

*Sensor Network Operat*

and iii) SDDA employs a sleep protocol to coordinate the activation of sensing units of sensor nodes in such a wa

circuits [20] accelerate the feasibility of the inexpensive sensor networks applications from military networks (surveillance, intelligence) to environmental monitoring networks (climate, agriculture, etc.).

fromm



selecting certain pixels from the actual image data. Cluste

Section 3 discusses the performance eva

has great potential to reduce the amount of data to be transmitted from sensor nodes to cluster-heads. The basic motivation behind differential data aggregation is that significant changes in sensor readings can occur only when a *critical* event (e.g., a fire event for sensor network monitoring temperature) happens in the env

## ***2.1 Differential Data Aggregation***



environment in which the network is deploy



13. **endif**

14. Find the respective critical value for each current data sensed using

*interval* and *ht* #4580446807440752036361071(810)7610707 8.336231070 3pt28R13612

30]) from 5 to 8 while keeping the second interval ([31-50])'s critical value as 3, same with the previous case.

- The data interval that contains the sensed temperature is found from the *interval* table.

Then, from the interval value, cor 3.96 0 Td (e)Tj 5.28 0 Td ( )Tj Td (f)Tj 3.96 0 or











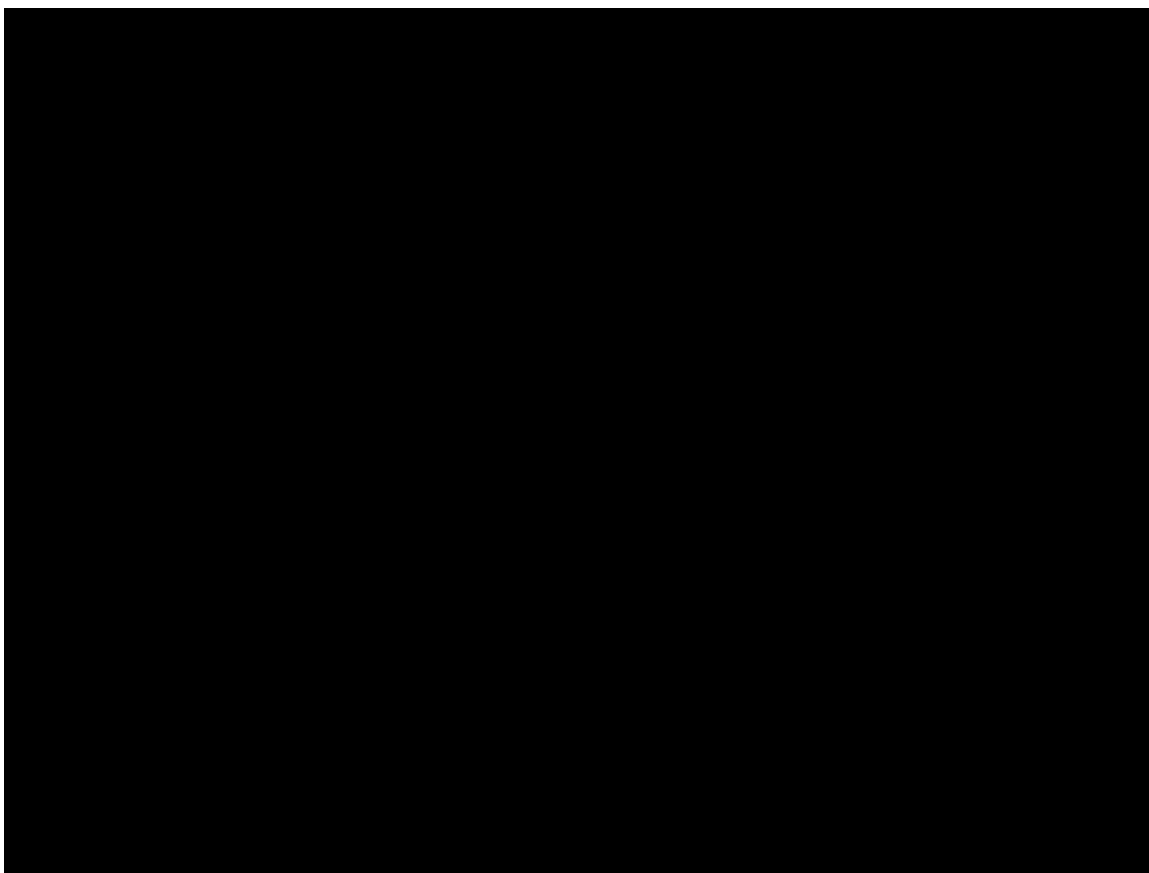


communic]dc



common neighboring area of four or less deployment grids. The global connectivity of the sensor network is ensured, if all of the deploym

be from neighboring deployment grids, since global key rings are selected from key pools assigned to neighboring grids.



**Figure 2** Lo2



The proposed security algorithm concentrates on three main aspects of security namely,



*Step 5: Sen*

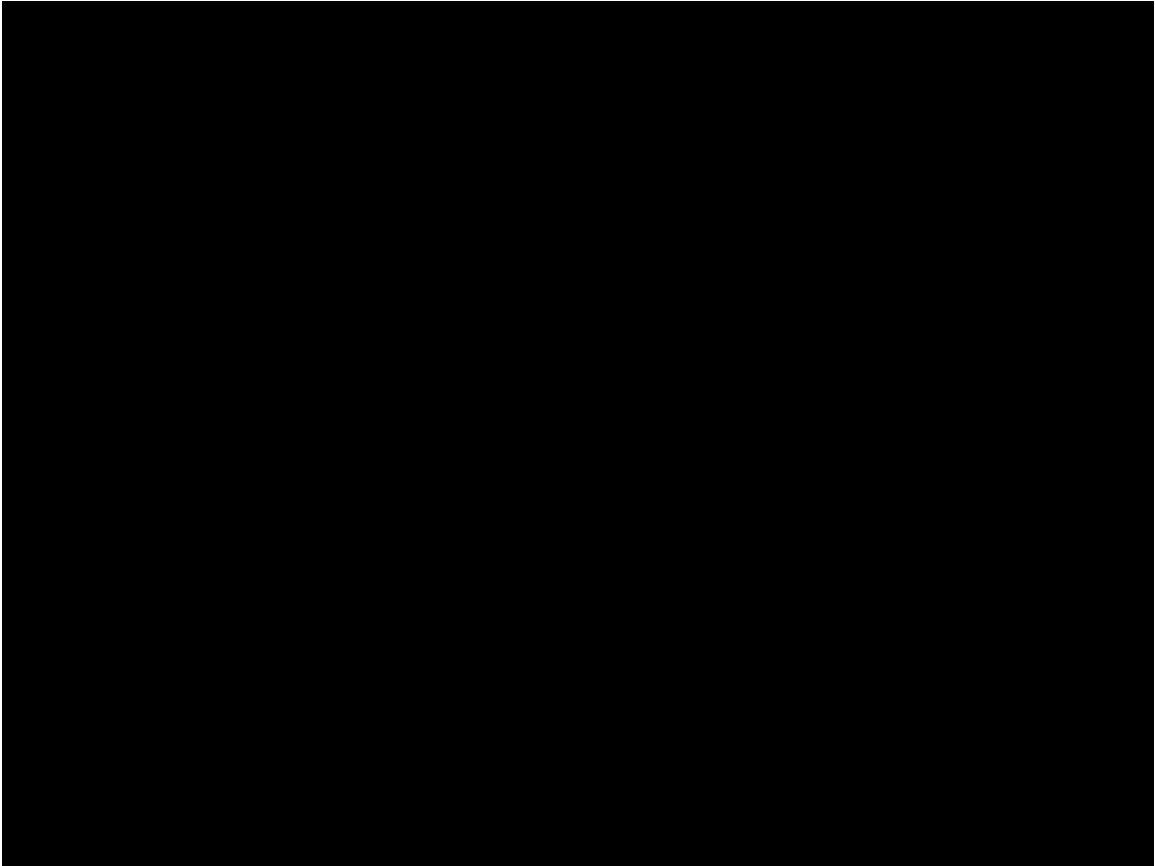
wireless sensor nodes and using peer-to-peer (a) Tj 4.68 0 .96 0 Td (-)Tj 3.96 0 Td (t)Tj 3.3

The sleep protocol is a distributed protocol in which sensor nodes cooperate w.360 Top (s)Tj 408 0 T



exchanges its buffer with active neigs





**Figure 7:** Blind spot effee

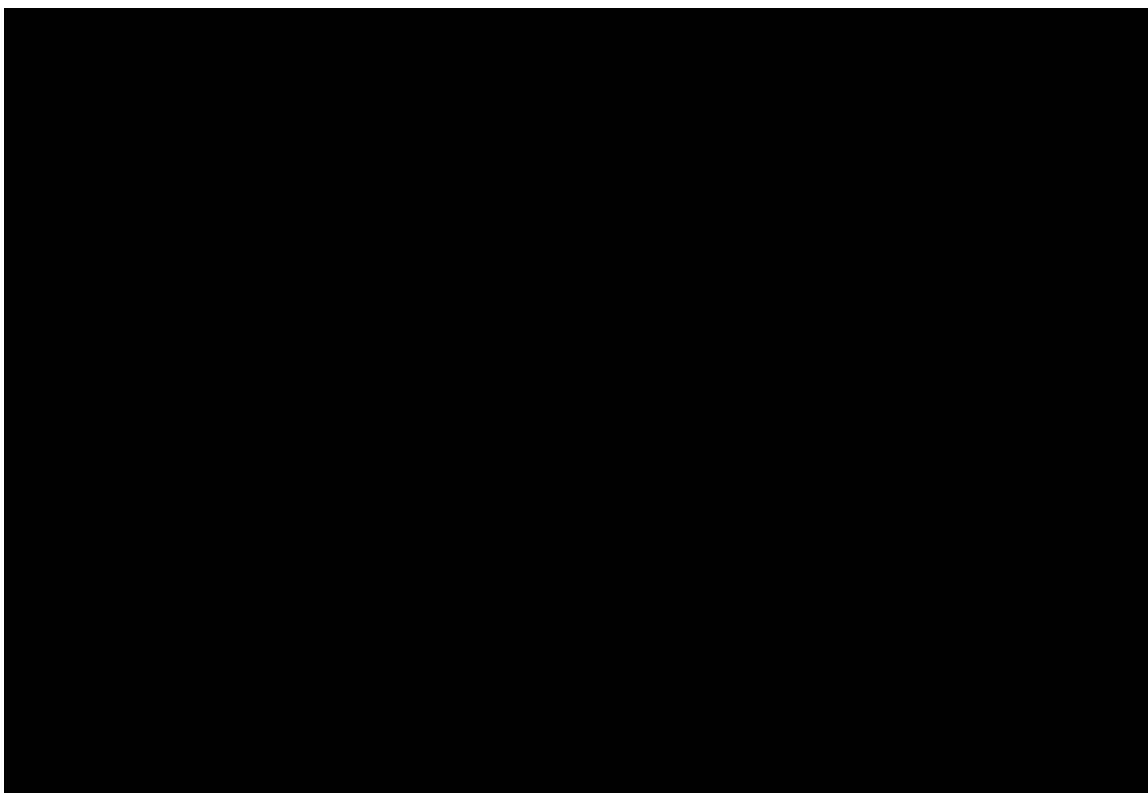
efficient than the conventiii



To assess the energy efficiency of SDDA, we wrote a simulator in C and used GloMoSim [9]. Our simulator is used in differential pattern generation and differential pattern comparison aspects of SDDA. GloMoSim is used to simulate the transmission of data and differential pattern codes from sensor nodes to cluster







**Figure 9:** Comparison of encryption algorithms using Strong-Arm SA-1100 profiling [19].

### 3.4.2 Cryptographic strength of the Security Protocol

In this subsection we will e

allow the attacker to complete a brute force attack on the mep

encryption keys by taking advantage of the fact that the number of possible keys is small (only 256 possible keys). This is a brute force attack.

[3] A.

[10] W



