ISSN 2347 - 3983

International Journal of Emerging Trends in Engineering Research (IJETER), Vol. 3 No.6, Pages : 27 – 31 (2015)
Special Issue of NCTET 2K15 - Held on June 13, 2015 in SV College of Engineering, Tirupati
http://warse.org/IJETER/static/pdf/Issue/NCTET2015sp06.pdf

AN ALTERNATIVE SECURED AND EFFICIENT ROUTING STRATEGY FOR WIRELESS SENSOR NETWORKS

B.Sireesha[1], G.TagoreSai Prasad[2]
[1]M.Tech CSE Student, S.V.Engineering College for Women, Tirupati, AP, India
Sireesha209@gmail.com
[2]Assistant Professor, Dept. of CSE, S.V.Engineering College for Women, Tirupati, AP, India,
gtsprasad@gmail.com

ABSTRACT

Efficient protection against security attacks is an important task in the wireless sensor network location. Even ifmost important research has been done on the design to identifythe malicious nodes based on uninterrupted and interrupted evidence, this createsextra energy consumption based on of its cost. The position createsgreat problem to the next generation of wireless sensor network will be more and more.To solve this problem, we propose a secured and efficient routing strategy which implements the adjacent node routing principle be able todo with the network extents and depend on a distributed trust model for the finding the malicious nodes. Both interrupted and uninterrupted trust information is engaged and it can calculate the trustworthiness of each adjacent node. An important character of the secured routing strategy is which calculates the left over energy of every adjacent node, soit achieves for good load balancing and improves network lifetime. According to the theoretical results we calculate theextra energy depletionmake happen by the changing of interrupted trust data. Our algorithm reduces of energy wastage and improves security .

Key Words: Energy Balance,Routing , Security,WSN.

1.INTRODUCTION

The modern technological improvements make wireless sensor network (WSNs) technically and economicallyreasonable to be extensively used in both military and civilian applications, such as observing of ambient circumstances related to the environment, expensive species and critical infrastructures. A key feature of such networks is that each network contains large number of untied and unattended sensor nodes. These nodes often have very limited and non- replenishable energy resources, which makes energy an important design issue for these networks.

Routing is the important design concern for WSN.A well designed routing protocol provides less energy depletion for message delivery and have the good message delivery ratio.To increase the Sensor network lifetime and also manage total sensor network energy depletion.

Wireless Sensor Networks have the solutions which maintains extensive range of applications. Based on the application, their WSN environment is the risky, challenging and fewerproblematic. Even the Encoded Security Systems in WSNs not to notice the node physical internment, the **malicious** or selfish nodes. So, novel security systems isessential for the secure routing of message from source to sink node of WSNs. A novelmethod of getting security without using cryptography is Trustbased security in WSNs. Trust is “The mark of Trustworthiness”.It captures the nodes information and collect all record about the node.it can also check the of other node in doing actions and can be formed by keeping a details of the communications with the other nodes directly as well as indirectly. By using these details a trust value will be find out. To maintain the decision making processes of the network in wireless sensor network Trust management will be used. Thesehelps to the removal of the unsecured nodes in the WSN about the coming actions of other nodes (trustees).

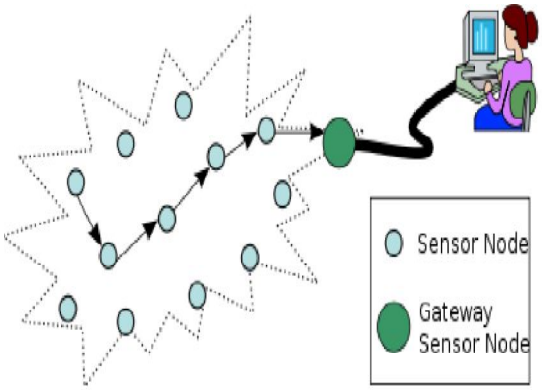

Figure 1:Wireless Sensor Networks

Several examines on trust associated in WSN are done, but it is vital to design and develop a trust management system which uses the a lesser amount of resources of the node in valuation and management of faithbetween/among the nodes. The trust management of the WSN would be a simple.It not have the limitations on energy consumption, software,

ISSN 2347 - 3983

International Journal of Emerging Trends in Engineering Research (IJETER), Vol. 3 No.6, Pages : 27 – 31 (2015)

Special Issue of NCTET 2K15 - Held on June 13, 2015 in SV College of Engineering, Tirupati

http://warse.org/IJETER/static/pdf/Issue/NCTET2015sp06.pdf

hardware, memory usage, computing, processing speed and communication bandwidth, and it identify various attacks easily, and mange and change trust relations based on it.

Routing is a interesting task in WSNs because of the limited resources. Geographic routing was largely observed as is theimportant way for WSNs. Geographic routing protocols uses the relative positiondetails and send the packets one after another from the source node to the sink node[1].Based on the direction or distance the source node selects the next adjacent node and send the message.By using signal strength or using Gps receivers are find the tototal distance between adjacent nodes [2].The details about the nearer one of next nodes can be exchanged between adjacent nodes.

In a little power GPS receivers are used in the sensor networks through thegeographic adaptive fidelity (GAF) routing scheme. In GAF, the network area is separated into constant size ofgrids.The single node is in active state remaining all nodes are in sleep state to decrease the energy consumption.The sensor sends the messages based on greedy geographic routing strategy.

A query based geographic and energy aware routing (GEAR) was proposed in [3]. In GEAR, the destination node propagates requests with relative attributes to the objectiveregion because not to fall on problems of flooding.Each node sends messages to the relative nodes based on assessed cost and learning cost. The assessed cost studiesthe distance to the destination and left over energy of nodes in sensor networks.The learning cost gives the changing information to suffer with the local minimum problem.

Lifetime plays a key role and also major issuein Wireless sensor networks.In a secure and routing strategy was got the shortest way.Always selecting and calculating the lowest energy level node and the way is reduced by the secured routing strategy in the wireless sensor networks.AODV or directed diffusion is also a reactive protocol to route multiple paths as the secure routing stategy. Then, the routing strategy can select a route based on a probabilistic method according to the remaining energy. In the transmitter power level can be adjusted according to the distance between the transmitter and the receiver.

Routing was communicated as a linear programming problem of adjacent node choice to make best use of the network lifetime. Then examined the uneven energy consumption for consistentlyarranged data-assembly sensor networks.The network is divided into manyregions and each node can make data aggregation. In routing strategy was proposed to stabilize the energy consumption between the nodes within each grid.in [formulated the combined way of finding the routes and the traffic load allocation, and the network lifetime values increases by thesleep scheduling. By using this the concept of opportunistic routing, [4] developed a routing metric to report both link reliability and node remaining energy.The sensor node calculates the best metric value in a localized area to attain both reliability and lifetime maximization.

2.CASER PROTOCOL

WSNs routing is frequently geography based, a geography-based secure and efficient Cost-Aware Secure routing (CASER) protocol for WSNs without any effect on traffic in te network. The protocol agrees messages to be communicated using the secure routing ways, unsystematic way and deterministic routing,based on the correctness. The sharing of these two strategies is resolute by the definite security requirements. This strategy issimilar to distributing US Mail through USPS: send mails cost more than regular mails; however, mails can be send fastly and it gives deliver report. The protocol gives a safety and privacy message transmissionchoice to improve the message delivery ratio by the various and different attacks.

These protocol has two mainbenefits:

1.It improves the lifetime of total sensors in the grid and decrease the wastage of energy.

2.This protocol helps various routing schemes based on the routing requirements.It checks whether the message delivering is good or not and also this protocol can reduce the various attacks like traceback attacks ,jamming and etc[7] in WSNs.

Main strategies of this paper can be précised as follows:

1)A secure and efficient Cost-Aware Secure Routing (CASER) protocol for WSNs. In this protocol, routing strategies can be useful to maintains the message delivery requirements.

2)A quantitative scheme maintains the energy depletionthen the sensor network lifetime and the total number of messages that can be delivered are improved under the same energy usage.

3)Developed theoretical formulas to assessment the sum of routing hops in protocol based on changing routing energy balance control and security requirements.

4) To examine security of the routing algorithm.

5)Providedan optimal non-uniform energy deployment strategy for the given sensor networks based on the energy depletion ratio.

3.SECURE AND EFFICIENT ROUTING STRATEGY

The proposed Secure and Efficient Routing (SESR) Strategy uses the relative node approach. The SERS is used relative location for routing.Otherwise to calculate the number of hops to reduce flooding and various attacks. This strategy is good to detect routing attacks and gives the efficient support of wide sensor networks. Relative location sending is essentially protected which opposes on various attacks to sending the message calculation, have the more preference for secure

ISSN 2347 - 3983

International Journal of Emerging Trends in Engineering Research (IJETER), Vol. 3 No.6, Pages : 27 – 31 (2015)
Special Issue of NCTET 2K15 - Held on June 13, 2015 in SV College of Engineering, Tirupati
http://warse.org/IJETER/static/pdf/Issue/NCTET2015sp06.pdf

routingit is node ID and attributes. And also above characteristics are same for all relative location routing strategies such as the Greedy Perimeter Stateless Routing (GPSR).SESR includes the next adjacent node selectionIt gives the location of a node, low energy usage and trust or secure message routing.Energy managing is important for reducing all the attacks with high trust calculated value.Thelimiting factor is observed by the nodes energy and routing trust calculated value will be reduced i.e. the chance to complete all the total work.Due to the calculation, we have merged the energy calculations in the total trust value a node computes all of theiradjacent nodes. Energy management allows load balancing. It plays very crucial to reduce the traffic analysis attacks and increase the network lifevalue.The SERS architecture which is Secure and Efficient Routing Strategy is shown in Figure 2**.**In the SERS each and every time an event performed based on the direct trust metrics (packet forwarding, network Acknowledgement) occurs, the consistentresults placed in the Direct Trust table or uninterrupted trust table are updated. At the same, each time reputation response messages are taken, their information is placed in the indirect trust table or uninterrupted Trust table after the checkings. Both tables have information for each adjacent node. The entire node's trust value is calculated when a new message has to be sended, even though the trust values and reputation data is updated each and every time an event has got or an reputation response message has been taken. This event-driven scheme was adopted to balance the energy and also maintaining the resources. It calculates both interrupted and interrupted trust and it takes as a total trust value and it considers the distance of adjacent nodes. The final value calculated and conforms whether the node sends the information or not.

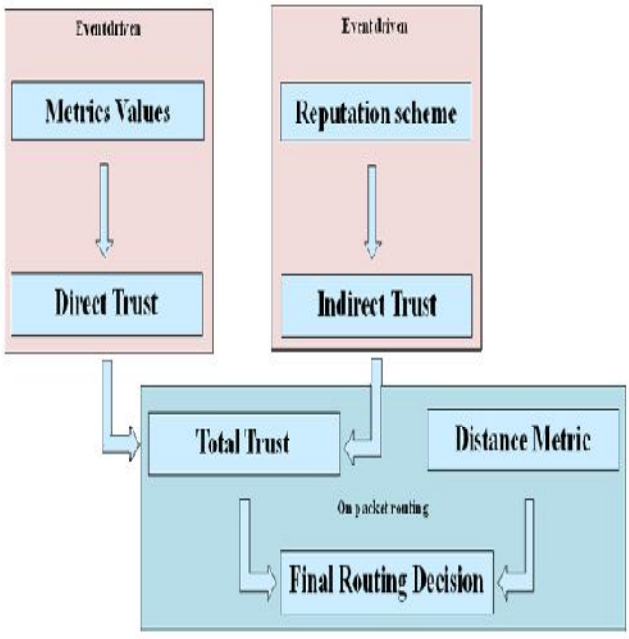

Figure 2:SERS Architecture

4.SERS FOR IDENTIFYING AND AVOIDS THE MALICIIOUS NODES

To assess the effectiveness of the secured and Efficient routing strategy of the attendance of problematic nodes, first to compare the strategy with the totally malicious nodes place is implemented in that the relative location node routing is prepared. connection is jammed when it have malicious nodes on that effective SERS strategy the malicious nodes will be removed and stopped. The Trust of any node is assessed by using the geometric mean of trust metrics of the node (uninterrupted trust), and total mean of data created on all the adjacent (neighbor) nodes. The node's information given by adjacent nodes (interrupted trust) is the direct trusts with the node. All the nodes in the network ,have to keep a database list i.e, what they are doing for every of its adjacent node. This database listenclosesthe details about the various trust values, i.e. Quality Of Service etc are the features for all its adjacent nodes based on the how many times their attempts performed in the network. This trust values information have to use for computing the Uninterrupted trust of its each adjacent node.
To calculate the distance of the adjacent node information to the work station, the related calculations joined in the routing function is done as below:

$$T_d^{A,B} = 1 - \frac{d_i}{\sum d_i}$$

Where *di* is the distance between the adjacent node i to the work station and *Σdi* represent the distance between the adjacent nodes to the base station. The above equation gives minimum distance and improves the best value.

We have various scenarios for differ the largenumber of malicious nodes. In this, the weightsare used to the computation of the entire trust were 0.5, 0.2, 0.1, and 0.2 for the sending , network ACK, integrity and remaining energy metrics respectively. As per the weights of the routing function, W was set equal to 0.6 and W to 0.4 We have also run the same network set up using the SERS algorithm for evaluation of causes (grey-hole) nodes in the network It is clear that our protocol performs better than CASER in the presence of malicious nodes since it detects the attacks and make itdiscoveryanother paths to the destination, due to the existing trust model. The loss ratio maintains below 20% as long as the number of malicious nodes remains lower than 24% of the network nodes.
The distance to the base station and the total trust value (which has already incorporated the remaining
energy value) are add up in a weighted way and are used to calculate the Routing Function following the equation:

$$RF^{A,B} = W_d * T_d^{A,B} + W_T * T^{A,B}$$

ISSN 2347 - 3983

International Journal of Emerging Trends in Engineering Research (IJETER), Vol. 3 No.6, Pages : 27 – 31 (2015)
Special Issue of NCTET 2K15 - Held on June 13, 2015 in SV College of Engineering, Tirupati
http://warse.org/IJETER/static/pdf/Issue/NCTET2015sp06.pdf

Where *Wd*and *WT*, denotes the correct distance and trust value. The node that improves this routing function calculation is selected for sending the packet. It gives the better values and detect the malicious nodes in the network.

SERS Algorithm

The SERS algorithm can be explained below

Algorithm 1: Node A finds the adjacent node routing grid based on the given factors

Step1:Intially select a source node in the network.

Step 2:Source node can checks whether the neighboring nodes are trusted one or not based on weighting factor.

Step 3:

If the nodes are trusted. Source node can check the distance and energy levels of the neighboring node.

Step 4:

```
if(distance<x)
{
if(energy level > y) then
 {
   Send the message to the closest node in the grid.
 }
else
{
 The message can be blocked.
}
}
```

Based on the shortest distance and higher energy level information send to that node.

5.SERS ENERGYUSAGE

In the usage of SERS strategy frequentlyexamine and find correct to the energy depletion in a Wireless Sensor Network, we made a large set of attempts and scenarios. Each node in the network uses the energy sending and receiving messages and for the communications. It exchange routing and information messages and energy usage based on the place where the nodeis and the messages it creates or sends.

To calculate the problems, we are using a strategy to manage or decrease the malicious nodes in the network (the method which presented SERS strategy performs adjacent node secure strategy without any trust or energy awareness).200 nodes are divided in a 20x20 grid .Ten nodes communicate data to the station (node 99). It checks all the node have less distance and high energy level. If the high energy level is there but the distance is large it not sends the data packets.it must satisfies the threshold energy level and low distance. first it selects one node in the grid based on factors.It calculates the energy level, the energy level must less than the threshold energy level.

6.RESULTS

Alternate and efficient routing strategy is used based on shortest distance and high energy level source node and weighting factor can send messages to destination node. Distance is calculated in the weighting Factor. This routing strategy can decrease the packet dropping and increase high message delivery ratio. It calculates the shortest distance and higher energy levels. for example threshold energy level>= 40. Node D and E have the the energy level 39 and 20.Instead of having the shortest distance its not satisfy the threshold energy level.so those nodes not send the data packets.

Node satisfy the threshold energy levels and they have the good weighting factor so they send the packets from source node to destination node. Due to this SERS strategy we achieve high message delivery ratio, high performance ,reduce the energy wastage and also improves the security and reduce the attacks.

7.CONCLUSION

We presented SERS Secure Routing strategy for WSNs to improve security, balance the energy consumption and increase network lifetime. SERS Secure Routing strategy has the flexibility to maintenancethe several routing strategies in message forwarding to spread the lifetime while aggregate routing security. Both theoretical analysis and analytical results shows that SERS secure routing strategy has an tremendous routing performance in terms of energy maintainance and routing path delivery and the routing path security. We also proposed a non-uniform energy deployment scheme to improve the sensor network lifetime. Our analysis and theoretical results shows that we can improve the lifetime and the number of messages that can be delivered under the non-uniform energy deployment by more than four times by the SERS algorithm.AlsoSERS provides high security as well as high efficiency on transmitting the messages.

REFERENCES

[1] Y. Li, J. Li, J. Ren, and J. Wu, "**Providing hop-by-hop authentication and source privacy in wireless sensor networks,"** in IEEE INFOCOM 2012 Mini-Conference, Orlando, Florida, USA., March 25-30, 2012 2012.

[2] N. Bulusu, J. Heidemann, and D. Estrin, "**Gps-less low cost outdoor localization for very small devices,"** Computer science department, University of Southern California, Tech. Rep. Technical report00-729, April 2000.

[3] Y. Yu, R. Govindan, and D. Estrin, **"Geographical and energy-aware routing: A recursive data dissemination protocol for wireless sensor networks,"** UCLA Computer Science Department Technical Report, UCLACSD,May 2001.

[4] C.-C. Hung, K.-J.Lin, C.-C.Hsu, C.-F.Chou, and C.-J. Tu, "**On enhancing network-lifetime using opportunistic routing in wireless sensor networks**," in Computer Communications and Networks (ICCCN), 2010 Proceedings of 19th International Conference on, Aug. 2010, pp. 1–6.

[5] H. Zhang and H. Shen, "**Balancing energy consumption to maximize network lifetime in data-gathering sensor networks**," Parallel and Distributed Systems, IEEE Transactions on, vol. 20, no. 10, pp. 1526–1539, Oct. 2009.

[6] A. Pathan, H.-W. Lee, and C. seon Hong, "**Security in wireless sensor networks: issues and challenges**," in The 8th International Conference on Advanced Communication Technology (ICACT), vol. 2, 2006, pp. 6 pp.–1048.

[7] W. Xu, K. Ma, W. Trappe, and Y. Zhang,"**Jamming sensor networks: attack and defense strategies**,"IEEE Network, vol. 20, no. 3, pp. 41–47,2006.

[8] R. Shah and J. Rabaey, "**Energy aware routing for low energy ad hoc sensor networks," in Wireless Communications and Networking Conference**,2002. WCNC2002. 2002 IEEE, vol. 1, 17-21 March 2002, pp. 350–355 vol.1

[9] A. Pathan, H.-W. Lee, and C. seon Hong, "**Security in wireless sensor networks: issues and challenges**," in The 8th International Conference Advanced Communication Technology (ICACT), vol. 2, 2006, pp. 6pp.–1048.

[10] P. Kamat, Y. Zhang, W. Trappe, and C. Ozturk, **"Enhancing sourcelocation privacy in sensor network routing,"** ICDCS, pp. 599–608, June 2005.