Asian Journal of Information Technology 16 (1): 69-76, 2017
ISSN: 1682-3915
© Medwell Journals, 2017

Detection and Prevention of Wormhole Attacks in Leach Protocol for Wireless Sensor Networks

[1]R.M. Dilip Charaan, [1]R. Ramesh and [1]E. Uma
[1]Department of Electrical and Electronics Engineering,
College of Engineering, Anna University, 25 Chennai, India
[2]Department of Information Science and Technology, Anna University, 25 Chennai, India

Absract: Due to the remote wireless nature and human unattended environment of WSN, they are more vulnerable to various types of attacks and intruders may visit these networks purposely or unintentionally. The algorithms proposed in order to detect if any intruder is inside the network and to detect the wormhole and black hole attacks. In this detection technique it tries to prevent the attacks in LEACH protocol in a wireless sensor networks using the multiple base stations and key. Since, LEACH protocol is used the consumption of energy is also reduced to maximum extent. This in turn reduces the overhead and data delivery increases. As multiple base stations are employed data gets delivered cent percent. Since, LEACH protocol is used, it guarantees power supply for a considerable amount of time with extra energy. This ensures that the packet delivery ratio has increased prolonging the lifetime of the network. The individual nodes are given more security, adding security to nodes will consume more energy thus reducing the lifetime of the network. If the nodes are solar aware, the energy level gets equalised and also surplus energy may be obtained because of usage of LEACH protocol. The proposed protocols are made to detect and prevent the attacks thus controlling the overhead, increasing packets delivered and extending the lifetime of the wireless sensor networks.

Key words: Wireless sensor networks, LEACH, worm hole attacks, black hole attacks, secured LEACH, network density, PDR

INTRODUCTION

WSN has unique benefits with low power, low latency and versatile in the human unattended locations. WSNs are deployed in large numbers (hundreds or thousands of integrated sensor nodes) to collect data from observed environment. The mission of sensor networks is to occasionally assemble information from a remote landscape where every node ceaselessly faculties the earth and sends back the information to the Base Station (BS) for further examination; the BS is normally found extensively a long way from the objective territory. The most prohibitive element in the lifetime of wireless sensor network is restricted energy asset of the sent sensor nodes. Since, the sensor nodes convey restricted and for the most part fundamental force source, the protocols intended for the wireless sensor networks must take the issue of energy productivity into thought. Additionally, the network convention ought to deal with different issues, for example, self-setup, adaptation to internal failure. Another essential measure in the configuration of a sensor network is information conveyance time since it is basic in numerous applications including war zone and medicinal/security observing framework (Chengfa *et al*., 2005; Heinzelman *et al*., 2000). Such applications require getting the information from sensor nodes inside of some time limit. Correspondence protocols exceedingly influence the execution of wireless sensor networks by an equitably dispersion of energy load and diminishing their energy consumption and immediately drawing out their lifetime (Hady *et al*., 2013).

In this manner, outlining energy efficient protocols is crucial for drawing out the lifetime of wireless sensor networks. Since, the nodes are abundant in number it is difficult to recharge the batteries. Therefore, extending the lifetime of the nodes is the primary concern. The end goal to improve the system life time by the time of a specific mission, numerous routing protocols has been formulated. Those protocols can be ordered into two classes: level routing and hierarchical routing (Wen and Sethares, 2005). Especially, the clustering protocols can fundamentally reduce vitality utilization by accumulating multiple sensed information to be transmitted to the destination node. Data gathering can be utilized for diminishing vitality utilization (Saeidmanesh *et al*., 2009). In the Gracefully

Corresponding Author: R.M. Dilip Charaan, Department of Electrical and Electronics Engineering, College of Engineering, Anna University, 25 Chennai, India

Degraded Data Aggregation (GDDA) scheme false data from the overall sensed data can be detected and eliminated (Gopi and Karthik, 2013). After data gathering the data collected from the nodes can be checked for redundant data. If there is any redundant data or false data it can be removed using this technique.

Data aggregation: Data aggregation is known as data fusion where the multiple packets received from different sensor nodes are combined. The data packet size is eliminated by reducing the redundant data. Due to this the wireless communication cost is also decreased. Thus, the clustering protocols improve the energy consumption and the lifetime of the WSNs. While using the clustering algorithms there are two kinds of nodes CH and nCH. The sensor nodes are organized such a way that the clusters are formed with a single CH and many nCH. The nCH nodes transmit the collected data to the CH after aggregating the data. The CH in turn routes all the data to remote sink node or the processing node (Karaki *et al*., 2004).

LEACH (Low Energy Adaptive Clustering Hierarchy): LEACH (Low Energy Adaptive Clustering Hierarchy) is the most famous and ordinary cluster based hierarchical directing convention which is by and large acknowledged in every one of its repercussions and its significance can't be overemphasized. LEACH however mainstream and strong has not yet accomplished flawlessness. Upgrades can be performed considering any of the accompanying parameters cluster head selection plan, group development algorithms, decreasing energy overheads, thinking about residual energy and so on which intend to expand the proficiency and heartiness of LEACH (Heinzelman *et al*., 2000).

LEACH is one critical understood hierarchical clustering protocol. The operation of LEACH is separated into rounds where each and every round starts by means of a set-up phase, when the clusters are composed, trailed by a steady state phase, at the point when information exchanges to the base station happen. At first, each node picks an irregular number something around 0 and 1. In the event that the number is not exactly a limit, the node turns into a CH for the current round. Cluster head for the current round shows a promotion message to whatever is left of the nodes. The non-CH nodes must keep their collectors on amid this phase of set-up to hear the promotions of all the CH nodes and chooses the cluster to which it will have a place for this round. The cluster head node makes a TDMA plan telling every node when it can transmit and show back to the nodes in the cluster. Once the groups are made and the TDMA plans settled, information gets transmitted (Heinzelman *et al*., 2000).

Need for leach and connecting solar panel: Every node should be made a Cluster Head (CH), the probability of every node to be a CH is equal. In order to achieve this state a proper routing algorithm should be chosen. In the LEACH protocol all the node members are given importance and are given priority to become a cluster head. Hence, the wireless system acts fairly and gently.

The method adopted should have high efficiency and should select a cluster periodically. The network should be efficient in the sense it should have battery backup. To add the energy level to nodes, solar panel is included and this adds energy level to the residual energy. The sensor network obtained is of high efficiency:

$$\text{Energy}_{\text{avg}} = \sum_{1}^{n} \text{Energy}(i)$$

where, i→1-n. The Energy$_{\text{avg}}$ is always found to be in close proximity to the threshold limit. The Energy$_{\text{threshold}}$ is set with first energy average obtained during the start of the transmission. After that average energy is frequently observed for every round. This continues for all the p rounds. As the number of rounds increases the node death rate increases. After p/2 rounds are over, around one fifth of the nodes are found dead only remaining four fifth of the nodes are found to be thriving. Many nodes may lose its energy soon after few more rounds are over. This will decrease the number of packets delivered increasing the end to end delay. In order to increase the threshold energy, average energy and maintain the energy level in all the nodes of the network. All the nodes of the network are made solar aware by connecting a solar panel to the sensor nodes. If such a setup is made all the nodes will have enough energy to operate. Since, the protocol in this sensor network is LEACH, all the nodes with high energy are made a cluster head. This rule gives equal chance for all the nodes to become a CH for each different round. Also, considering that there are p rounds and in these p rounds every node from 1 till p becomes the CH. If a node x becomes the CH for the first cycle it will take p more rounds to become the cluster head again. Mean while the node gets ample number of time to recharge its battery with the solar energy. The full amount of energy (total energy) in the sensor node is given by Energy$_{\text{tot}}$. The total energy in the sensor node is given by Energy remaining in the node after heat loss and natural loss from which the energy gets depleted after working as a cluster head and also as a non cluster head and finally the energy that is stored from the solar panel:

$$\text{Energy}_{\text{tot}} = \text{Energy}_{\text{residual}} - \text{Energy}_{\text{transceive}} + \text{Energy}_{\text{solar}}$$

If all the nodes are made solar aware the performance increases, thus increasing the number of packets delivered, packet delivery ratio, reduces end to end delay, control overhead. Even if a security is maintained for all the nodes the energy gets depleted rapidly but making a node solar aware makes the sensor node to operate smoothly. Adding a solar panel to all the nodes is definitely a benefit in many ways.

MATERIALS AND METHODS

Intrusion detection: Intrusion detection is the procedure of observing abnormalities on the system, distinguishing the attack of any adversary node and confirming whether abnormalities are a consequence of intrusions and reacting with proper counter measures. Wireless sensor networks are susceptible to different attacks and intrusions. This increases the networks vitality consumption and memory (Perrig *et al*., 2004). The current secure conventions or intrusion detection schemes are typically proposed for one convention layer. The one ought to be named an abnormality is absolutely application-specific. A sensor node can perceive a few inconsistencies as intrusions all alone, e.g., whether it is stuck, yet for some different irregularities such as whether it is being focused with Sybil attacks (misguided character), it needs to correspond with its neighbours. However, there are chances that even some of its neighbours themselves might be gate crasher; a few reputation-based schemes have been proposed. In these schemes, a node rates the reputation of a neighbour based on whether the neighbour is 'agreeable'. A node's capacity to assess helpfulness is however flawed. For sample, only accepting information from its neighbour does not infer that the neighbour is coordinating if the information is false. The node might counsel different neighbours on the legitimacy of the information, yet relying upon what quality is measured, alternate neighbours could conceivably have the capacity to substantiate the information's legitimacy (Gupte and Singhal, 2003).

However, this methodology is vitality devouring, it's better to relegate the occupation of approving information to a protected aggregator. Reputation-based schemes does not play a crucial part in the security of WSNs, various intrusion reactions are relevant to different layers (Younis *et al*., 2002).

Detection of attacks in leach protocol: The CH sends a nonce along with advertising message during the setup phase. The node which is chosen as the cluster head will receive the interest to join from the nCH nodes after joining the CH the nCH has to get their keys from the base station via their Chs. In the second round when the set up phase starts each node has to send their interest to join along with their old key. In turn the new CH collects the keys from their cluster nodes and sends to the base station. If the number of nodes and number of keys are the same as the previous cycle no new intruder is inside the WSN. If there is redundant data there is node replication attack. If the key and the node ID are different then there is a intruder.

After every p/2 rounds the nodes are made to communicate with each other. The CH node in each cluster sends a hello message to the left neighbour nodes. Finally the number of nodes and the availability of the nodes along with their information like energy level are reported to the CH. After collecting the complete details of the nCH, all the CH sends their node information to the BS. So that, the number of nodes that have failed and the battery level of the nodes are determined in advance.

Security attacks in WSN: The one that compromises a system in order to gather information illegally affecting the system is called a security attack. The attacks are classified into two categories passive attacks and active attacks.

Passive attacks: Passive attacks are those attacks in which an attacker does not actively participate in making the network collapse. In a passive attack the intruder comes to know about the information and may use the information from the network. Finally the intruder makes the network down.

Active attacks: Active attacks are those attacks in which the attacker actively participates in the disruption the network. Here the packets get dropped; packets are modified, fabricating messages. The node finally steals the information and instantly changes the data in any form (David and Scott, 2008). DOS can be unintentional or intentional in which the nodes fails or of malicious action. DOS attack is also exhausts the system by sending unnecessary data and prevents the legitimate nodes from accessing resources. DOS attacks diminishes the capacity to provide a service also they subvert and destroy the whole network (Wood and Stankovic, 2002). To prevent DOS attack it needs pushback, strong authentication, network traffic review. As the nodes have a wireless connection and infrastructure fewer environments these WSNs are vulnerable to different security attacks. Worm hole is a very harmful active attack.

Blackhole attack: A black hole attack is an attack that is foe on a subset of the sensor nodes in the system. The rival captures these nodes and re-programs them with the goal that they don't transmit any information clusters to be specific in the pack expected to forward. Wireless Sensor Networks (WSNs) have numerous attacks from which black hole is one of them (Younis *et al*., 2002).

In this attack, a malevolent node advertises an absurd path as good path to the source node when the node searches for path. The good path is the shortest path routing created from source node to the destination node. This node can also be a stable path in the sensor network. A black hole has two properties, firstly the intruder node exploits the whole system. In this attack the node advertises itself as a valid node and has a legitimate route to the destination node. These black hole node's intention is to intercept packets. At the point when the source node selects the way including the attacker node, the traffic begins going through the adversary node and this nodes begins dropping the packets specifically or in whole. Here, these re-modified nodes are termed as black hole nodes. Once a black hole region is detected it is the mother of all the attacks giving way too many other attacks. This algorithm 1 is used to detect for the black hole attack with the packets transmitted and the received packets for n nodes in each cluster.

Black hole attack detection

Algorithm 1 (To detect black hole attack):

```
All the nodes that are receiving more packets are detected.
for ($NODE_i$ = 1; $NODE_i$< = n; NODE++)
Consider the node i transmits data to a neighbour j and then k and so on
if ($NODE_i$ forwards to $NODE_j$) here j = i+1 always j = Cluster Head, i = member node
then
i transmits x bit information j receives x bit information.
NODEj transmits 0 bit information
$NODE_i$ is a black hole attacker.
else
$NODE_j$ is not a black hole attacker node.
End if
End for
```

In a black hole attack the source transmits x packets but the destination receives 0 packets transmitting packets = x, receiving packets = 0:

$$\text{Packets Delivered (PD)} = \frac{\sum \text{Transmitting packet}}{\sum \text{Receiving packets}} = \infty$$

In this algorithm, the intruder is detected with the response after receiving the data with their threshold waiting time.

Detecting an intruder (black hole)

Algorithm 2 (detecting a intruder (black hole)):

```
In nodes where delivery fails for( i-n)
if (data-Arrived == 1)
then
no intruder or threat
else if (no arrival response data)
then
if(wait time >= Threshold waiting time)
then
node failure
else
wait for response
else if (no data arrival)
then
Intruder node detected (black hole attack)
else
wait for response
end if
```

Wormhole attacks: A wormhole attack can be used as a base for eavesdropping not forwarding packets in a DOS like fashion, may alter information in packets before forwarding them. Wormhole attack is quite server and records traffic from one region if the network and replaying them in different region. The attacker receives packets at one point in the network, forwards through a wireless link which is with less latency and they relay them to another location in the network.

Considering a node X located inside the transmission range of legitimate nodes A and B being an intruder. A and B are within a transmission range of each other. Intruder node X just tunnels control traffic between A and B without stating its address as the source in the packet header. So, X is virtual node invisible in the network. X afterwards drop tunnelled packets or break the link. The wormhole attack is very difficult to detect. It is effective in a network where confidentiality, integrity, authentication are preserved (Younis *et al*., 2002).

Detecting wormhole attacks

Algorithm 3 (to detect wormhole attacks):

```
IF(Transmitted mesg==1)
Delivered mesg == 0
Node Failure or Attack Detected.
IF ( Delivered mesg == 1 after time $T_n$ = T+T(x)
Delay (node failure or due to overhead)
Else
Attack detected.
IF (Transmitted mesg = n)
Delivered Message = m after time delay $T_n$ = T+T(x)
Expected node to deliver = $\alpha$
Node delivered = $\Omega$
Wormhole attack detected.
End if
```

Prevention of wormhole attacks: The wormhole is controlled by an attacker in between two different locations in the network. Malicious nodes or the intruder node may interfere in the communication that is taking place in between the cluster heads and later attracts the traffic. In the wormhole attacks the information from a legitimate node is obtained by a malicious wormhole node tunnels the packets through a low latency path and transmits in some other part of the network. The transmitted information can be modified or replayed or transmitted as such. In a network where a information that is transmitted from the source to the destination, starting from the source the before reaching the destination the data hops many times and finally reaches the destination. In this case the attacker may sit beside any of the node and absorb the data and tunnels them to a very long distance. Since, the technique followed is cluster based approach, LEACH protocol is utilised. In the LEACH protocol the group of nodes are split into many clusters based on their signal strength and distance. Among the nodes in a network, one with more energy than and one interested to be an organiser is elected as the CH node. The operation of the networks is as follows, member nodes send the data to the cluster head and the cluster head in turn sends an acknowledgement to the member nodes. Finally, the cluster head sends the data to the base station and then to the destination. The conclusion is that base station and the cluster head are the ones that are vulnerable to attacks.

In this technique the CH is elected frequently and the destination nodes also change continuously. If the CH and the BS are protected the network operates without vulnerability. Multiple BS is employed in the proposed system and new CH is elected after every round. In the proposed system four base stations are utilised. This measure reduces the possibilities of attacks to a greater extent. The base station for each round is selected randomly. The BS before receiving the information enquires the distance from which the data has come in that single hop. With the previous information and the obtained information the BS checks for gentility. If both are same the nodes are not vulnerable. Also, it is made default that all the nodes before receiving a message checks for its distance. The nodes are also provided key to completely eliminate the wormhole attack.

Preventing black hole and wormhole attack in leach for wsn (Secured LEACH) using key: The protocol we use is the LEACH protocol this gets spilt into many clusters and each cluster has one Cluster Head (CH) and many non Cluster Head (nCH).These nCH are the nodes that may become a CH in the next round. In the LEACH protocol all the nCH nodes send the collected information to the CH. The main task of the CH is to gather information or in other words the CH aggregates the data and after collecting handful information it sends to the CH. The CH then transmits the information to the base station and then the BS transmits to the destination. Here the CH and the BS are nodes where the information is available completely. So, these are the nodes that are liable to attacks. If the attacker compromises these nodes it can attack the target easily.

To avoid this and handle the situation properly an extra bit is added to the transmitting message after each cycle. In order to make a check for a attack the base station sends a one bit message to all the nodes also to the CH. During communication all the nodes share a single bit key. All the nodes are not given the same key.

While distributing the key say in a cluster half of the nodes are given a key and other half of the nodes are given some other key. Totally the BS has two different keys for a cluster. When the CH node is ready to gather data, the nodes before sending data gets the key and along with its own key checks if they are same or not, depending upon the instant information (whether the keys are equal or not) got from the BS. Here the base station gives a instant message before gathering the information whether the keys are same or different. If two nodes have the same key but the CH gives unequal key then the CH is reported as an illegitimate node. If the CH has been hacked it cannot guess the keys of the all the nodes. Hence the CH that is illegitimate can be easily detected. This kind of key generation can withstand for the communication between nCH nodes and the different CH. Here a third party is included to monitor the BS. Considering that in our sensor system we have multiple BS. At a time period the entire BS sends security packets among them and requests for the previous cycle security packet key. If the BS fails to send the new and old keys they can be a illegitimate node. The old key is the key that is utilised in the previous cycle (p-1) and the new key is the key obtained for the present cycle (p). The base station can be declared a haunted one and can be excluded from the network and the communication takes place with the remaining base stations. Then, the affected base station is assessed and removed from the group:

$$\Pi = [BS_1, BS_2, BS_3, BS_4], i \rightarrow 1\text{-}4$$

Say, one of the base station is found to be malevolent (BS_3 is considered to be malicious). Then to remove the affected base station:

$$\Pi_{new} = \Pi - \Pi$$

where, ith node is the malicious node. Now the new base stations are:

$$\Pi_{new} = [BS_1, BS_2, BS_4]$$

This makes the network from free of attackers. So, each and every time the check process is done. It is made sure that the nodes are legitimate and also the base stations are free of attacks.

RESULTS AND DISCUSSION

The simulation was performed in network simulator 2 and the results are shown below, the sensor area considered is 200×200 wide areas. The number of total number of nodes is 500 and all the nodes are made solar aware, the base station is four in numbers and are placed r metres from the centre. The distance between two base stations is 2r m and the remaining simulation parameter is as follows (Table 1 and 2).

Simulation parameters

Energy in nodes: Table 1 and 2 shows the amount of energy available after p rounds in the network. The energy in the load node and destination node are found to be higher in the secured LEACH whereas the traditional LEACH without any intruder has comparatively less energy and the LEACH protocol utilised system which has a intruder or the attacker in the sensor network has very less energy. Here in this case sometimes the PDR may become zero.

Packet Delivery Ratio (PDR): The ratio between the received data packets to the data packets forwarded from the source node. Figure 1 shows the received packets to the transmitted packets. Figure 2 shows the Number of alive nodes vs time. The performance of the Secured LEACH is very high when compared to the LEACH protocol. As the nodes are made solar ware and security is added the number of dead nodes decreases increases the PDR and controls overhead.

Network density: The network density is plotted across the Packet Delivery Ratio (PDR). In the secured LEACH the number of packets delivered is high as the number of nodes increases. This graph is demonstrated below in the Fig. 3 explains the Packet Delivery Ratio (PDR). Against time. The performance of the Secured LEACH is much better than the traditional LEACH. Packet Delivery Ratio (PDR) is the ratio between numbers of packets delivered to the numbers of packets transmitted (Fig. 4 and 5).

PDR vs. time: The graph below is drawn across energy vs. time for the secured LEACH. This energy is the energy obtained after using a solar panel or in other words the energy obtained from the sensor nodes after making the nodes solar aware. The energy value reduces gradually after tiresome tasks at the sensor network. This is mere energy obtained from solar panel in addition to this there is battery energy available in the battery.

Table 1: Simulation parameters

Variables	Values
Simulation area	200×200
Nodes in number	200
Size of each packet	4000 bits
Energy in each node	4 J
Cluster head proportion	p = 8%
No of base station	4
Number of nodes with solar panel connected	100%

Table 2: Energy in nodes

Name of the node	Traditional LEACH	LEACH sans security	Secured LEACH
Load node	79	60	88
Destination node	81	66	84

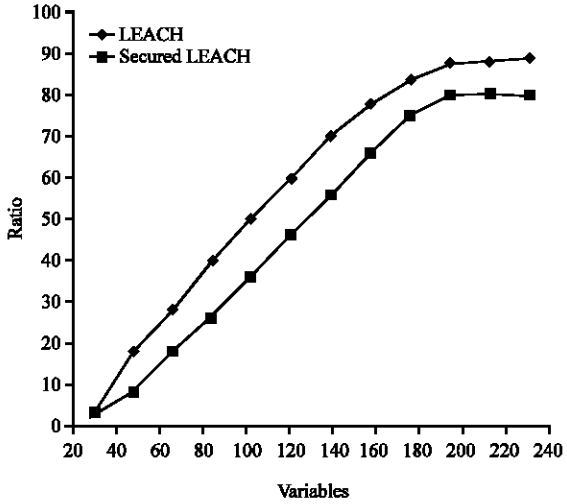

Fig. 1: Packet delivery ratio

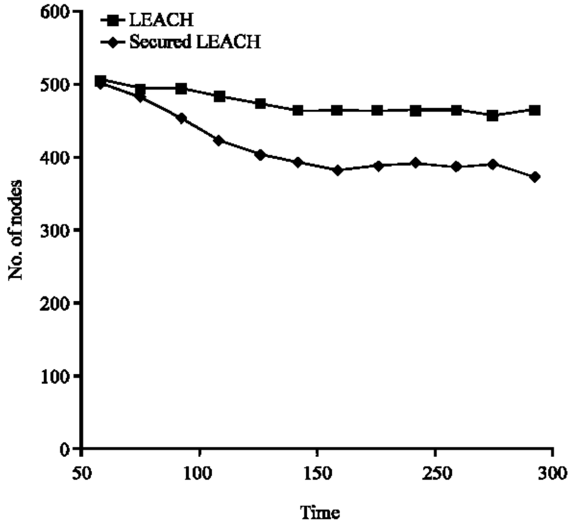

Fig. 2: Node alive rate

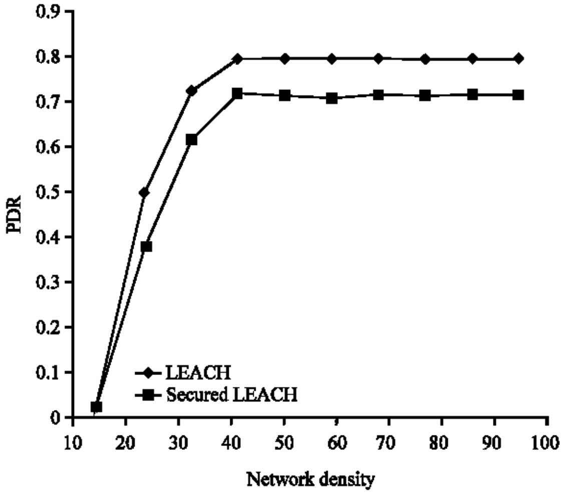

Fig. 3: Packet Delivery Ratio (PDR) vs. network density

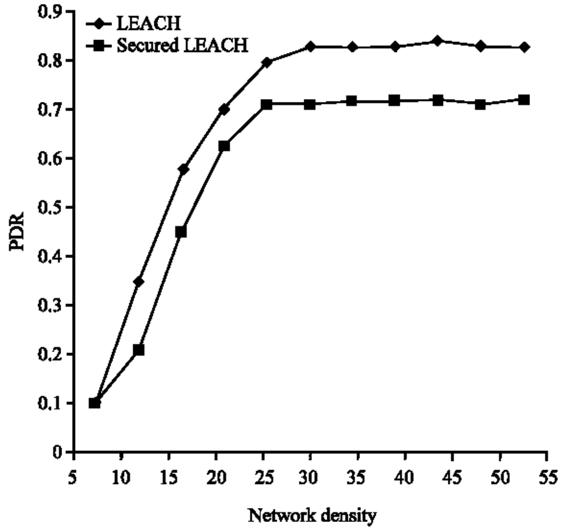

Fig. 4: Solar energy vs. time

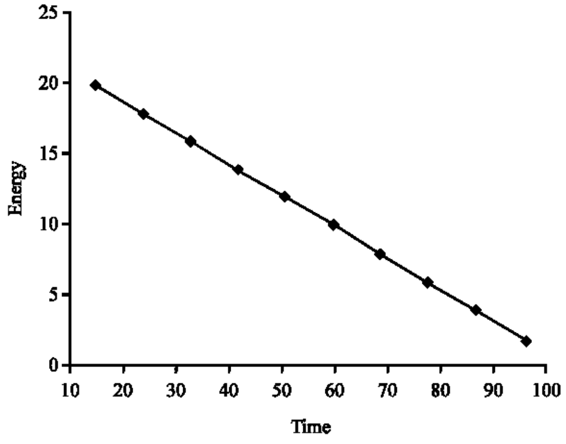

Fig. 5: Solar energy vs. time

CONCLUSION

The vast majority of the attacks against security in wireless sensor networks are brought on by the insertion of false data by the bargained nodes inside of the network. For guarding the incorporation of false reports by traded off nodes, a method is required for identifying false reports. Be that as it may, growing such a location instrument and making it productive speaks to a awesome exploration challenge. Once more, guaranteeing holistic security in wireless sensor network is a noteworthy exploration issue. A large number of today's proposed security plans depend on particular network models. As there is an absence of joined push to take a basic model to guarantee security for every layer in future despite the fact that the security instruments turn out to be settled for every individual layer, joining every one of the instruments together for making them work as a team with one another will bring about a hard research challenge. Regardless of the possibility that holistic security could be guaranteed for wireless sensor arranges, the cost-adequacy, vitality effectiveness to utilize such components could even now posture extraordinary exploration challenge in the coming days.

REFERENCES

Chengfa, L., Y. Mao, C. Guihai and W. Jie, 2005. An energy-efficient unequal clustering mechanism for wireless sensor networks. Proceedings of the International Conference on Mobile Adhoc and Sensor Systems Conference, November 7, 2005, Washington, DC., pp: 599-604.

David, R.R. and F.M. Scott, 2008. Denial of multihop performance. IEEE. Pervasive Comput., 7: 74-81.

Gopi, A. and S. Karthik, 2013. A secure and fault tolerant routing protocol based on GDDA and HLUA. Asian J. Inf. Technol., 12: 208-216.

Gupte, S. and M. Singhal, 2003. Secure routing in mobile wireless ad hoc networks. Ad. Hoc. Networks, 1: 151-174.

Hady, A.A., E.S.M.A. Kader and H.S. Eissa, 2013. Intelligent sleeping mechanism for wireless sensor networks. Egypt. Inf. J., 14: 109-115.

Heinzelman, W.R., A. Chandrakasan and H. Balakrishnan, 2000. Energy-efficient communication protocol for wireless microsensor networks. Proceedings of the 33rd Annual Hawaii international conference on System Sciences, January 7-7, 2000, IEEE, Massachusetts, USA., ISBN: 0-7695-0493-0, pp: 3005-3014.

Karaki, A.J.N., U.R. Mustafa and A.E. Kamal, 2004. Data aggregation in wireless sensor networks-exact and approximate algorithms. Proceedings of the 2004 Workshop on High Performance Switching and Routing, April 19-21, 2004, IEEE, Iowa, USA., ISBN: 0-7803-8375-3, pp: 241-245.

Perrig, A., J. Stankovic and D. Wagner, 2004. Security in wireless sensor networks. Commun. ACM, 47: 53-57.

Saeidmanesh, M., M. Hajimohammadi and A. Movaghar, 2009. Energy and distance based clustering: An energy efficient clustering method for wireless sensor networks. World Acad. Sci. Eng. Technol., 55: 555-559.

Wen, C.Y. and W.A. Sethares, 2005. Automatic decentralized clustering for wireless sensor networks. EURASIP. J. Wireless Commun. Networking, 2005: 686-697.

Wood, A.D. and J.A. Stankovic, 2002. Denial of service in sensor networks. IEEE Comput. Mag., 35: 54-62.

Younis, M., M. Youssef and K. Arisha, 2002. Energy-aware routing in cluster-based sensor networks. Proceedings of the 10th IEEE International Symposium on Modeling, Analysis and Simulation of Computer and Telecommunications Systems, October 16, 2002, Fort Worth, TX., USA., pp: 129-136.