1

Energy Efficient and Secured Cluster Based Routing Protocol for Wireless Sensor Networks

Dananjayan P, Samundiswary P and Vidhya J
Pondicherry Engineering College
Pondicherry,
India

1. Introduction

Recent advances in wireless and ubiquitous computing have prompted much research attention in the area of wireless sensor network (WSN). Sensor network consists of hundreds to thousands of low power multifunctioning sensor nodes operating in hostile environment with limited computational and sensing capabilities. They represent a new paradigm to support a wide variety of data gathering applications such as military, environmental monitoring and other fields ranging from traffic management to high secured monitoring of physical phenomenon (Akyildiz et al., 2002, Kazem et al., 2007). The main task of sensor nodes is to sense and collect data from a target domain, process the data and route the information to the specific sites where the underlying application resides. To achieve these potential, WSNs require novel routing techniques that take into consideration the immense scalability and inaccessibility of sensor devices with limited resources deployed in a harsh environment (Ilyas & Mahgoub, 2005). Moreover, sensor devices are subjected to severe fading, interference and susceptible to various attacks when operated in wireless medium. These constraints present unique design challenges. One of the challenges considered in the chapter is interconnecting a large group of sensors in a viable and secure network. This involves the need of designing a routing protocol which prolongs the network lifetime.

Routing of sensed data from sensor nodes to base station in a wireless sensor network occurs in different methods (Karki & Kamal, 2004). The classical approaches like direct transmission (DT) and multihop routing do not guarantee well balanced distribution of energy among the sensor nodes and are vulnerable to severe attacks. Using DT, each sensor directly sends the gathered information to remote receiver (sink) independent of each other. This approach has an inherent scalability problem and is prone to channel fading. With multihop routing, data is routed over minimum cost routes, and the nodes near the sink tend to die faster (Heinzelman et al., 2000). It can be easily compromised by attackers.

Clustering is the most promising technique that can significantly save the energy of sensor nodes and improve the scalability of the network. In clustering approach, sensors group together to form clusters. One of the sensors in each of the cluster will be elected as cluster head. The elected cluster head will be responsible for relaying data from each sensor in the cluster to the remote receiver. In addition, data fusion and data compression can occur in

the cluster head by considering the potential correlation among data from neighbouring sensors (Do hyun mam & Hong-Ki-Min, 2007, Muruganathan et al., 2005).

Clustered sensor networks can be classified into two broad types: homogenous and heterogeneous sensor networks (Vivek & Catherine, 2004). In homogeneous sensor network, all the sensor nodes are identical in terms of energy and hardware complexity. This type of network consists of purely static clustering (cluster heads once elected, serve for the entire lifetime of the network) and the head node can be easily compromised. It is evident that the cluster head nodes will be over-loaded with the long range transmissions to the remote base station. And also, the extra processing is necessary for the cluster head for data aggregation and protocol co-ordination. As a result, the cluster head nodes expire before other nodes. It is desirable to ensure that all the nodes run out of their battery at about the same time.

One way to ensure this is to rotate the role of a cluster head randomly and periodically over all the nodes as proposed in low energy adaptive clustering hierarchy (LEACH) (Heinzelman et al., 2002, Yu et al., 2007). Since, all the nodes should be capable of acting as cluster heads; the network should possess the necessary hardware capabilities. Hence, the homogenous network requires high hardware cost. It also suffers from poor performance and scalability. To improve the network performance, heterogeneous sensor network (HSN) is formed by deploying a small number of high-end sensors (H-sensors) in addition to a large number of low-end sensors (L-sensors). Compared to an L-sensor, an H-sensor has better computation capability, larger storage and better reliability. However, the performance of HSN will be degraded when sensor nodes are distributed in an insecure and wireless environment. Hence this chapter considers two routing protocols to forward the data packets from source to remote receiver using the cluster based heterogeneous sensor network to overcome fading and defend against attacks such as selective forwarding and sinkhole attacks.

To reduce the fading effects in wireless channel, muti-input muti-output (MIMO) scheme is implemented for sensor network to save energy consumption at sensor nodes (Cui et al., 2004, Bravos & Efthymoglou et al., 2007). Applying multiple antenna technique directly to sensor network is impractical because, the limited size of sensor node usually supports a single antenna. If cooperative transmission and reception from antennas in a group of sensor nodes is used, an equivalent MIMO system for WSN can be realised. Normally, a MIMO system needs to estimate all channels between source and destination. If cooperative transmissions from multiple sensor nodes are allowed, the amount of channel estimation at the receiver can be reduced and hence can save the energy of sensor nodes (Cheng et al., 2006, Jayaweera, 2004).

Li et al., 2005 analysed cooperative multi input single output (MISO) transmission scheme based on LEACH protocol. However cooperative MISO system performs only single hop transmission and does not prolong the network lifetime. To overcome these drawbacks, the proposed model modifies the LEACH routing scheme using HSN architecture and suggests two solutions such as cooperative LEACH (C-LEACH) and cluster head cooperative LEACH (CH-C-LEACH) scheme to maximise the network lifetime. The proposed C-LEACH scheme allows cluster heads to form a multihop backbone and incorporates cooperative MIMO on each single hop transmission by utilising a set of sending and receiving cooperative nodes in each cluster. In CH-C-LEACH scheme, the cluster heads gets paired with other cluster head. They intelligently exchange data and balance communication load and transmit data cooperatively to the base station. To enhance the performance of the proposed routing scheme, cooperative MIMO utilises space time block code (STBC) to

Energy Efficient and Secured Cluster Based Routing Protocol for Wireless Sensor Networks 3

provide significant diversity gain (Tarokh et al., 1999). For the proposed cooperative heterogeneous MIMO routing scheme, the energy consumed and the number of nodes alive for each round of data transmission is evaluated to reduce the channel fading effects and is compared with the traditional LEACH protocol.

Moreover, the lifetime of the network can be enhanced by providing security and privacy against network layer attacks when the nodes are scattered in an unsupervised environment. In order to protect network, few of the routing protocols such as sensor protocols for information via negotiation(SPINS) (Adrian Perrig et al., 2001) and path redundancy based security algorithm (PRSA) for homogeneous based wireless sensor networks (Sami et al., 2007) address the security mechanism and authentication against the various attacks.

Some of the secured routing protocols of heterogeneous sensor networks (Xiaojiang et al., 2006) can detect the malicious nodes and deliver the packets to the sink successfully. But these routing protocols increase the buffering requirements, overheads and delay. Hence, PRSA is extended for heterogeneous sensor networks by including alternate path mechanism to protect the nodes from selective forwarding (Jeremy & Xiaojiang, 2008) and sinkhole attacks in HSN. For the proposed secured routing mechanism, the network performance in terms of energy, delay and delivery ratio in the presence of compromised nodes is evaluated and compared with the heterogeneous network model.

The chapter is organised as follows: section 2 describes the heterogeneous sensor network model. The proposed cluster based cooperative MIMO routing protocols such as C-LEACH and CH-C-LEACH are discussed to minimise the channel fading effects in section 3. The energy consumption model of proposed scheme is analysed in section 4. Simulation results of the cooperative MIMO scheme in terms of energy and delay are discussed to minimize the channel fading in section 5. The various network layer attacks that exist in the sensor network are outlined in section 6. To defend against these attacks section 7 describes the proposed secured path redundancy algorithm in heterogeneous sensor network. Simulation results of the proposed algorithm are discussed in section 8 in terms of energy consumption, delay and delivery ratio and conclusion are drawn in section 9.

2. Heterogeneous sensor network

In the HSN model, H-sensors and L-sensors are randomly distributed in the field and clusters are formed. The cluster formation is shown in Fig.1, where L-sensors are the small squares, H-sensors are large rectangles, and the large square at the top-right corner is the base station (BS). H-sensors serve as cluster heads. The H-sensors have more energy resource, longer transmission range and can handle higher data rate than L-sensors. All the H-sensors form a backbone in the network. H-sensors use multi-hop communications to reach the BS. L-sensors can use single-hop or multi-hop communications to reach H-sensors (Xiaojiang et al., 2006, 2007).

2.1 Routing in heterogeneous sensor network

The primary functionality of a wireless sensor network is to sense the environment and transmit the acquired information to the BS for further processing. Since sensor nodes are small and unreliable devices, they are prone to failures. The routing protocol designed for the network has to be robust to sensor failures by providing new paths. The basic idea of routing in HSN is to let each non-cluster head (L-sensor) to send data to its cluster head (an H-sensor).

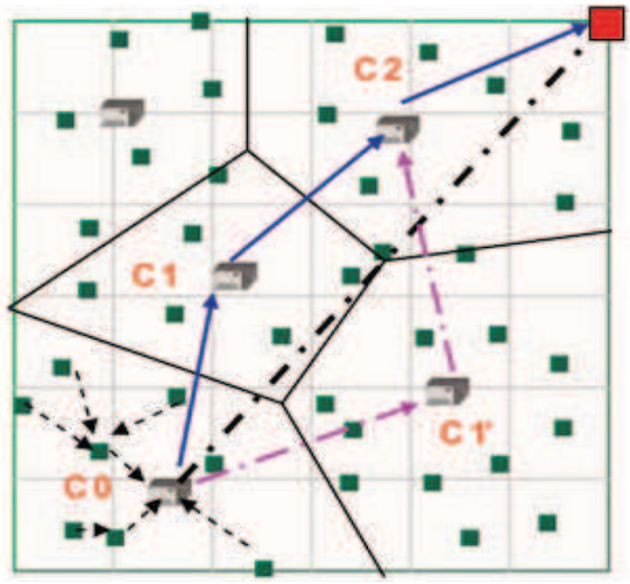


Fig. 1. Heterogeneous sensor network model

i. *Intra- cluster routing*

Routing within a cluster (from an L-sensor to its cluster head) is referred to as intra-cluster routing which is illustrated in Fig.1. L-sensor sends its location information to the cluster head during the cluster formation. The location of H is broadcasted to all L-sensors in the cluster. All the L-sensors in a cluster form a tree, rooted at the cluster head (denoted as H) so that each L-sensor sends packets to its H-sensor, when it generates packets. If data from nearby L-sensor nodes are highly correlated, then a minimum spanning tree (MST) can be adopted to approximate the least energy consumption case.

A centralised algorithm created by H-sensor can be used to construct an MST. Then H disseminates the MST structure information to L-sensors, i.e., informing each L-sensor which node its parent is. If a data fusion is conducted at intermediate L-sensors nodes, then MST consumes the least total energy in the cluster. If there is few or no data fusion among L-sensors in a cluster, a shortest-path tree (SPT) should be used to approximate the least total energy consumption.

Similarly, the cluster head (H-sensor) can construct an SPT by using a centralised algorithm and the locations of L-sensors (Xiaojiang et al., 2006, 2007). In the above route setup, each L-sensor may record two or more parent nodes. One parent node serves as the primary parent, and other parent nodes serve as backup parent. If the primary parent node fails, an L-sensor can use a backup parent for data forwarding. Further each L-sensor records one or more backup cluster heads during cluster formation. When a cluster head fails, L-sensors in the cluster send their packets to a backup cluster head.

ii. *Inter-cluster routing*

Routing across clusters (from an H-sensor to the BS) is referred to as inter-cluster routing which is shown in Fig.1. After receiving data from L-sensors, cluster heads may perform data aggregation via the H-sensor backbone. Each cluster head exchanges location information with neighbor cluster heads. During route discovery, a cluster head draws a straight line L between itself and the BS, based on the location of the BS and itself which is shown in Fig.1. Line L intersects with a serial of clusters, and these clusters are denoted as $C_0, C_1, ..., C_k$,which are referred to as relay cells.

Energy Efficient and Secured Cluster Based Routing Protocol for Wireless Sensor Networks 5

The packet is forwarded from the source cluster head to the BS via cluster heads in the relay cells. H-sensors are more reliable nodes than L-sensors. However, an H-sensor may also fail because of various reasons, such as harsh environment, or may be destroyed by an adversary. If any cluster head in the relay cells is unavailable, then a backup path is used. A backup path is set up as follows: The current cluster head (say R1) draws a straight line L′ between itself and the BS, and line L intersects with several cells $C'_1,...,C'_{k-1},C'_k$. If the next cell is the cell having the failed cluster head, R1 will use a detoured path to avoid the cell. The sequence cells $C'_1,.....,C'_{k-1},C'_k$ will be the new relay cell and are used to forward the packet to the BS.

3. Proposed cluster-based cooperative MIMO routing scheme

A heterogeneous cluster based sensor network model is considered as discussed in section 2. The base station for the network model is assumed to have no energy constraints and is equipped with one or more receiving antennas. The sensor nodes are geographically grouped into clusters consisting of H-sensors, L-sensors, cooperative sending and receiving nodes that sense the data from the sensing field. The H-sensors are reelected after each round of data transmission as in LEACH protocol (Xiangnin & Song Yulin, 2007, Vidhya & Dananjayan, 2009).

3.1 Cooperative heterogeneous MIMO LEACH scheme

The proposed multihop cooperative MIMO LEACH transmission model is illustrated in Fig.2. The transmission procedure of the proposed scheme is divided into multiple rounds. Each round has three phases:

i. *Cluster formation phase*

In this phase, clusters are organised and cooperative MIMO nodes (Yuan et al, 2006) are selected according to the steps described below:

a. *Cluster head advertisement*

Initially, when clusters are being created, each node decides whether or not to become a cluster head for each round as specified by the original LEACH protocol. Each self-selected cluster head, then broadcasts an advertisement (ADV) message using non-persistent carrier sense multiple access (CSMA) MAC protocol. The message contains header identifier (ID).

b. *Cluster set up*

Each non-cluster head node i.e L-sensor node chooses one of the strongest received signal strength (RSS) of the advertisement as its cluster head, and transmits a join-request (Join-REQ) message back to the chosen cluster head i.e H-sensor. The information about the node's capability of being a cooperative node, i.e., its current energy status is added into the message.

If H-sensor receives advertisement message from another H-sensor y, and if the received RSS exceeds a threshold, it will mark H-sensor y as the neighbouring H-sensor and it records y's ID. If the base station receives the advertisement message, it will find the cluster head with the maximum RSS, and sends the base station position message to that cluster head marking it as the target cluster head (TCH).

c. *Schedule creation*

After all the H-sensors have received the join-REQ message, each cluster head creates a time division multiple access(TDMA) schedule and broadcasts the schedule to its cluster members as in original LEACH protocol (Vidhya & Dananjayan, 2010). This prevents collision among data messages and allows the radio of each L-sensor node to be turned off until its allocated transmission time to save energy.

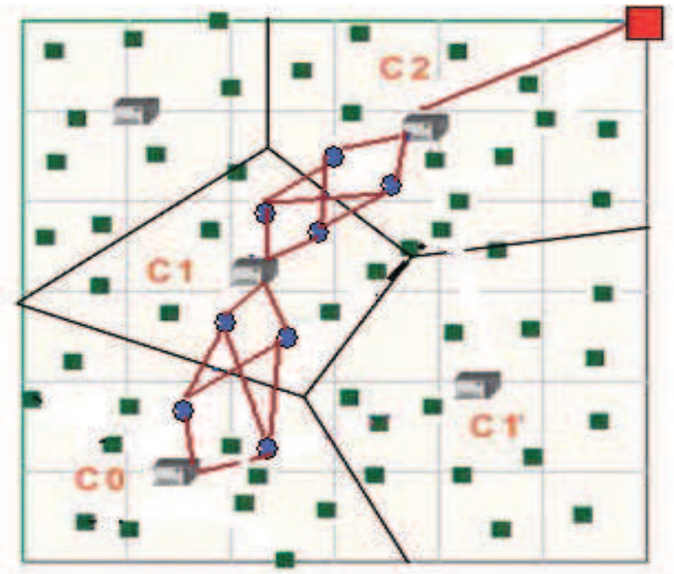


Fig. 2. C-LEACH transmission model

d. *Cooperative node selection*

After the cluster formation, each H-sensor will select J cooperative sending and receiving nodes for cooperative MIMO communication with each of its neighbouring cluster head. Nodes with higher energy close to the H-sensor will be elected as sending and receiving cooperative nodes for the cluster. At the end of the phase, the cluster head will broadcast a cooperative request (COOPERATE-REQ) message, to each cooperative node which contains the ID of the cluster itself, the ID of the neighbouring H-sensor y, the ID of the transmitting and receiving cooperative nodes and the index of cooperative nodes in the cooperative node set for each cluster head to each cooperative node. Each cooperative node on receiving the COOPERATE- REQ message, stores the cluster head ID, the required transmitted power and sends back a cooperate-acknowledgement (ACK) message to the H-Sensor.

ii. *Routing table construction*

Each H-sensor will maintain a routing table which contains the destination cluster ID, next hop cluster ID, IDs of cooperative sending and receiving nodes. Each cluster head will simply inform its neighbouring cluster heads of its routing table. After receiving route advertisements from neighbouring cluster heads, the cluster heads will update the route cost and advertise to their neighbouring cluster heads about the modified routes. Then the TCH will flood a target announcement message containing its ID to each H-sensor to enable transmission paths to the base station.

iii. *Data transmission phase*

In this phase, the L–sensors will transmit their data frames to the H-sensor as in LEACH protocol during their allocated time slot. Each cluster member will transmit its data as specified by TDMA schedule in cluster formation phase, and will sleep in other slots to save energy. The duration and the number of frames are same for all clusters and depend on the number of L-sensor nodes in the cluster. After a cluster head receives data frames from its cluster members as shown in Fig.2, it performs data aggregation to remove redundant data and broadcasts the data to J cooperative MIMO sending nodes. When each cooperative sending node receives the data packet, they encode the data using STBC (Tarokh et al.,1999) and transmit the data cooperatively. The receiving cooperative nodes use channel state

Energy Efficient and Secured Cluster Based Routing Protocol for Wireless Sensor Networks 7

information to decode the space time coded data. The cooperative node relays the decoded data to the neighbouring cluster head node and forwards the data packet to the TCH by multihop routing.

3.2 Cluster head cooperative heterogeneous MIMO LEACH scheme

To further prolong the network lifetime a CH-C-LEACH scheme is proposed and is illustrated in Fig.3. In this scheme the cluster head nodes cooperate and pair among themselves to transmit data cooperatively rather than selecting the cooperative sending and receiving groups in each cluster as specified in section 3.1. The transmission procedure of the proposed scheme split into different rounds and each round has four phases:

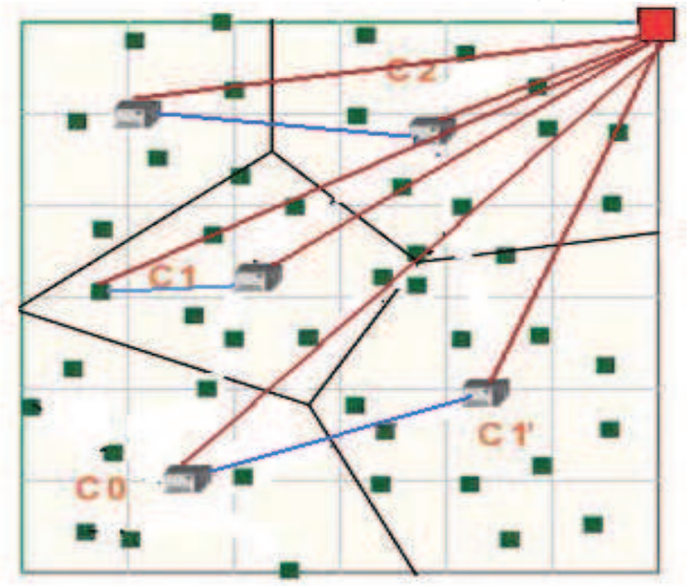


Fig. 3. CH-C-LEACH transmission model

i. *Cluster formation phase*

During this phase, clusters are organised following the same procedure of C-LEACH scheme as described in section 3.1.

ii. *Intra-cluster transmission and data aggregation*

In this phase, the L-sensor sends its packets to the H-sensor. The cluster head then performs data aggregation. At this point, each cluster head knows the volume of data it needs to transmit to the base station.

iii. *Data volume advertisement*

In this phase, the H-sensors inform each other about their data volume by broadcasting a short message that contains the node's ID and the volume of data it needs to transmit. All messages are recorded by each H-sensor. Besides, according to the received signal strength of the advertisement, each cluster head estimates the distances to all other cluster heads and records the information.

iv. *Data exchange and cooperative transmission*

In this phase each H-sensor gets paired with other H-sensor and transmits data cooperatively. The data transmission in CH-C-LEACH scheme is shown in Fig.4 and is described below:

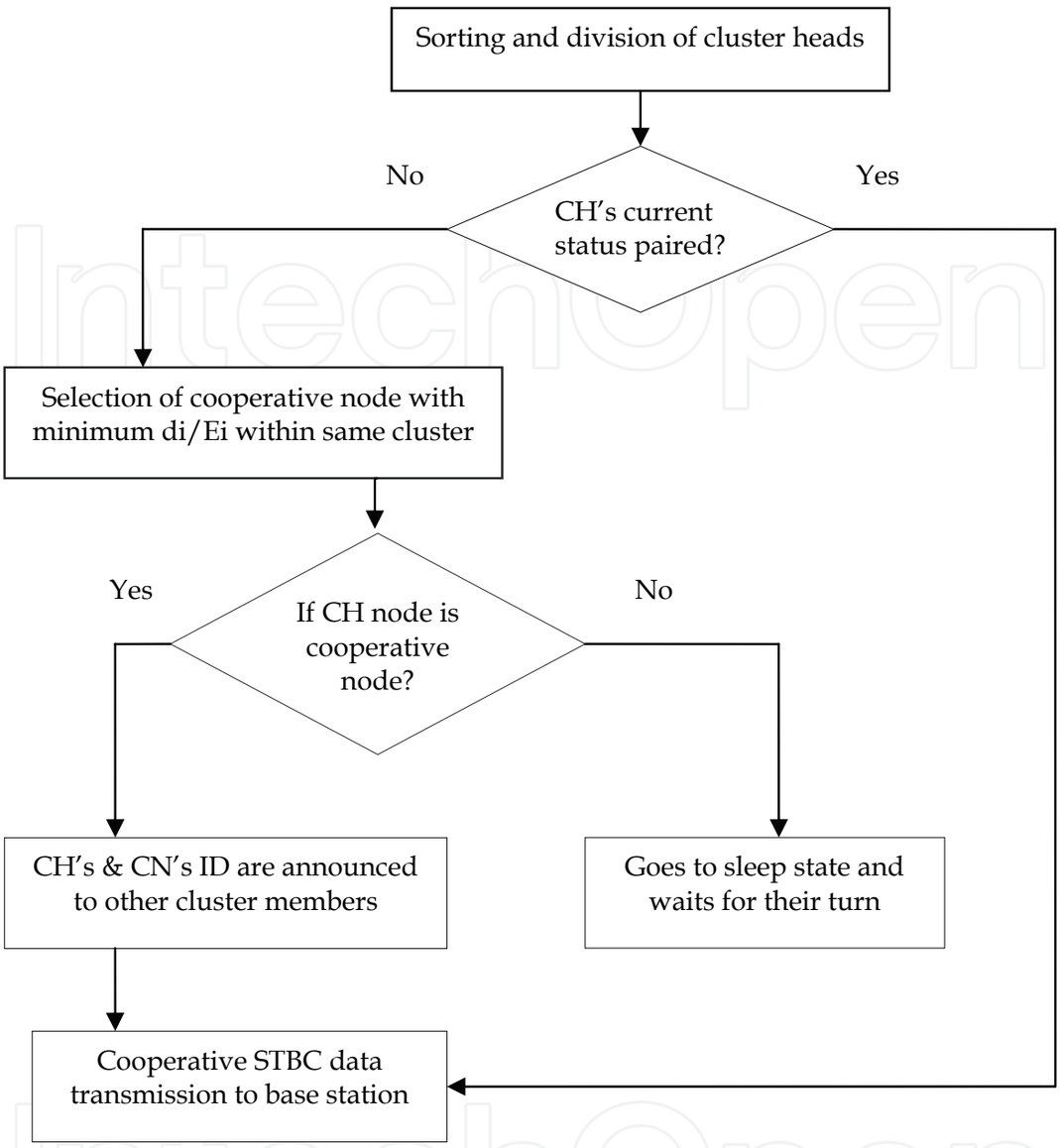


Fig. 4. Flow chart of data transmission in CH-C-LEACH scheme

a. *Sorting and division*

Based on the volume of data available at cluster head, each CH sorts the data and gets the reordered sequence for pairing to enable cooperative MIMO data transmission.

b. *Cooperative node selection and transmission*

If the number of H-sensors is odd, one of the H-sensor selects a cooperative node with minimal di/ Ei within its own cluster, where Ei is the energy status reported by node i and di is the distance between node i and the cluster head. This H-sensor informs the selected cooperative node by broadcasting a short message containing the cluster head's ID, the selected node's ID and an appropriate transmission time T that this pair needs to transmit data to base station. Upon receiving the message, all nodes except this pair of nodes can turn off their radio components to save energy. The cluster heads should wake up at time T, and other L–sensor nodes can remain in the sleep state till the next round. On the other hand, the

Energy Efficient and Secured Cluster Based Routing Protocol for Wireless Sensor Networks 9

H-sensor node sends its data to the selected cooperative node, and they encode the transmission data according to STBC and transmit the data to the base station cooperatively. Once the transmission ends, these two nodes go into the sleep state till the next round.

4. Energy consumption model of the proposed scheme

The energy consumed during each round of data transmission using C-LEACH scheme results from the following sources such as: L-sensor transmitting their data to the H-sensor, routing table constructed by the H-sensor, cluster head transmitting the aggregated data to the cooperative nodes, cooperative node transmitting the data to the receiving cooperative nodes and to the receiving H-sensor. The energy consumed using CH-C-LEACH is due to cluster members transmitting their data to the H-sensor, cluster head transmitting the aggregated data to the cooperative cluster head and H-sensor nodes cooperate to transmit the data to the base station.

i. *Energy consumption of cluster member*

The energy consumed by the source nodes i.e L-sensor to transmit one bit data to the cluster head node for C-LEACH and CH-C-LEACH scheme is given by

$$E_{bs}(k_c) = -\frac{1}{\pi k_c}(1+\alpha)N_f\sigma^2\ln(P_b)G_1M^2M_1 + \frac{P_{ct}+P_{cr}}{B} \tag{1}$$

where k_c is the number of clusters, α is the efficiency of radio frequency (RF) power amplifier, N_f is the receiver noise figure, $\sigma^2=N_o/2$ is the power density of additive white Gaussian noise (AWGN) channel, P_b is the bit error rate (BER) obtained while using phase shift keying, G_1 is the gain factor, M is the network diameter, M_1 is the gain margin, B is the bandwidth, P_{ct} is the circuit power consumption of the transmitter and P_{cr} is the circuit power consumption of the receiver.

The total number of bits transmitted to cluster head of each cluster in each round is given by

$$S_1(k_c) = \left\lceil \frac{N}{k_c} \right\rceil F_n Ps \tag{2}$$

where N is the number of sensor nodes, F_n is the number of symbols in a frame, P is the transmit probability of each node and s is the packet size.

The energy consumed by a cluster member to transmit data to the cluster head is given by

$$E_s(k_c) = k_c S_1(k_c) E_{bs}(k_c) \tag{3}$$

ii. *Energy consumption of cluster heads*

To construct routing table, the energy consumed by H-sensor node for C-LEACH scheme is

$$E_r(k_c) = k_c R_{ts} R_{bt}\left((1+\alpha)M_1N_f \frac{N_0(4\pi)^2(2M)^k}{P_bG_tG_r\lambda^2(\pi k_c)^{k_c/2}} + \frac{P_{ct}+4P_{cr}}{B} \right) \tag{4}$$

where R_{bt} is the time required for exchanging routing information, R_{ts} is the routing table size, k is the path loss factor, G_t is the gain of transmitting antenna, G_r is the gain of receiving antenna and λ is the wavelength of transmission.
The energy per bit consumed by the cluster head node to transmit the aggregated data to J cooperative nodes for C-LEACH and CH-C-LEACH scheme is given by

$$E_{bc0}(k_c, J) = -\frac{1}{\pi k_c}(1+\alpha)N_f\sigma^2\ln(P_b)G_1M^2M_l + \frac{P_{ct} + JP_{cr}}{B} \tag{5}$$

The amount of data after aggregation for each round by H-sensor node is given by

$$S_2(k_c) = \frac{S_1(k_c)}{([N/k_c]Pagg - agg + 1)} \tag{6}$$

where agg is the aggregation factor.
The energy consumed by cluster head node to transmit the aggregated data to J cooperative nodes is given by

$$E_{c0}(k_c, J) = k_c S_2(k_c) E_{bc0}(k_c, J) \tag{7}$$

iii. *Energy consumption of cooperative nodes*
The transmitter cooperative nodes of the cluster will encode and transmit the sequence according to orthogonal STBC to the H-sensor node. Consider the block size of the STBC code is F symbols and in each block pJ training symbols are included and are transmitted in L symbol duration. The actual amount of data required to transmit the $S_2(k_c)$ bits is given by

$$S_e(k_c, J) = FS_2(k_c)/R(F - pJ) \tag{8}$$

where R is the transmission rate.
The energy consumed by J cooperative sending nodes to transmit MIMO data to the J cooperative receiving nodes for C-LEACH scheme is given by

$$E_{cs}(k_c, J) = S_e(k_c, J)\left((1+\alpha)M_lN_f\frac{JN_0(4\pi)^2(2M)^k}{P_b^{1/J}G_tG_r\lambda^2(\pi k_c)^{k_c/2}} + \frac{JP_{ct} + JP_{cr}}{B}\right) \tag{9}$$

Similarly, the energy consumed by J receiving cooperative nodes/cluster head cooperative nodes to transmit data to the neighbouring cluster head/base station respectively for C-LEACH and CH-C-LEACH scheme is given by

$$E_{cr}(k_c, J) = S_e(k_c, J)\left((1+\alpha)M_lN_f\frac{JN_0(4\pi)^2(2M)^k}{P_b^{1/J}G_tG_r\lambda^2(\pi k_c)^{k_c/2}} + \frac{JP_{ct} + P_{cr}}{B}\right) \tag{10}$$

iv. *Over all energy consumption for a round*
The energy consumption for each round of cooperative multihop MIMO data transmission for C-LEACH scheme can be obtained from Equations (3), (4), (7), (9) and (10) and it is given by

Energy Efficient and Secured Cluster Based Routing Protocol for Wireless Sensor Networks 11

$$E(k_c, J) = E_s(k_c) + E_r(k_c) + n_k E_{c0}(k_c, J) + n_k E_{cs}(k_c, J) + n_k E_{cr}(k_c, J) \quad (11)$$

where n_k is the average number of hops.
The energy consumption for each round of data transmission for CH-C-LEACH scheme is given by

$$E(k_c, J) = E_s(k_c) + n_k E_{c0}(k_c, J) + n_k E_{cr}(k_c, J) \quad (12)$$

5. Simulation results

The analysis of the proposed cooperative heterogeneous MIMO schemes discussed in section 4 is carried out using MATLAB to evaluate the energy consumption and maximise the lifetime of the sensor network. A sensing field with a population of N= 100 nodes is considered for simulation with 80 normal nodes and 20 advanced nodes deployed over the region randomly. The initial energy of a normal node is set to 0.5 J and the energy of the advanced node is 2 J.

5.1 Energy consumption analysis

The performance of the proposed C-LEACH scheme is compared with that of the original LEACH scheme in terms of energy and is shown in Fig.5.

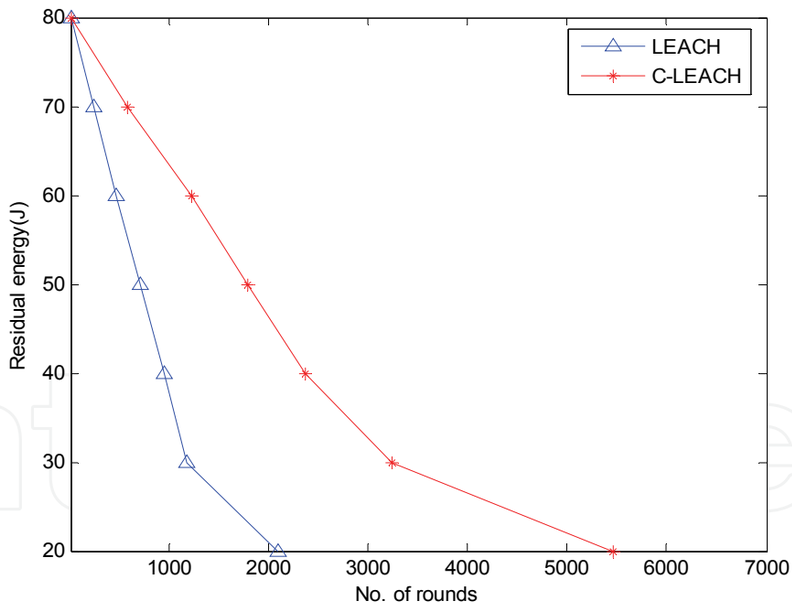


Fig. 5. Energy analysis of C-LEACH scheme

With the use of two cooperative nodes for data transmission, the energy consumption of the network is decreased. This is due to the diversity gain of the MIMO STBC encoded system. From the graph it is clear that the proposed scheme utilising two cooperative sending and receiving nodes can achieve twice the energy savings than LEACH protocol. Fig.6 illustrates the energy performance of proposed CH-C-LEACH scheme. When the cluster head nodes are paired and involved in MIMO data transmission the residual energy of the network for

1000 rounds is 30% more than the LEACH protocol. This is due to the diversity gain of MIMO system.

The performance comparison of proposed C-LEACH and CH-C-LEACH scheme is plotted in Fig.7. The proposed CH-C-LEACH scheme performs better than the proposed C-LEACH scheme by approximately 150 rounds. This is because C-LEACH contributes additional energy consumption in selection of cooperative nodes within a cluster during the cluster setup process.

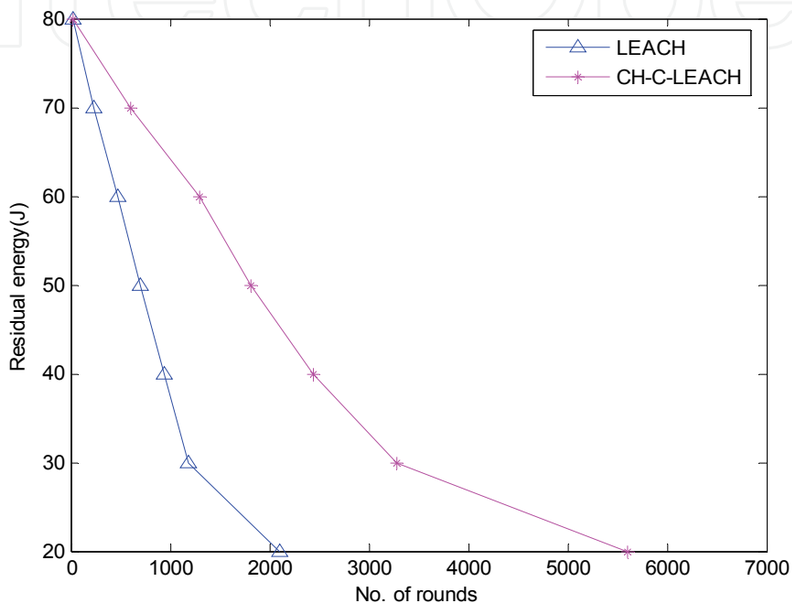


Fig. 6. Energy analysis of CH-C-LEACH scheme

5.2 Network lifetime

The number of nodes alive for each round of data transmission is observed for the proposed scheme to evaluate the lifetime of the network. Fig.8 shows the performance of the system for the LEACH and proposed C-LEACH scheme. It is observed that the proposed C-LEACH scheme outperforms LEACH scheme due to balanced energy dissipation of individual node through out the network.

Similar performance is observed for the proposed CH-C-LEACH scheme in Fig.9. The number of nodes alive after each round of data transmission is greater than LEACH scheme. It is vivid from the graph that 70% of nodes in the LEACH network die in 1250 rounds whereas the proposed CH-C-LEACH scheme prolongs the life time up to 4250 rounds. The performance comparison of proposed C-LEACH and CH-C-LEACH scheme is plotted in Fig.10. The proposed CH-C-LEACH scheme performs better than the proposed C-LEACH scheme by approximately 250 rounds. This is because, the larger energy consumption involved in the data transmission process for C-LEACH scheme reduces the number of alive nodes in the network.

Energy Efficient and Secured Cluster Based Routing Protocol for Wireless Sensor Networks 13

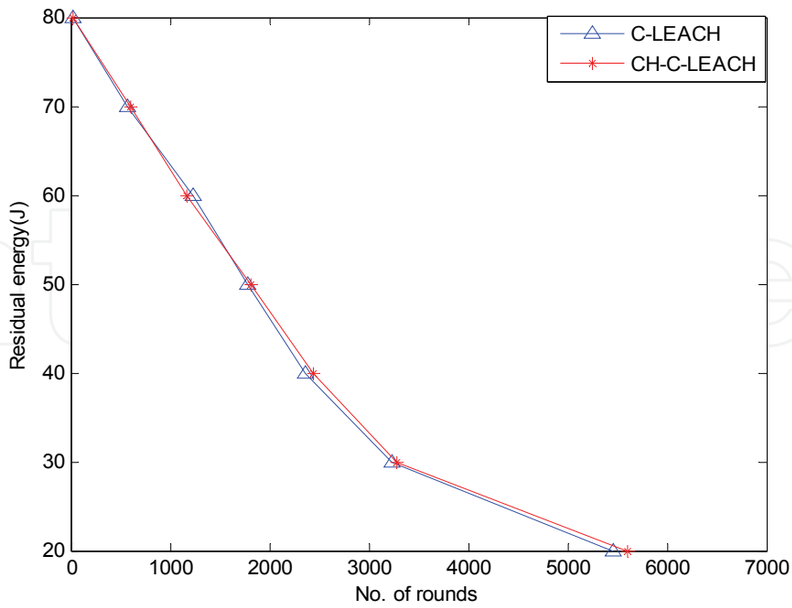


Fig. 7. Energy analysis comparison of C-LEACH and CH-C-LEACH scheme

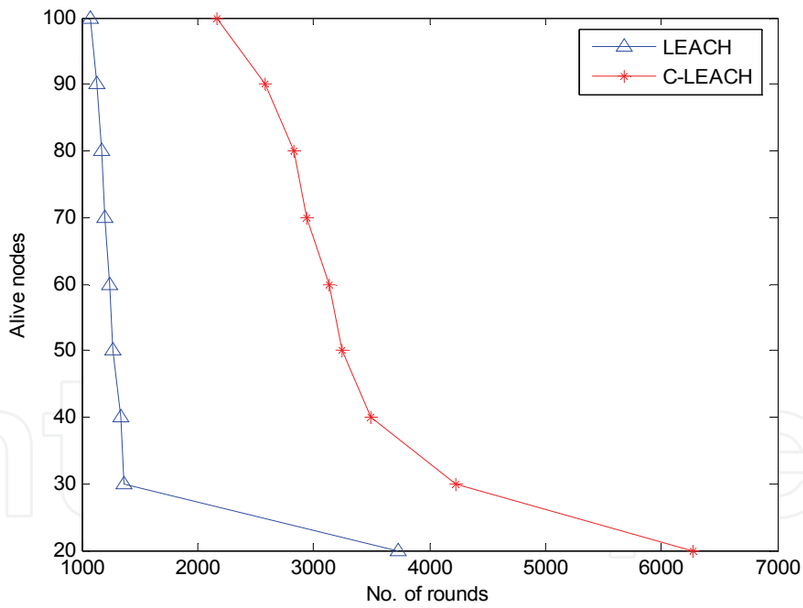


Fig. 8. Network lifetime of C-LEACH scheme

5.3 Percentage of Node death

The number of rounds for every 10% of node death is observed for LEACH and the proposed C-LEACH scheme in Fig.11. From the results it is evident that the lifetime of LEACH protocol is limited to 3750 rounds and the proposed MIMO scheme extents up to 6250 rounds. The proposed C-LEACH scheme provides an extended lifetime of

approximately twice LEACH protocol. Similar performance can be observed with CH-C-LEACH scheme and is shown in Fig.12. The proposed CH-C-LEACH scheme has longer life time than LEACH scheme. Also, the proposed CH-C-LEACH scheme performs better than the proposed C-LEACH scheme by extending the lifetime of approximately 500 rounds as shown in Fig.13.

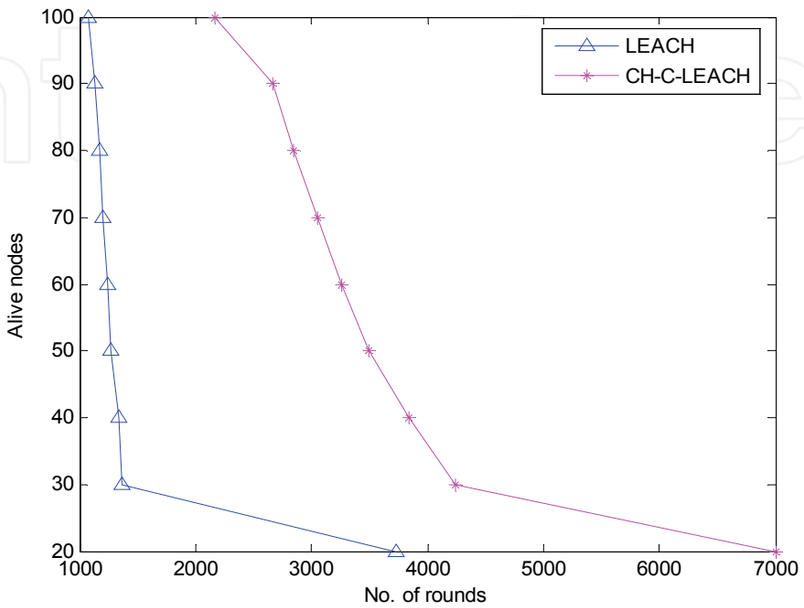


Fig. 9. Network lifetime of CH-C-LEACH scheme

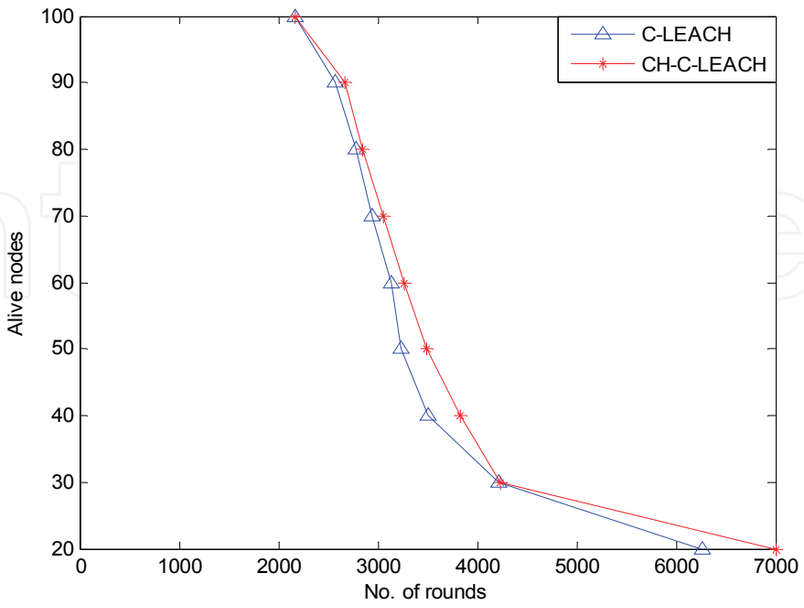


Fig. 10. Comparison of network lifetime for C-LEACH and CH-C-LEACH scheme

Energy Efficient and Secured Cluster Based Routing Protocol for Wireless Sensor Networks 15

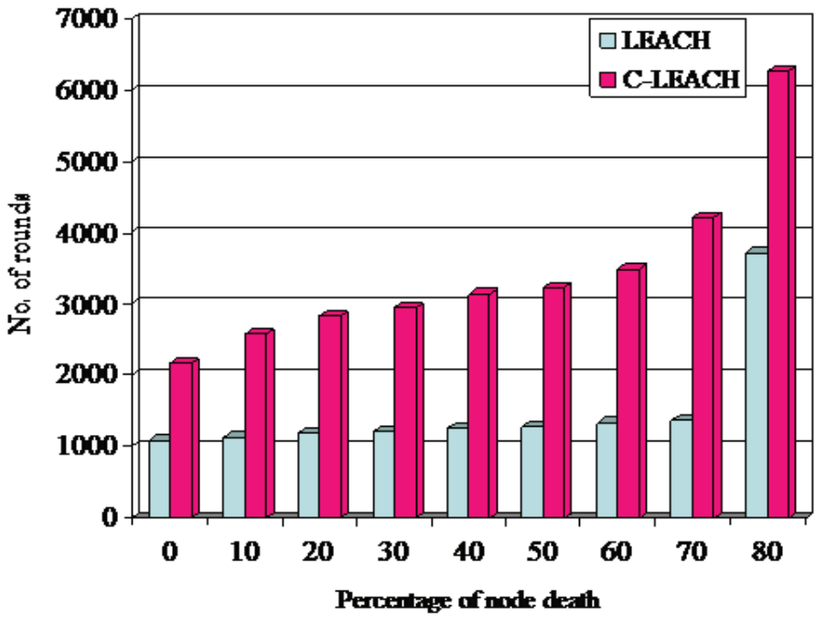


Fig. 11. Percentage of node death with C-LEACH scheme

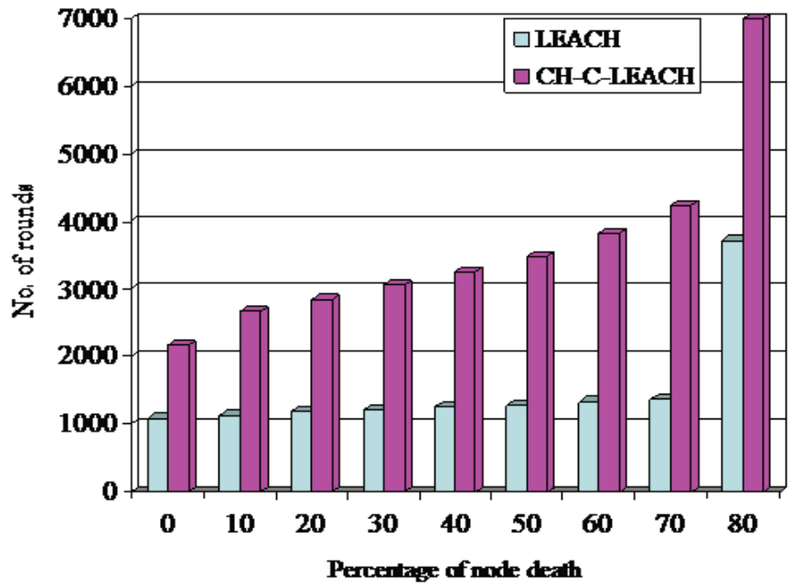


Fig. 12. Percentage of node death with CH-C-LEACH scheme

6. Attacks in wireless sensor network

Security plays an important role in WSN since the nodes are exposed to attacks in ruthless environment. Due to the unattended deployment of the sensor nodes, the attackers can easily capture and convert them as malicious nodes. Routing protocols are common target of these compromised nodes. So the capability of avoiding compromised nodes is quite weak.

The adversary can damage the nodes in physical layer or manipulate data in the data link layer and choose incorrect routing path to destroy the network. The malicious nodes can either join the network externally or may originate internally by compromising an existing benevolent node (Le et al., 2008).

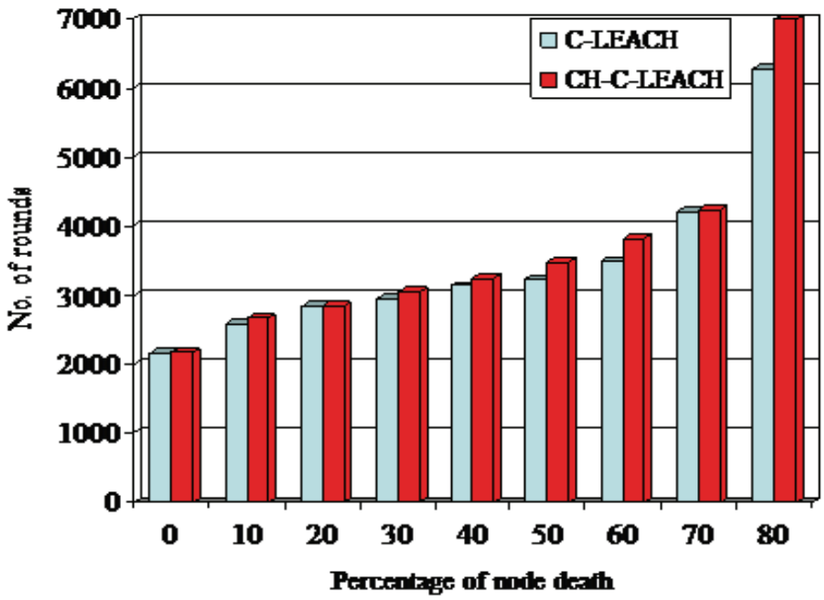


Fig. 13. Percentage of node death with C-LEACH and CH-C-LEACH scheme

These nodes can carry out both passive and active attacks. In passive attacks a malicious node only eavesdrop upon the packet contents, while in active attacks it may imitate, drop or modify legitimate packets. The main active attacks are as follows: spoofed, altered, or replayed routing information, selective forwarding attacks, sinkhole attacks, wormholes, sybil attacks and HELLO flood attacks which are applied to compromise the routing protocols of wireless sensor network. The various types of attacks that occur in sensor networks are shown in Fig.14.

6.1 Attacks in heterogeneous sensor network

i. *Selective Forwarding*

In a selective forwarding attack, malicious nodes may refuse to forward certain messages and simply drop them, ensuring that they are not propagated any further. A simple form of this attack is when a malicious node behaves like a black hole; it refuses to forward every packet it sees. However, such an attacker runs the risk that neighboring nodes will conclude that it has failed and decided to seek another route. A more subtle form of this attack is when an adversary selectively forwards packets. An adversary interested in suppressing or modifying packets originating from a selected set of nodes can reliably forward the remaining traffic and limit suspicion of its wrong doing (Xiaojiang et al., 2006, 2007).

Selective forwarding attacks are typically most effective when the attacker is explicitly included on the path of a data flow. However, it is conceivable that an adversary overhearing a flow passing through neighboring nodes might be able to emulate selective forwarding by jamming or causing a collision on each forwarded packet of interest. The

Energy Efficient and Secured Cluster Based Routing Protocol for Wireless Sensor Networks 17

mechanics of such an effort are tricky at best, and may border on impossible. Thus, an adversary launching a selective forwarding attack will likely follow the path of least resistance and attempt to include itself on the actual path of the data flow.

ii. *Sinkhole attack*

In a sinkhole attack, a malicious node uses the faults in a routing protocol to attract much traffic from a particular area, thus creating a sinkhole (Karlof et al., 2003). The adversary's goal of this attack is to lure nearly all the traffic from a particular area through a compromised node, creating a metaphorical sinkhole with the adversary at the center. Because, sinkhole attacks can enable many other attacks (selective forwarding, for example). Sinkhole attacks typically work by making a compromised node look especially attractive to surrounding nodes with respect to the routing algorithm (Xiaojiang, 2008). For instance, an adversary could spoof or replay an advertisement for an extremely high quality route to a base station. Some protocols might actually try to verify the quality of route with end-to-end acknowledgements containing reliability or latency information.

In this case, a laptop-class adversary with a powerful transmitter can actually provide a high quality route by transmitting with enough power to reach the base station in a single hop. Due to either the real or imagined high quality route through the compromised node, it is likely each neighboring node of the adversary will forward packets destined for a base station through the adversary, and also propagate the attractiveness of the route to its neighbours. Effectively, the adversary creates a large "sphere of influence", attracting all traffic destined for a base station from nodes several hops away from the compromised node. Since all packets share the same ultimate destination, a compromised node needs only to provide a single high quality route to the base station in order to influence a potentially large number of nodes.

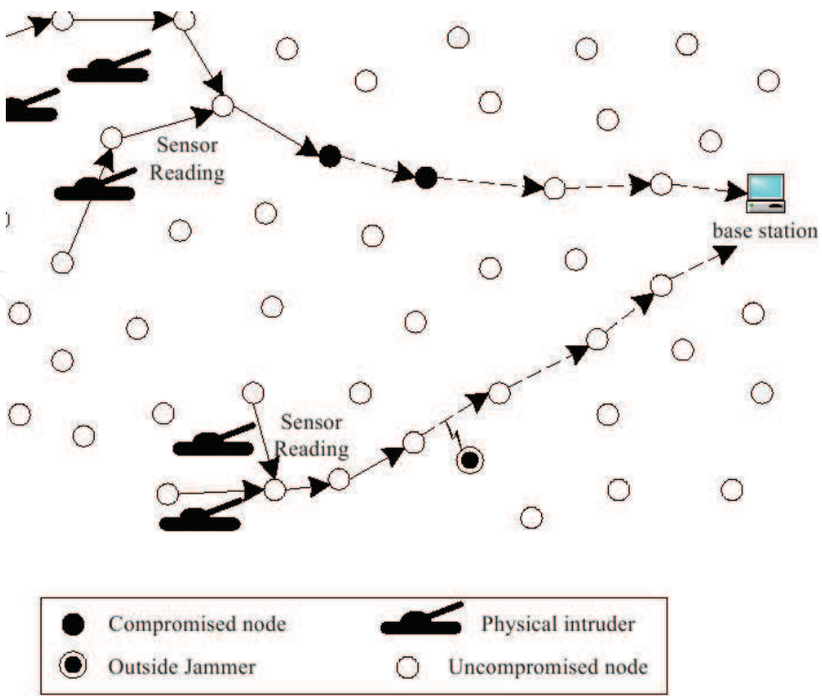


Fig. 14. Attacks in sensor network

7. Secured path redundancy algorithm in heterogeneous sensor network

The alternate path redundancy algorithm is used to find secure multiple paths between the source and destination nodes in the presence of attackers. Selective forwarding and sinkhole attacks are types of attackers that make a compromised node look more attractive to surrounding L-sensor nodes of HSN by forging routing information (Samundiswary & Dananjayan, 2010). The end result is that surrounding L-sensor nodes of HSN will choose the compromised node as the next node to route the data through. This is achieved by removing one or more L-sensor nodes that is suspected to be an active adversary node from the routing path. Such nodes are identified by algorithm using a set of parameters that is usually reflecting the presence of adversary nodes. The parameters used are packet ID, number of hop counts and delay to reach the destination. This secured path redundancy algorithm mechanism can defend against the above mentioned attacks (Xiaojiang, 2008).
Further more, sink mobility brings new challenges to data dissemination in large sensor networks. Sink mobility suggests that information about each mobile sink's location be continuously propagated throughout the sensor field in order to keep all sensor nodes informed about the direction of forwarding future data reports. Unfortunately, frequent location updates from multiple sinks can lead to both excessive drain of sensors' battery resources and increased collisions in wireless transmissions. To avoid these limitations, the same secured path redundancy algorithm for HSN approach is extended for mobile sinks as shown in Fig. 15.

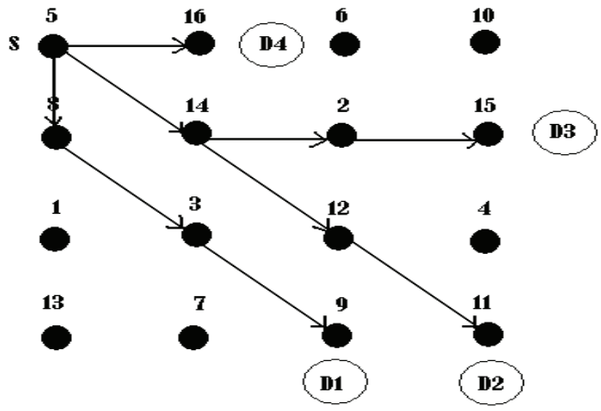


Fig. 15. Mobile sink

8. Simulation results

The secured path redundancy algorithm for static nodes with sink mobility in heterogeneous sensor network is simulated by varying the number of nodes from 25 to 500 with 30 and 50 numbers of malicious nodes for different coverage area in Glomosim. The energy consumption, delivery ratio and delay are calculated for proposed algorithm considering constant bit rate (CBR) traffic in the network.

8.1 Energy consumption

The simulation results shown in Fig.16, Fig.17 and Fig.18 prove that there is a significant reduction in the energy consumption of secured heterogeneous sensor networks by

Energy Efficient and Secured Cluster Based Routing Protocol for Wireless Sensor Networks 19

increasing the numbers of nodes and number of mobile sinks for different coverage area and different values of malicious nodes. Fig.16 shows that there is increment in the energy consumption of secured heterogeneous sensor networks for increased coverage area. When the number of nodes increases, the energy consumption of secured heterogeneous sensor networks reduces from 57% to 81.5% compared to heterogeneous sensor networks with 30 malicious nodes and the coverage area of 300m×300m.

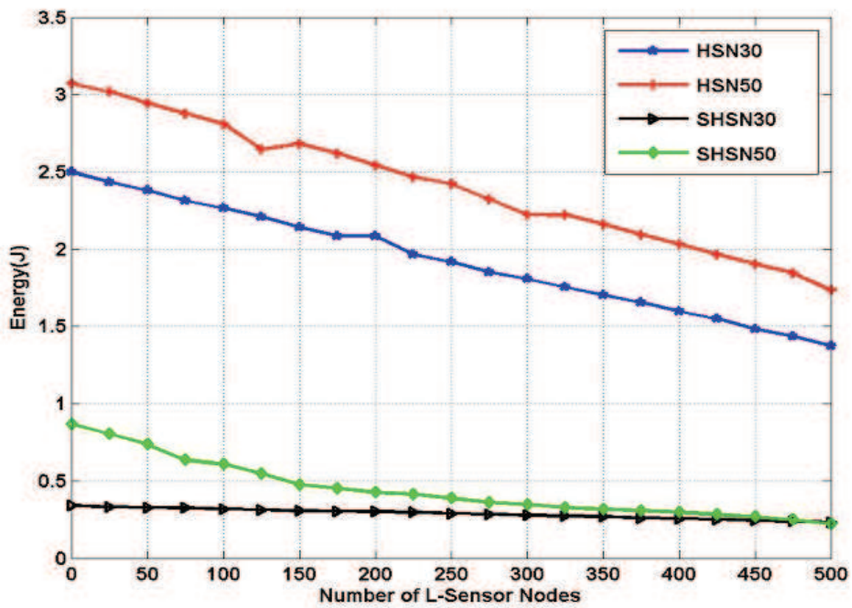


Fig. 16. Energy consumption with number of L-sensor nodes for coverage area 300m×300m

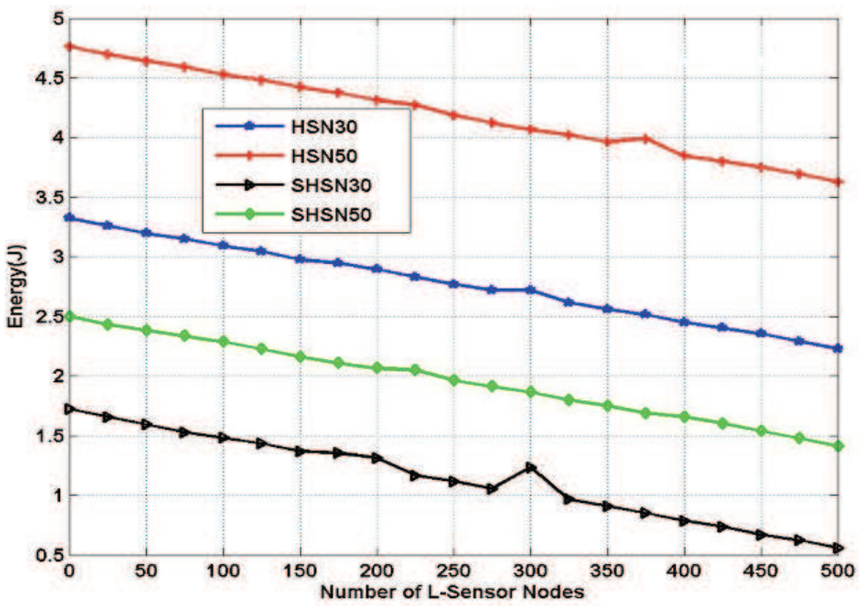


Fig. 17. Energy consumption with number of L- sensor nodes for coverage area 500m×500m

Even if the number of malicious nodes and coverage area increases, the energy consumption reduces by 49% to 67% with respect to heterogeneous sensor networks. Energy consumption of secured heterogeneous sensor networks is lesser than heterogeneous sensor networks because nodes involve alternate shortest secured path and less number of broken paths by using H-sensors even in the presence of malicious nodes.

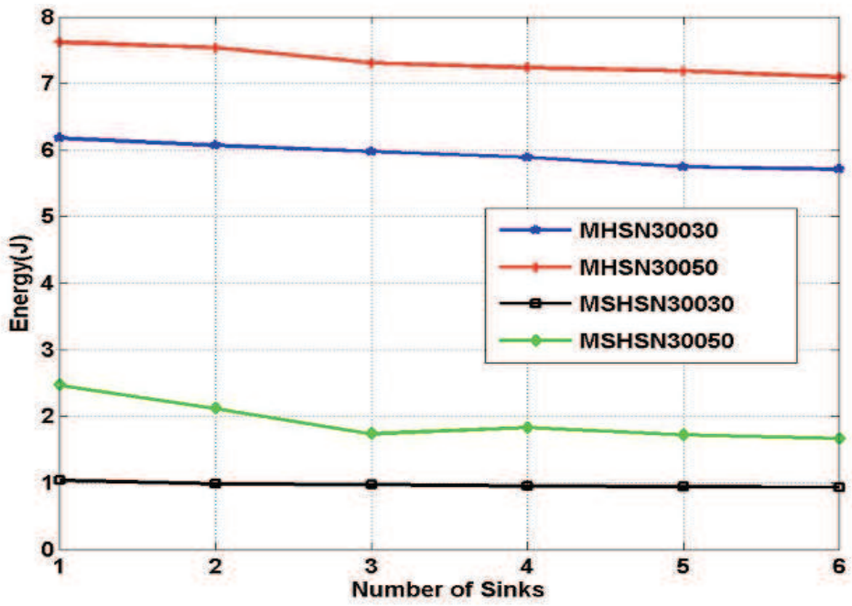


Fig. 18. Energy consumption with number of mobile sinks for coverage area 300m×300m

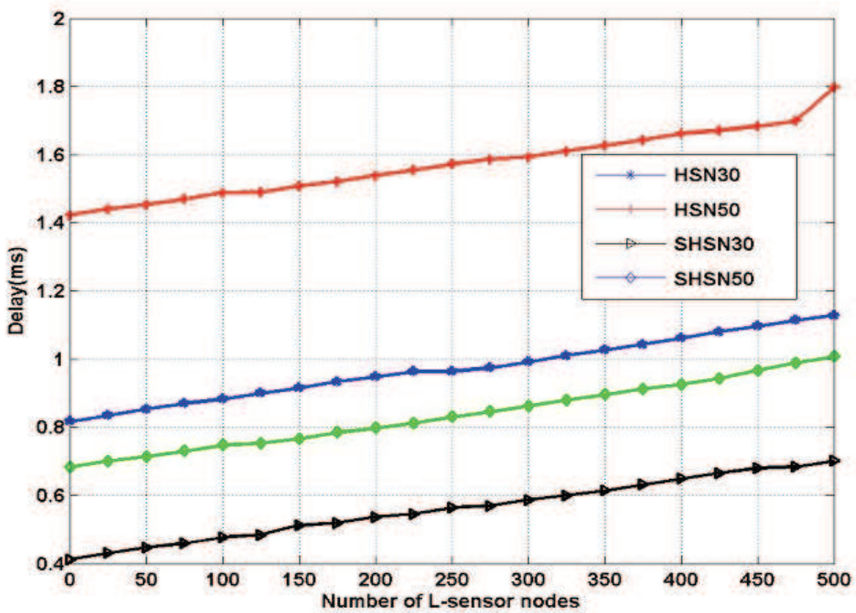


Fig. 19. Delay with respect to number of L-sensor nodes for coverage area 300m×300m

Energy Efficient and Secured Cluster Based Routing Protocol for Wireless Sensor Networks 21

8.2 Delay

The delay graph is illustrated in Fig.19, Fig.20 and Fig.21 considering different coverage areas and various values of mobile sinks with 30 and 50 malicious nodes. The results prove that secured path redundancy algorithm (SPRA) for heterogeneous sensor network nodes is lower than that of HSN by 50% to 55% in case of 30 malicious nodes for network coverage area of 300m×300m and 500m×500m. Since proposed security algorithm for heterogeneous sensor network uses a secured path, packets require less hop count and link failures to reach the mobile sinks from the source even in the presence of malicious nodes.

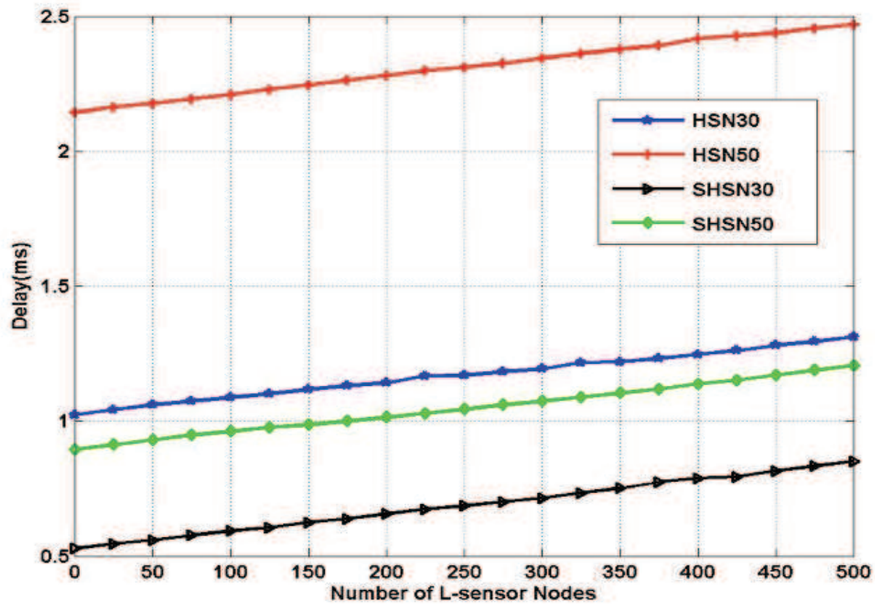


Fig. 20. Delay with respect to number of L-sensor nodes for coverage area 500m×500m

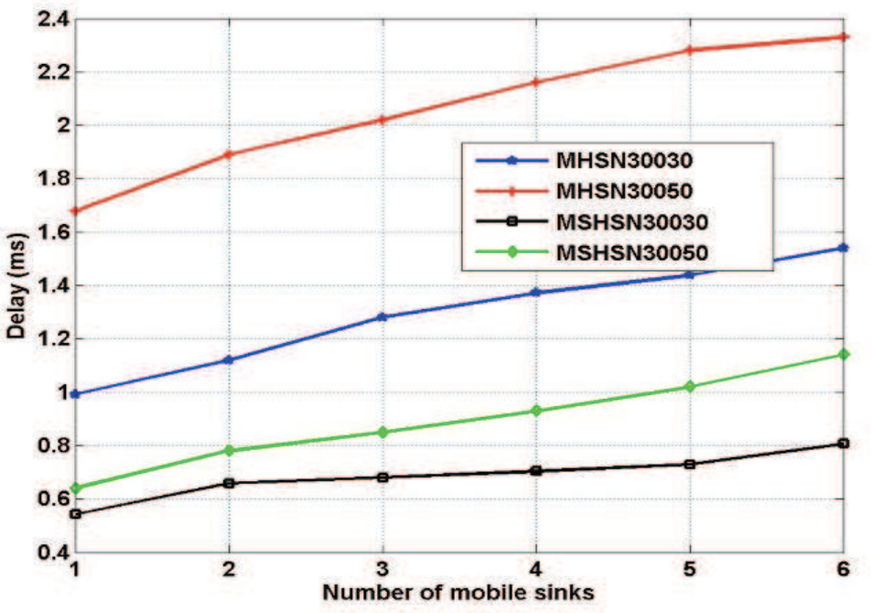


Fig. 21. Delay with respect to number of mobile sinks for coverage area 300m×300m

8.3 Delivery ratio

Delivery ratio of proposed SPRA for heterogeneous sensor networks is higher than conventional HSN which is shown in Fig.22, Fig.23 and Fig.24 for different values of malicious nodes and different coverage area.

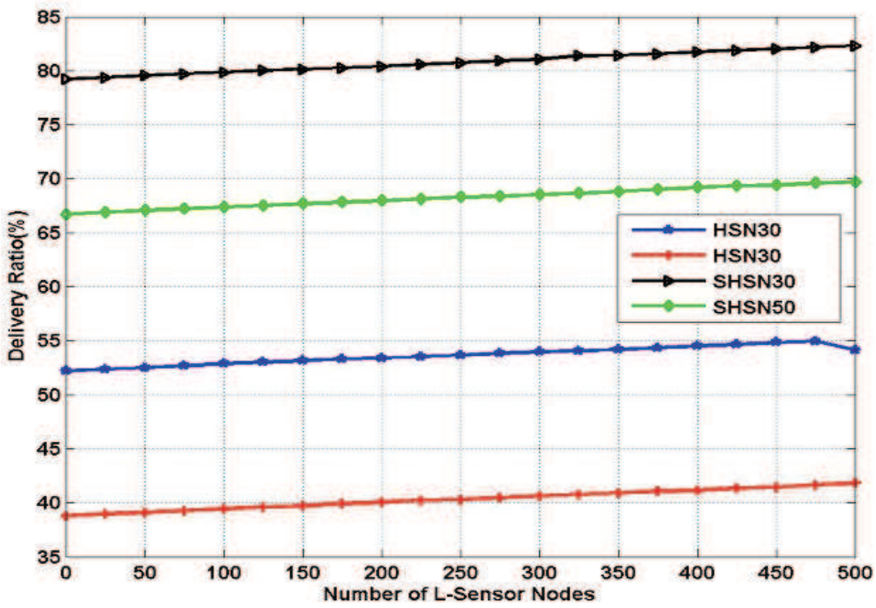


Fig. 22. Delivery ratio with respect to number of L-sensor nodes for coverage area 300m×300m

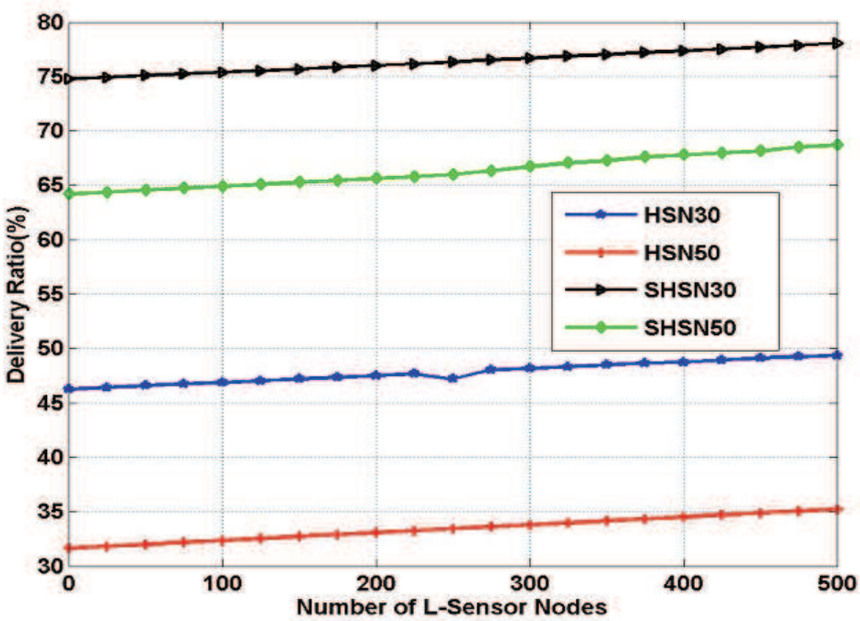


Fig. 23. Delivery ratio with respect to number of L-sensor nodes for coverage area 500m×500m

Energy Efficient and Secured Cluster Based Routing Protocol for Wireless Sensor Networks 23

In Fig.22, the delivery ratio of proposed security algorithm (SPRA) of heterogeneous sensor network is higher than that of heterogeneous sensor network in the presence of malicious nodes by 60%-70%. The fact is that secured HSN packets require less number of hops from the L-sensors to the cluster head than HSN. Moreover, the packet loss is reduced due to secured path from source to sink in secured heterogeneous sensor network.

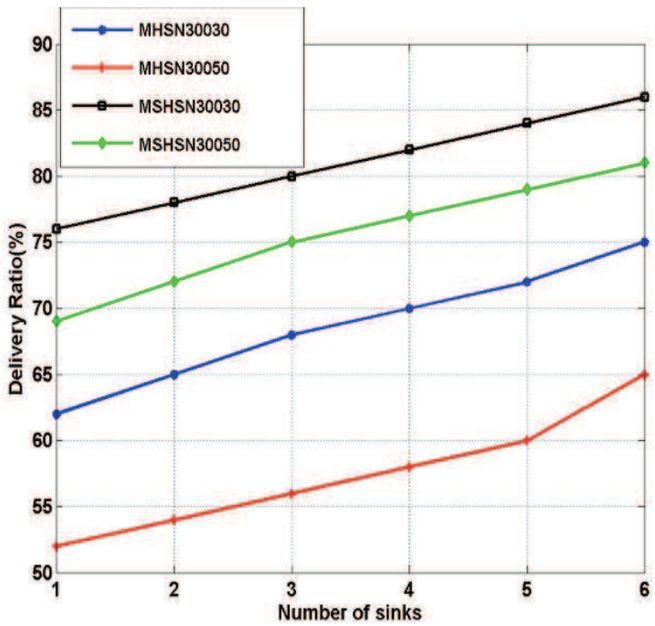


Fig. 24. Delivery ratio with respect to number of mobile sinks for coverage area 300m×300m.

9. Conclusion

This chapter proposed two routing mechanisms to reduce the fading effects and defend against network layer attacks by incorporating cooperative MIMO routing scheme and SPRA in heterogeneous sensor networks.

A cluster-based cooperative heterogeneous MIMO routing scheme using STBC for WSN has been explored for 100 sensor nodes with initial energy of 0.5J for normal nodes and 2J for advanced nodes. The secured path redundancy algorithm for heterogeneous sensor networks is simulated by varying the number of nodes from 100 to 500 and malicious nodes (30 and 50) with mobile sinks (1 to 6).

The performance of the proposed cooperative heterogeneous MIMO system is evaluated to minimise the energy consumption and increase the lifetime of sensor nodes. The simulation results reveal that the LEACH protocol consumes more energy and has shorter lifetime of 3750 rounds due to the adverse channel fading effects. The proposed cooperative heterogeneous MIMO CH-C-LEACH performs better and extends 3250 rounds and 750 rounds more than the LEACH scheme and C-LEACH scheme respectively for data transmission. The proposed scheme saves up to 50% energy compared to LEACH by the exploitation of the diversity gain of MIMO systems.

The performance of the proposed SPRA of heterogeneous sensor network is verified through simulation by evaluating energy consumption, delay and the delivery ratio in the

presence of selective forwarding and sink hole attacks. The simulation results prove that secured path redundancy algorithm in heterogeneous sensor networks has better network performance than that of conventional heterogeneous sensor networks. The reduction in the energy consumption of 60% is achieved by using this algorithm compared to that of conventional heterogeneous sensor networks. The results also demonstrate that the enhancement in delivery ratio of approximately 65% and end to end delay of roughly 52% is achieved through secured heterogeneous sensor network. The improved performance of this algorithm is due to the usage of a secured alternate path which involves less number of broken paths, hop count and less packet loss to reach the destination node.

The further enhancement of the work is to extend the routing scheme taking into account mobile H- sensors. To reduce the energy consumption further due to fading effects other space time encoding schemes and modulation levels of PSK can be implemented to improve network lifetime. For enhancing the security of the system a modified algorithm can be suggested to defend against other network layer attacks such as worm hole and sybil attack.

10. References

Adrian Perrig,; Robert Szewczyk,; Victor Wen,; David Culler & Tygar, J.D. (2001). SPINS: Security protocols for sensor networks, *Proceedings of ACM Annual International Conference on Mobile Computing and Networking*, pp.189-199, ISBN: 1-58113-422-3, Rome, Italy, July, 2001, ACM, New York.

Akyildiz, L.; Su, W.; Sankarasubramanian, Y. & Cayirci, E. (2002). A survey on sensor networks. *IEEE Communications Magazine*, Vol.40, No.8, August 2002, pp.102-114.

Bravos, G.N. & Efthymoglou, G. (2007). MIMO-based and SISO multihop sensor network: Energy efficiency evaluation. *Proceedings of* 3rd *IEEE International Conference on Wireless and Mobile Computing, Networking and Communications*. pp.13, ISBN: 0-7695-2889-9, NewYork, USA, October 2007.

Cheng, W.; Xu, K.; Yang, Z & Feng, Z. (2006). An energy-efficient cooperative MIMO transmission scheme for wireless sensor networks. *Proceedings of International Conference on Wireless Communication, Networking and Mobile Computing*, pp.1-4, ISBN: 1-4244-0517-3, Wuhan, September 2006.

Cui, S.; Goldsmith, A.J. & Bahai, A. (2004). Energy-efficiency of MIMO and cooperative techniques in sensor networks, *IEEE Journal on Selected Areas in Communications*, Vol.22, No.6, August 2004, pp.1089-1098.

Do hyun mam & Hong-Ki-Min. (2007). An Efficient Ad hoc routing using a hybrid clustering method in a wireless sensor network. *Proceedings of 3rd IEEE International Conference on Wireless and Mobile Computing, Networking and Communications,* pp.60, ISBN: 0-7695-2889-9, NewYork, USA, October 2007.

Heinzelman, W.B.; Chandrakasan, A.P. & Balakrishnan, H. (2000). Energy –efficient communication protocol for wireless micro sensor networks, *Proceedings of the 33rd Hawaii International Conference on System Science*, pp.3005-3014, Mauri, Hawaii, January 2000.

Heinzelman, W.B.; Chandrakasan, A.P. & Balakrishnan, H. (2002) . An application-specific protocol architecture for wireless microsensor networks, *IEEE Transactions on Wireless Communications*, Vol.1, No.4, October 2002, pp.660 - 670.

Ilyas, M. & Mahgoub, I. (2005). *Handbook of sensor networks: Compact wired and wireless sensing systems*. Boca Raton, FL.

Energy Efficient and Secured Cluster Based Routing Protocol for Wireless Sensor Networks 25

Jayaweera, S.K. (2004). Energy analysis of MIMO techniques in wireless sensor networks. (2004). *Proceedings of 36th Annual Conference on Information Sciences and Systems*, Princeton, NJ, March 2008.

Jeremy Brown & Xiaojiang Du. (2008). Detection of selective forwarding attacks in heterogeneous sensor networks. *Proceedings of IEEE International Conference on Communications,* pp.1583-1587, ISBN: 978-1-4244-2075-9, Beijing, China, May 2008, IEEE.

Karki, J.A. & Kamal, A.E. (2004). Routing techniques in wireless sensor networks: A survey. *IEEE Personal Communication*, Vol.11, No.6, December 2004, pp.6-28.

Karlof.C. & Wagner.D (2003).Secure routing in wireless sensor networks: attacks and countermeasures. *Proceedings of 1st International Workshop on Sensor Protocols and Applications*, pp.113-127, ISBN: 0-7803-7879-2, Anchorage, AK, May 2003, IEEE.

Kazem Sohraby,; Daniel Minoli & Taieb Zanti. (2007). *Wireless sensor network technology, protocols and applications*. John Wiley and Sons Inc., ISBN: 978-0-471-74300-2.

Li, X.; Chen, M. & Liu, W. (2005). Application of STBC-encoded cooperative transmissions in wireless sensor networks. *IEEE Signal Processing Letters*, Vol.22, No.2, February 2005, pp.134-137.

Le Xuan Hung,; Ngo Trong Canh,; Sungyoung Lee,; Young-Koo Lee & Heejo Lee. (2008). An energy-efficient secure routing and key management scheme for mobile sinks in wireless sensor networks using deployment knowledge. *Journal on Sensors,* Vol.8, December 2008, pp.7753-7782.

Muruganathan, S.D.; Ma, D.C.F.; Bhasin, R.I & Fapojuwo, A.O. (2005). A centralized energy-efficient routing protocol for wireless sensor networks. *IEEE Radio Communications*, March 2005, pp. s8-s13.

Sami,; Al-Wakeel, S. & Al-Swailem, A. (2007). PRSA: A path redundancy based security algorithm for wireless sensor networks. *Proceedings of IEEE Wireless Communication and Networking Conference,* pp.4156-4160, ISBN: 1-4244-0658-7, Kowloon, China, March, IEEE.

Samundiswary, P. & Dananjayan, P. (2010). Detection of Sinkhole attacks for mobile nodes in heterogeneous sensor networks with mobile sinks. *International Journal on Computer and Electrical Engineering*, Vol.2, No.1, February 2010, pp.127-133, ISSN online: 1793-8198.

Tarokh,V.; Jafarkhani, H. & Calderbank, A.R. (1999). Space-time block codes from orthogonal designs. *IEEE Transactions on Information Theory,* Vol.45, No.5, July 1999, pp. 1456-1467.

Vidhya, J. & Dananjayan, P. (2009). A hybrid clustering protocol for energy-efficient routing in wireless sensor networks. *International Journal of Electronics Engineering*, Vol.1, No.1, January 2009, pp.7-12, ISSN: 0973-7383.

Vidhya, J. & Dananjayan, P. (2010). Life time maximization of multihop WSN protocol using cluster based cooperative MIMO scheme. *International Journal of Computer Theory and Electrical Engineering*, Vol.2, No.1, February 2010, pp. 1793-8201, ISSN online: 1793-8201.

Vivek Mhatre & Catherine Rosenberg. (2004). Homogeneous Vs Heterogeneous clustered sensor networks: A comparative study. *Proceedings of IEEE International Conference on Communications*, Vol.6, pp.3646-3651, ISBN: 0-7803-8533-0, Paris, France, June 2004, IEEE.

Xiaojiang Du, ; Sghaier Guizani,; Yang Xiao & Hsiao-Hwa Chen. (2006). A secure routing protocol for heterogeneous sensor networks. *Proceedings of IEEE Global Telecommunication Conference (GLOBECOM'06),* pp.1-5, ISBN: 1-4244-0356-1, San Francisco, California, December, IEEE.

Xiaojiang Du,; Mohsen Guizani,; Yang Xiao & Hsiao-Hwa Chen. (2007). Two tier secure routing protocol for heterogeneous sensor networks. *IEEE Transactions on Wireless Communications*, Vol.6, No.9, September 2007, pp.3395-3407, ISSN: 1536-1276.

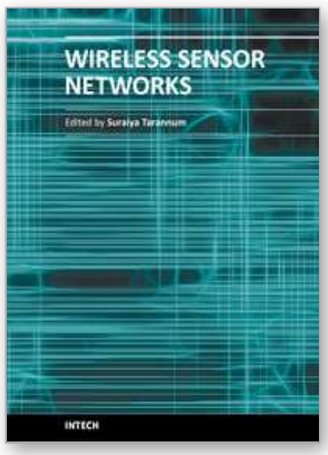
Xiaojiang Du. (2008). Detection of compromised sensor nodes in heterogeneous sensor networks. *Proceedings of IEEE International Conference on Communications,* pp.1446-1450, ISBN: 978-1-4244-2075-9, Beijing, China, May, IEEE.

Xiangning, F. & SongYulin. (2007). Improvement on LEACH protocol of wireless sensor network. *Proceedings of International Conference on Sensor Technologies and Applications*, pp. 260-264, Valencia, Spain, October 2007.

Xu, K.; Hong, X. & Gerla, M. (2005). Improving routing in sensor networks with heterogeneous sensor nodes. *Proceedings of IEEE 61st Vehicular Technology Conference*, pp.2528-2532, ISBN: 0-7803-8887-9, Stockholm, Sweden, Vol.4, May 2005, IEEE.

Yuan, Y.; He, Z. & Chen, M. (2006). Virtual MIMO- based cross-layer design for wireless sensor networks. *IEEE Transactions on Vehicular Technology*, Vol.55, No.3, May 2006, pp.856 -864.

Yu, M.; Leung, K. & Malvankar, A. (2007). A dynamic clustering and energy efficient routing technique for sensor networks. *IEEE Transactions on Wireless Communication*, Vol.6, No.8, August 2007, pp.3069-3078.



Wireless Sensor Networks

Edited by

ISBN 978-953-307-325-5
Hard cover, 342 pages
Publisher InTech
Published online 29, June, 2011
Published in print edition June, 2011

How to reference

In order to correctly reference this scholarly work, feel free to copy and paste the following:

Dananjayan P, Samundiswary P and Vidhya J (2011). Energy Efficient and Secured Cluster Based Routing Protocol for Wireless Sensor Networks, Wireless Sensor Networks, (Ed.), ISBN: 978-953-307-325-5, InTech, Available from: http://www.intechopen.com/books/wireless-sensor-networks/energy-efficient-and-secured-cluster-based-routing-protocol-for-wireless-sensor-networks

INTECH
open science | open minds

InTech Europe
University Campus STeP Ri
Slavka Krautzeka 83/A
51000 Rijeka, Croatia
Phone: +385 (51) 770 447
Fax: +385 (51) 686 166
www.intechopen.com

InTech China
Unit 405, Office Block, Hotel Equatorial Shanghai
No.65, Yan An Road (West), Shanghai, 200040, China
中国上海市延安西路65号上海国际贵都大饭店办公楼405单元
Phone: +86-21-62489820
Fax: +86-21-62489821

IntechOpen