parallel method of data collection results in reducing the delay in completing each round as compared to PEGASIS which utilizes a single chain.

Now these lower-level leaders on the other hand form a higher-level chain and among this higher-level chain only one node acts as higher-level leader. The higher-level leader now takes initiative to collect information from other lower-level leaders in a similar manner as used in lower-level chain. When this higher-level leader accumulates all leaders' data, it sends this data to the remote BS. It is worth mentioning that data undergoes further compression while travel along the higher-level chain toward the higher-level leader.

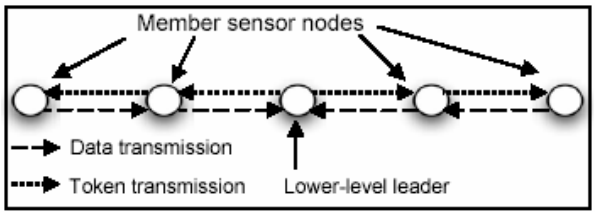


**Fig. 5.** Data and token passing in a chain

### 5.2 Secure key distribution protocol (SecCOSEN)

The second protocol we run on the proposed multi-chain logical topology is a key distribution protocol (SecCOSEN) which is based on partial keys pre-distribution and symmetric cryptography. A detailed description of this protocol is available in [2]. On account of resource-constraint nature of sensor network, both pre-distribution of keys and symmetric cryptography are appropriate with WSN. Furthermore, we do not assign keys randomly from a key-pool as in [14]. Consequently number of keys generated is much lower when compared with [14]. Nonetheless, the key management system remains secure because large number of keys can be generated by the sensors participating in a chain and each pair of sensor nodes uses different communication key.

Another important feature of the scheme is that two communicating nodes always use a new secret key for data encryption/decryption in each round. This feature enables WSN to achieve resilience to attacks as well as data freshness without generating a long nonce.

We propose each of the sensors keeps a set of partial key rather than the set of full keys. This has a two-fold advantages – i) lower storage requirement and ii) even if a sensor is captured by an attacker, it cannot obtain the encryption/decryption keys. Due to

the proposed logical topology, a sensor communicate with its successor and predecessor only, two neighboring sensors establish their encryption / decryption key concatenating their partial keys.

It is pointed out in [11] that public key cryptography is not well-suited for securing WSNs. Indeed, the memory of a sensor is typically insufficient to hold the long keys necessary to guarantee secure asymmetric cryptography. Moreover, sensors are usually equipped with a low power processor which requires too much energy and too long to compute the modular exponentiations involved in the implementation of public key cryptography. Therefore we used symmetric cryptography.

## 6. Experimental Results and Performance Evaluation

In this section we describe the experimental results for the two applied protocols on the proposed logical topology. Our main purpose is to analyze energy efficiency, lifetime pattern of network and latency for the proposed logical topology with other existing logical topologies.

In practice it is difficult to model energy expenditure in radio wave propagation. Therefore in order to measure the energy expenditure in the network, we choose to use the same simplified radio model used in [20, 21] which use the first order radio model and it is assumed that the sources of energy dissipation are the transmitter which dissipates energy to run radio electronics and power amplifier, and the receiver which dissipates energy to run the radio electronics. [20, 21] also approximate that the transmitter amplifier requires $E_{amp}$=100 pJ/bit/m$^2$ to amplify the signal at an acceptable signal to nose ratio (SNR). In addition energy required in running transmitter and receiver electronics are equal and given by $E_{tx\text{-}elec}$=$E_{rx\text{-}elec}$=$E_{elec}$=50nJ/bit. Moreover, the energy cost for data aggregation is considered as 5nJ/bit/message [22]. The bandwidth of the channel was set to 1 Mb/s [22]. In our experiments each data message is 2000 bits long and information processing time in a node is taken between 5 to 10 milliseconds [22]. The medium is assumed to be symmetric such that the energy required for transmitting a message from node A to B and from B to A are same at a fixed SNR. So we can say, for free space propagation loss, energy dissipation is certainly dominated by the long distance transmissions. Thus the total transmission cost for a k-bit message is given by the equation (1). In case of receiving message, the energy consumption equation is given by equation (2).

$$E_{tx}(k,d) = E_{elec} \times k + E_{amp} \times k \times d^2 \quad (1)$$

$$E_{rx}(k) = E_{elec} \times k \quad (2)$$

where $d$ is the distance between sender and receiver measured in meters.

For experimental purposes we chose different prominent protocols designed on various topologies. For example, we chose LEACH as a representative for cluster based

topology, PEGASIS for single chain oriented topology, SPIN for flat topology and compare them with COSEN, a protocol based on multi-chain oriented topology.

Regarding our first protocol, the data collection protocol COSEN, Figure 6 demonstrates the comparative energy consumptions by SPIN, LEACH, PEGASIS and COSEN. It is obvious from the figure that energy requirements for PEGASIS and COSEN are far better than that of SPIN and LEACH. COSEN and PEGASIS have almost same amount of energy consumption. For example, in case of total aggregated energy consumption for all sensors in the network, after 100 rounds COSEN requires only 0.218 joules of energy additional than that of PEGASIS, after 500 rounds COSEN requires only 2.833 joules of energy additional than that of PEGASIS etc. But the significant point for COSEN is that, it spends the energy in a totally distributed way such that the network can operate higher number of rounds before the first sensor dies. The lifetime pattern of COSEN is depicted in Figure 7. Here we see that the first node dies for PEGASIS at 350 rounds, but the first node dies at around 475 rounds for COSEN. In case of LEACH and SPIN we find the first node dies at only 300 and 195 rounds respectively. This explicitly proves that chain oriented logical topologies are better than other topologies in respect of energy consumption. The problem with single chain oriented topology (PEGASIS) is the latency- it takes so long time to disseminate information to all nodes or to complete a data collection round. To find out the latency factor we choose data dissemination time required by each protocol using different logical topologies. That is, we calculate the time required by each protocol to disseminate data from a single source to all nodes of the network. Figure 8(a) shows that time required for SPIN, LEACH and COSEN are almost same whereas figure 8(b) shows the definitive improvement of COSEN over PEGASIS in respect of latency; figure 8(b) shows that where, for a network with 500 nodes, PEGASIS requires around 6500 milliseconds, COSEN requires less than 650 milliseconds.

Regarding the second protocol, the secure key distribution protocol SecCOSEN [2], here we discuss about the influences of the logical topology rather than how strong or secured the protocol is. The logical multi-chain oriented topology gives benefits in many folds. For example, because of the topology the convergence time is low, that is a node is able to set up the security keys very quickly. Also a large number of key can be generated using comparative low number of partial keys – this also helps sensor nodes to store low number of partial keys that means it lowers the memory requirements. Figure 9 shows number of session key candidates that can be generated using partial keys. For example, using only 100 partial keys (which requires only 325 bytes), more than 20000 candidate keys can be generated [2]. If we apply the same protocol in a cluster based topology, sensor nodes require more partial keys to store to create same number of session key candidates. We can describe it from other viewpoint as well. In a cluster based topology a node (specially the local coordinator) needs to communicate with all other members of the cluster. Now if there are $n$ number of nodes in a cluster, and the local coordinator is compromised, all the secret keys of that cluster will be revealed. On the other hand, in our topology if a node (even though it is a leader of a chain) is compromised, secret keys of at best three nodes (the compromised node itself, its successor and predecessor) can be

revealed. The contribution of the logical topology here due to the fact that the sensors create multiple chains and restrict the communication inside the chain only. A chain member communicates to its successor or predecessor member of that chain only. Thus finding out a secret key even knowing the partial key lists is nearly impossible.

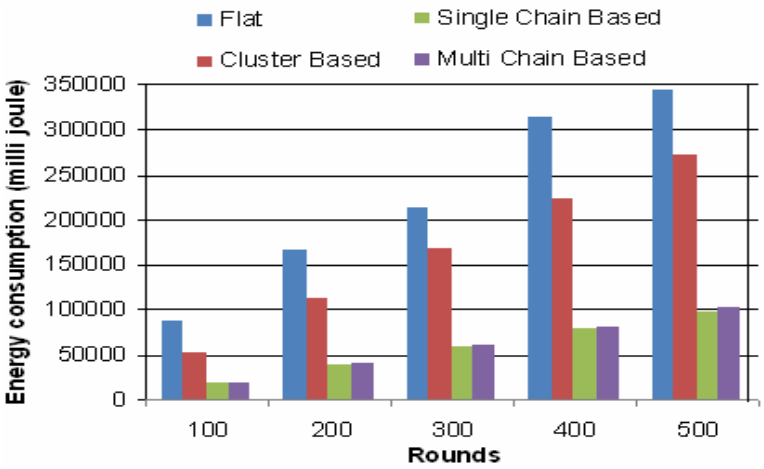


**Fig. 6.** Energy consumption

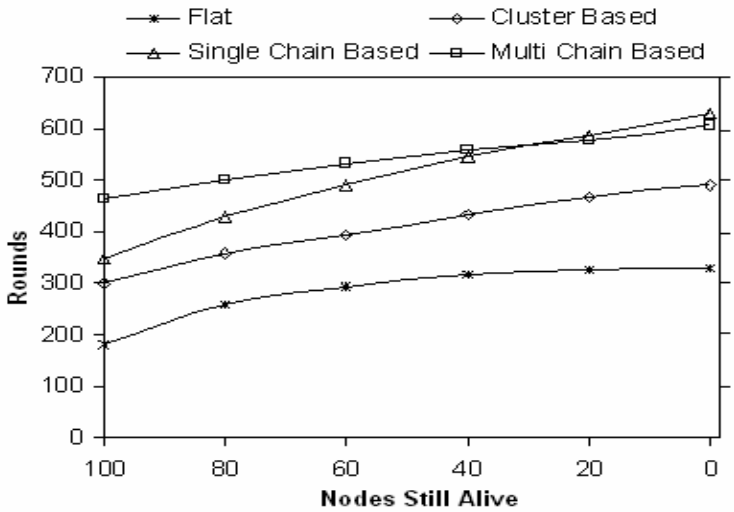


**Fig. 7.** WSN lifetime pattern (protocol 1)

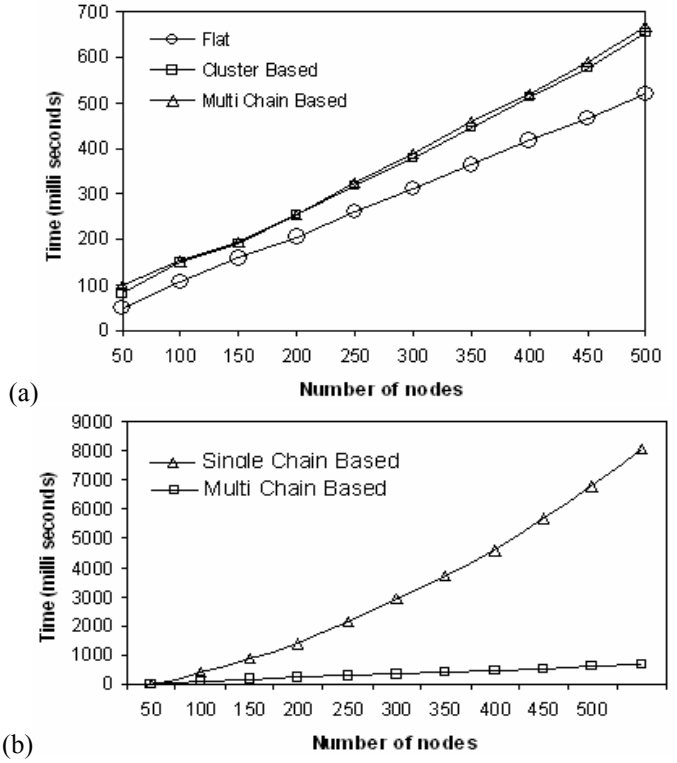


**Fig. 8.** Network latency. (a) COSEN vs (SPIN and LEACH) (b) COSEN vs PEGASIS

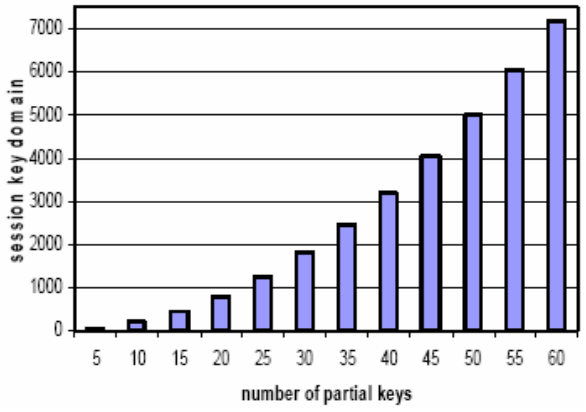


**Fig. 9.** Number of session key candidates in SecCOSEN

## 7. Conclusion

Wireless sensor networks are often densely deployed in hostile/unattended places. Moreover, nodes are easy to fail due to energy constraints. All these uncertainty preclude manual configuration and design-time pre-configuration. As a result physical topologies are not so popular in WSNs. All we have to rely on the logical topology constructed by the active sensors in a sensor network. In this paper we firstly discussed how logical topology affects the communication and resource usages and then we propose a multi-chain oriented logical topology. To test the logical topology, we run two different types of protocols on top of the topology. The first protocol, a data collection protocol, saves excellent amount of energy as well as latency. The second protocol, a data (secret key) dissemination protocol for establishing security, also performs well as it requires minimum space and gives a very large domain of secret keys. Moreover, due to the chain topology, the communication required for the protocol is minimal. These initial set of protocols and experiments serve to demonstrate the marked difference for energy conservation, latency and constraint resource usage. These differences are significant enough to warrant further research.

Our aim is to construct a logical topology, a base upon which different application protocols would be created in an efficient way. So far we know there is no significant amount of work that has been done in the area of topology of sensor networks. Different protocols like data collection protocol, dissemination protocols, routing protocols – did not assume an established logical topology, they created the topology by the way the protocols work. But we see from different angle. We would like to establish a logical topology first, on the top of that we think to derive different protocols. The creation of a successful logical topology for WSNs would allow far great reuse of existing components. The resulting reduction in development delays and costs would greatly broaden the sphere of potential applications. Thus, logical topology would break sensor networks out of the confines of the few very high payoff/budget applications like national security, and would enable their use in less lucrative but extremely valuable areas such as scientific research and ecosystem management. In so doing, the fruits of this proposal would have a significant beneficial impact on society.

## References


1. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci: A survey on sensor networks, IEEE Communication Magazine, vol. 40, issue 8, pp. 102-14, (August 2002)
2. Quazi Ehsanul Kabir Mamun and Siata Ramakrishnan: SecCOSEN – A Key Management Scheme for Securing Chain Oriented Sensor Networks, in proceedings of the 6th international conference on Communication Networks and Services Research (CNSR 2008)
3. Nahdia Tabassum, Quazi Ehsanul Kabir Mamun, A K M Ahsanul Haque, Yoshiyori Urano: A Chain Oriented Data Collection Protocol for Energy-Aware and Delay Constrained WSN.

African Journal of Information and Communication Technology. Vol 2 No. 3, Sept ’06, 126 -- 136 (2006)
4. L. Eschenauer and V. Gligor: A Key Management Scheme for Distributed Sensor Networks. In: 9th ACM Conf. Computer and Communication Security. pp. 41—47 (2002)
5. H. Chan, A. Perrig, and D. Song: Random Key Predistribution Schemes for Sensor Networks. In: IEEE Sec. and Privacy Symposium. pp. 197--213 (2003)
6. W. Du et al.: A Key Management Scheme for Wireless Sensor Networks Using Deployment Knowledge. In: IEEE INFOCOM ’04. (2004)
7. D. Liu and P. Ning: Improving Key Pre-Distribution with Deployment Knowledge in Static Sensor Networks. ACM Trans. Sensor Networks, 204 –39 (2005)
8. M. Eltoweissy et al.: Group Key Management Scheme for Large-Scale Wireless Sensor Network. J. Ad Hoc Networks, Sept. ‘05, 796--802 (2005)
9. M. Younis, K. Ghumman, and M. Eltoweissy: Location-aware Combinatorial Key Management Scheme for Clustered Sensor Networks. IEEE Trans. Parallel and Distributed Sys., (2006) Press, (2001)
10. J. Hill, R. Szewczyk, A. Woo, S. Hollar, D. Culler, K. Pister: System Architecture Directions for Networked Sensors. In: ACM ASPLOS IX Conf. pp. 93--104, (2000)
11. Adrian Perrig, Robert Szewczyk, Victor Wen, David Culler, and J. D. Tygar. Spins: Security Protocols for Sensor Networks. In: Seventh annual international conference on Mobile computing and networking, pp. 189--199. ACM Press, (2001)
12. J. Hill, R. Szewczyk, A. Woo, S. Hollar, D. Culler, K. Pister: System Architecture Directions for Networked Sensors. In: ACM ASPLOS IX Conf. pp. 93--104, (2000)
13. Kui Ren, Kai Zeng, Wnjing Lou: On efficient key- redistribution in large scale wireless sensor networks. (2005)
14. Yanchao Zhang, Wei Lue, Wenjing Lou, and Yuguang Fang: Securing sensor networks with location-based keys. In: IEEE WCNC Conference. (2005)
15. W. Du. J. Den, Y. S. Han and P. K. Varshney: A pairwise key pre-distribution scheme for wireless sensor networks. In: 10th ACM Conference on Computer and Communications Security (CCS). Washington DC. USA. pp. 42--51, (2003)
16. D. Liu and P. Ning: Establishing pair-wise keys in distributed sensor networks. In: 10th ACM Conference on Computer and Communications Security (CCS). Washington DC. USA. pp. 52--61, (2003)
17. M. Eltoweissy, M Moharrum and R. Mukkamala: Dynamic key management in sensor network. IEEE Communications magazine, April ’06, 122--130 (2006)
18. Crossbow Technology – Revolutionary Wireless Sensors and Inertial Systems, (2007). http://www.xbow.com
19. D. Liu, P. Ning, and W. Du: Group-Based Key Pre- Distribution in Wireless Sensor Networks. In: ACM Workshop on Wireless Security (WiSe 2005). pp. 11-- 20, (2005)
20. W. R. Heinzelman, A. Chandrakasan, and H. Balakrishanan, “An Application-Specific Protocol Architecture for Wireless Micro sensor Networks,” IEEE Trans. Wireless Commun., vol. 1, no. 4, pp. 660-670, (Oct 2002)
21. S. Lindsay and C. Raghavendra, PEGASIS: Power-Efficient Gathering in Sensor Information Systems,” in international Conf. on Communications, (2001)
22. J. Kulik, W. R. Heinzelman, and H. Balakrishnan: Negotiation-based protocols for disseminating information in wireless sensor networks, Wireless Networks, vol. 8, pp. 169-185, (2002)