Journal of Theoretical and Applied Information Technology
15th March 2017. Vol.95. No 5

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

SCTTM – SECURE CLUSTER BASED TRUSTWORTHY TOPOLOGY MANAGEMENT SCHEME FOR WIRELESS SENSOR NETWORKS

[1]T.SENTHIL, [2]DR. B. KANNAPIRAN

[1]Assistant Professor, Dept. of ECE, Kalasalingam University, India

[2]Associate Professor, Kalasalingam University, India

E-mail: [1]t.senthilklu@gmail.com

ABSTRACT

Lifetime enhancement of Wireless Sensor Networks (WSN) is the hottest research topic. As the lifeblood of network is the battery backup of sensor nodes, it is necessary to conserve the available energy. Security is another important requirement of WSN. This work addresses the two issues such as security and energy conservation by presenting a Secure Cluster based Trustworthy Topology Management (SCTTM) scheme. The target of the work is achieved by partitioning the network area into several grids, which is populated by equal number of sensor nodes. The BS reaches each and every grid for eagle eye observation and computes the trust point. The cluster leader and the working nodes are selected by taking the trust point into account. The BS is vigilant against selective forwarding, replay, snooze and impersonation attacks. Finally, the performance of SCTTM is analysed by varying working nodes to check the network lifetime and energy consumption pattern. Additionally, the attack detection rate is also measured. The experimental results prove the efficacy of SCTTM.

Keywords: *Lifetime enhancement, WSN, Topology management, Security.*

1. INTRODUCTION

A Wireless Sensor Network (WSN) possesses numerous sensor nodes that are distributed over certain geographical area. These sensor nodes are capable of sensing the geographical area, storing and manipulating the sensed data. Besides this, the sensor nodes can communicate among themselves. This quality of sensor nodes broadens the applicable areas of WSN and some of the popular applications of WSN are environment monitoring, remote healthcare monitoring, target detection and tracking and so on. Irrespective of the wider range of applications, the sensor nodes are strictly constrained to energy. The lifetime of the sensor nodes depends on the available energy backup.

The WSN can achieve its function effectively, only when the lifespan of the sensor networks is long enough. However, the performance of the WSN seriously depends on the lifetime of the sensors. As the wireless sensors are mostly scattered in remote geographical area, the sensors cannot be energized by battery recharging or replacement. Therefore, it is necessary to utilize the available energy in an efficient manner, which paves way for lifespan enhancement. There are many ways to save the energy of the sensor nodes and some of the prominent techniques are duty cycle scheduling, topology management and motion control [1-10].

Duty cycle scheduling technique maintains certain nodes in functioning state, while others are maintained in sleeping state. Topology management schemes conserve as much energy possible by organizing the sensor nodes in some means. It is believed that most of the energy is used up in node movement and thus, when the movement pattern of nodes is regularized the energy can be saved. This paper concerns to conserve energy by imposing a topology management scheme which ensures security. The proposed work inherits the properties of duty cycle management, hierarchical topology management scheme and movement control.

This paper introduces a secured topology management model which employs the techniques such as duty cycle scheduling and movement control for energy conservation. The constituent nodes of the network are stationary and thus the location coordinates of the nodes remain the same throughout the process. This idea saves considerable amount of energy, as the nodes are stationary. Besides this, the state of the

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

nodes is controlled by the cluster head. Some of the key points of this work are

- The proposed topology management model is secure against impersonation, replay, selective forwarding and snooze attacks.
- The proposed model involves no communication overhead, as the communication is held between the BS and the cluster heads only.
- The area separation supports divide and conquer methodology and is easy to maintain.
- The number of working nodes is limited and this improves the network lifetime.
- The hierarchical way of clustering conserves energy and provides high degree of organization.
- As the state of the nodes is controlled with respect to the location, the energy of the nodes is properly utilized.

The remaining sections of this paper are organized as follows. The related works with respect to the proposed model is presented in section 2. Section 3 presents the preliminaries of the work. Section 4 presents the elaboration of the proposed approach. The proposed work is evaluated with several performance measures and the experimental results are presented in section 5. Section 6 draws the concluding remarks.

2. REVIEW OF LITERATURE

Several trust based works have already been proposed for WSN. The work proposed in [11] presented a trust based routing protocol namely TARF. This protocol computes the route by taking the trust value and node's energy into account. This work safeguards the network from malicious nodes. In [12], the cluster head node is selected based on the trust model. The cluster head is chosen by probabilistic method and the nodes join the cluster head by taking the cluster head's trust value and energy. This process continues until all the nodes join the cluster head. This ends up in computational complexity and increased energy consumption.

A cluster head selection algorithm is presented in [13], which is based on trust. In this work, the trust value is computed by the neighbourhood nodes. The node with high trust value is chosen as the cluster head. In [14], an improvised version of LEACH [15] protocol, which is named as LEACH-TM is presented. This protocol selects the cluster head by trust value. This protocol is claimed to be secure. A trust based routing protocol namely TARP is presented in [16]. This protocol finds routes from nodes to the BS. This work conserves energy and provides scalability.

Motivated by the above works, this work intends to present a trust based scheme to select cluster leader and to schedule the duty of the nodes. The advantages of this work are threefold. Initially the network is partitioned into equal sized grids, which shoots up the simplicity, manageability and efficiency. The cluster leader and the working nodes are selected by the trust point, which is computed by several trust metrics. Thus, the trustworthy nodes are selected. The BS checks and observes the activities of the nodes by reaching all the grids in a regular period of time. This makes the network to be resistant against selective forwarding, replay, snooze and impersonation attacks.

3. PRELIMINARIES

The purpose of this section is to outline the basics of the proposed work such as system representation, threat pattern and the assumptions of this work.

3.1 System Representation

Initially, the network area is divided into several grids and the nodes are deployed. The sensor nodes of this work are motionless and the BS alone is mobile. The BS reaches each and every grid at certain time intervals. The nodes are clustered and the cluster head node is called as Cluster Leader (CL) node. The remaining nodes of the cluster are known as Cluster Member (CM) nodes. The CM nodes can communicate with the CL nodes alone and the CL nodes are responsible for transmitting the packets to the BS.

3.2 Threat Pattern

This part presents the basic idea about the attacker. The major goal of the attacker is to affect the normal functionality of the network and to gain some knowledge about the network. This is achieved by compromising and stealing the information from the sensor nodes. This work fights against security attacks such as impersonation, replay, selective forwarding and snooze attacks. All these attacks are explained as follows.

- Impersonation attack: In this type of attack, the attacker arrests the sensor

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

nodes and robs its data. By gaining all the confidential information, the attacker nodes imitate the identity of legitimate sensor nodes and perform unnecessary activities.

- Replay attack: Replay attack happens by forwarding the same packet repeatedly. This is to waste the energy of the sensor node, which seriously impacts over the network lifetime.
- Selective forwarding attack: This type of attack makes the nodes to forward the packets selectively. This means that the nodes do not forward all the incoming packets.
- Snooze attack: Snooze attack takes place by switching the node to sleep state, whenever it needs to forward packets. This attack may affect the entire network or a cluster of nodes alone.

All these attacks seriously affect the performance of the network and intend to reduce the network lifetime or to avoid packet forwarding. Both these activities are harmful to the normal network. Understanding the importance of security, this work considers all the aforementioned attacks and is observed to be secure against these attacks.

3.3 Assumptions

The major assumptions of the proposed work are listed below.

- The network possesses a BS with greater energy backup and is mobile.
- The CM nodes are immobile.
- All the sensor nodes of the network know its location.
- The participating nodes of the network may be either CL or CM nodes.
- The CM nodes forward the data to the CL node.
- This work divides the network region into grids.
- All the grids are loaded with equal count of sensor nodes.
- The working nodes of each grid are limited to two.

4. PROPOSED WORK

This section provides the overview of the work along with the proposed methodology in elaborate fashion.

4.1 Overview of the Work

The central theme of this work is to present a secured cluster based trustworthy topology management scheme (SCTTM). The major goals of this work are to save energy, impose security and improve the lifetime of the network. The proposed model is resistant to impersonation, replay and selective forwarding attacks. To attain the research goal, the network is initially partitioned into multiple grids. This way of network partitioning helps to focus on each network partition and thus, the nodes can be controlled and monitored effectively. After the completion of network area partitioning, the cluster leader node is selected. The main role of the cluster leader node is to manage, track and control the cluster member nodes. As the task of cluster leader node is very sensitive, the node must be reliable. The cluster leader node is selected on the basis of trust point, which is computed by taking several trust metrics into account.

The trust metrics being selected for computing the trust point are packet forwarding rate, energy level and node honesty. The cluster leader (CL) node controls the number of working nodes in each grid. The working nodes are selected on the basis of the same trust point by the Base Station (BS). This work limits the working nodes to two. For every two rounds, the BS checks the status of the CL and working nodes and recycles them. The main reason for node recycling operation is to share the load in a balanced fashion and not to overload the nodes. Suppose, if the energy of the node goes below the energy threshold within two rounds, then the nodes are immediately recycled.

The proposed scheme is impervious to impersonation attacks, as the nodes register themselves with the unique node identifier and location coordinates to the CL node. Besides this, the CL node shares the information with the BS. Thus, an adversary cannot compromise any node in the network. Selective forwarding and replay attacks are handled by checking the packet flow of the node. The proposed work combat against the snooze attack by CL nodes and BS, as it controls and decides the state of the nodes. The following sections describe the functionality of the proposed work in detail.

4.2 SCTTM's Work Principle

The major steps involved in SCTTM are network area division, selection of CL and working nodes and nodes' state management. All

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

these steps are explained in the following subsections.

4.2.1 Network area division stage

In this step, the whole network area is divided into equal sized grids. It is observed that it is easy to manage the grids rather than the whole network area. The efficiency and manageability of the work is improved, when the grids are handled separately rather than considering the entire network area. The entire network area is partitioned into equal sized grids. The nodes are equally distributed to all the available grids. The reason for equal count of nodes is to enforce uniformity. In case of random distribution of nodes, certain grids may be empty and certain others may be overcrowded. This may affect the network coverage also. In order to overcome these issues, this work distributes equal count of nodes to all the equal sized grids. This ensures that all the grids possess sensor nodes and in turn enhances the coverage also.

The count of nodes per grid depends on the total number of sensor nodes of the network. However, the number of working nodes per grid can be adjusted by setting the alteration parameter (α). The working nodes must be selected by taking the size of network area into account, as the network and grid size are mutually dependents. This stage is given more importance, as the process of clustering depends on the grid separation. Each and every grid is employed with a CL node and the remaining nodes are CM nodes. This work sets the count of working nodes as two, as the network area is considered as 100 by 100 metre square. As the clustering phase depends on the area division, the movement of nodes does not matter. Whenever a node enters a region, it joins a cluster. Thus, the mobility of nodes does not affect the clustering operation. However, this work sets the nodes as immobile and thus the location coordinates of the nodes are fixed.

4.2.2 Cluster formation

Cluster formation phase clusters the sensor nodes by taking the location coordinates into account. The nodes present in each grid forms a cluster of sensor nodes. This work deploys equal count of nodes in all the grids and therefore, all the clusters of the network are equally sized. However after the formation of clusters, it is necessary to employ a superior node as the CL. The CL nodes must be capable to manage, monitor and control the activities of its CM nodes. In order to select the superior node as CL, the proposed work relies on the trust point, which is computed by several trust metrics. This work chooses three important trust metrics to calculate the trust point and they are packet forwarding rate, energy level and node honesty.

The reason for choosing these trust metrics is that the forwarding tendency of the nodes can be decided by analysing the packet forwarding rate. In certain cases, the node may not show interest towards forwarding the packet. The energy is the basic requirement for the sensor nodes to perform any kind of operations. Hence, energy is considered as one of the metrics. Finally, the node's honesty is taken into account. The honesty of the node is measured by the node's intention towards modification of packets, before sending it to the destination. The packet forwarding entity has to forward the packets without any alteration being done to the packets. However, the malicious nodes tend to alter the packets being the process of packet forwarding. This misbehaviour can be detected by tracking the node honesty. All these trust metrics contribute to the trust point computation. The coming section elaborates the computation of trust point.

4.2.3 Trust point (τ) computation

The trust point is computed by clubbing three different trust metrics, which are packet forwarding rate (ρ), energy (ε) and node honesty (η). ρ is the most important trust metric, which measures the nodes tendency towards forwarding packets. ρ is computed by the total count of forwarded packets to the total count of received packets. The value of ρ ranges between 0 and 1. In case, if the node forwards no single packet even when it receives multiple packets, then the ρ is 0. Suppose, if a node forwards all the packets whichever is received, then the ρ is 1. In case of node's selective forwarding of packets, the value of ρ ranges from 0.1 to 0.9. The energy of a node is represented by ε. Initially, all the nodes have full (100%) battery backup. Based on the node's activity, the node's energy starts to drop. When the node has full and null energy backup, the value of ε is 1 and 0 respectively. The energy threshold is 0.3 and is computed by trial and error method. At any instant of time, when the energy level of the node drops below 0.3, the node's state is switched from working to sleeping state. Finally the node's honesty (η) is rated as 1, when the node doesn't attempt to alter or delete the packet before forwarding the packet. On the contrary, the node's honesty is rated as 0, when

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

the node alters or deletes the packet before forwarding. All these trust metrics are summed up together for computing the trust point and the average score is computed. The trust point computation is given below.

$$\delta = \rho + \varepsilon + \eta \quad (1)$$

$$\tau = \frac{\delta}{3} \quad (2)$$

The value of τ ranges between 0 and 1. The value 0 indicates that the node involves malicious behaviour. Conversely, the value 1 indicates that the node is completely trustworthy and is suitable to play the role of a CL. The nodes which score below 0.3 are blocked from participating in the activities of the network.

4.2.4 Activity of BS

The BS alone is mobile in this work and so, it reaches all the grids for every two rounds. The BS reaches each and every grid and selects the CL and working nodes. The selection is based on the trust point. The node with greatest trust point is selected as CL and the next two nodes are selected as working nodes. In case of energy drop below 0.3, the nodes are recycled at any instant of time. The BS monitors the nodes for a period of time and computes the trust point. All the nodes in a grid register itself with the BS by sending its' unique identifier and location coordinates.

The CL tracks the energy level of the working nodes and whenever it reaches below energy threshold, the nodes are recycled immediately. The packet flow of the CL is analysed by the BS, since node-to-node communication is not allowed here. The working nodes can communicate with CL alone and CL is the node with greatest trust point. Thus, there is no chance for CL node to misbehave. Though, in order to tighten the security, the packet flow of CL node is checked by the BS. In case of minimized packet outflow, the node is considered to be malicious and blocked. By this way, the selective forwarding and replay attacks can be detected. As the BS reaches and controls the grid for a regular interval of time, the possibility of snooze attack is overthrown. The overall algorithm of the proposed work is presented below.

SCTTM - work principle

Input : Sensor nodes, T, α
Output: Node cluster
Begin
//Area division
Split the network area into equal sized grids;
Deploy equal number of nodes in all the grids;
//Cluster formation
Form clusters with the nodes of each grid;
//On BS arrival
Store node's ID and location coordinates;
For each grid
BS observes the sensor nodes for t;
Compute τ;
Select CL and working nodes based on τ;
Do
Check current energy ce;
If ce<energy threshold;
Recycle node;
Check pf;
If i=o then normal
Else if i=2o then suspicious
Else malicious;
End;

As mentioned in the algorithm, the proposed work is observed to be secure against replay, selective forwarding, snooze and impersonation attacks. The CL and the working nodes are selected by taking the trust point into consideration. Besides this, the control over the count of working nodes per grid conserves as much energy as possible. The network area separation provides modularity and efficiency. The performance of the proposed work is analysed and the experimental results are presented in the forthcoming section.

5. PERFORMANCE ANALYSIS

The working ability of the SCTTM is analysed and compared with ECTTM [17] and ECTMRA [18]. The comparison is done with respect to the energy consumption, attack detection rate and network lifetime. The network lifetime is analysed by varying the working nodes. Finally, the malicious nodes are randomly distributed and the attack detection rate with respect to rounds is measured. The size of the network is chosen as 100 by 100 metre square and the grid size is set as 10 by 10 metre square. The experimentation procedure varies the count of deployed nodes between 100 and 2000. Besides this, the count of working nodes is varied as 2, 5 and 10 for analysis.

5.1 Network Lifetime w.r.t Working Nodes

The count of working nodes lays a serious impact over the lifetime of the network. Whenever the number of working nodes is

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

increased, it is found that the lifetime of the network is decreased to some extent. In order to show the impact of working nodes over network life, we vary the working nodes as 2, 5, 10 and 15. The results are presented in figure 1.

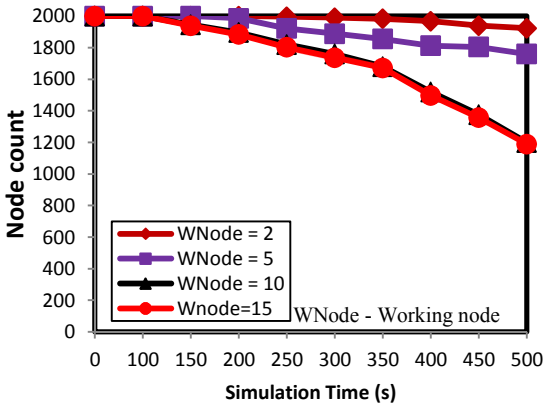

Figure 1: Network Lifetime w.r.t Wnode

When the number of working nodes is fixed as 2, the network consists of 1923 nodes. However, on increasing the count of working nodes to 15, the network has 1189 nodes alive. From the count of live nodes, the importance of setting the working nodes can be understood.

5.2 Network Lifetime w.r.t Working Nodes Per Grid

The lifetime of the network is again analysed by differentiating the working nodes per grid. The number of nodes per grid is adjusted as 5, 10, 15 and 20, for which the working nodes are varied as 3 and 5. The experimental results are shown in fig 2.

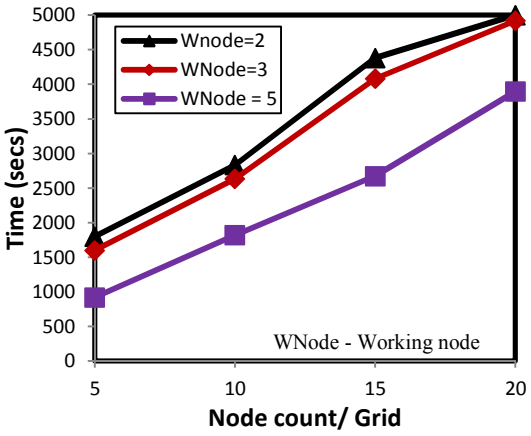

Figure 2: Network Lifetime w.r.t. Node Count per Grid

5.3 Energy Consumption

The energy consumption pattern of the SCTTM is analysed in this section. Initially, all the nodes are supplied with equal amount of energy, which is 60 joules. The average energy consumption of the nodes is measured with respect to simulation time. The energy consumption results are presented in figure 3.

From the experimental results, it can be observed that the lesser number of working nodes shows better network lifetime, irrespective of the number of nodes per grid. When the number of working nodes is set as 2, the network lifetime is about 5000 seconds. Similarly, when the working nodes are fixed as 3 and 5, the network lifetime is decreased to 4920 and 3897 seconds respectively.

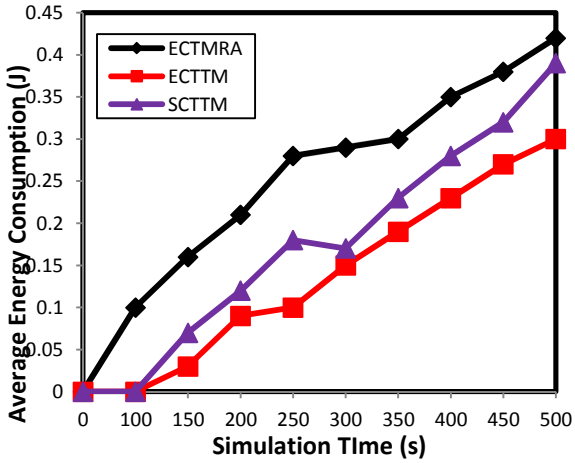

Figure 3: Energy Consumption

The above presented graph states that the energy consumption of the proposed work is little bit greater than ECTTM. This is because of tracking the packet flow of the nodes and to combat against security threats. However, security preservation along with energy conservation is the major goal of this work.

5.4 Network Lifetime Analysis w.r.t Node Count

Journal of Theoretical and Applied Information Technology
15th March 2017. Vol.95. No 5

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

The overall lifetime of the network is analysed in this section. The network lifetime is checked with respect to the node count. The results are shown in the below given graph (figure 4).

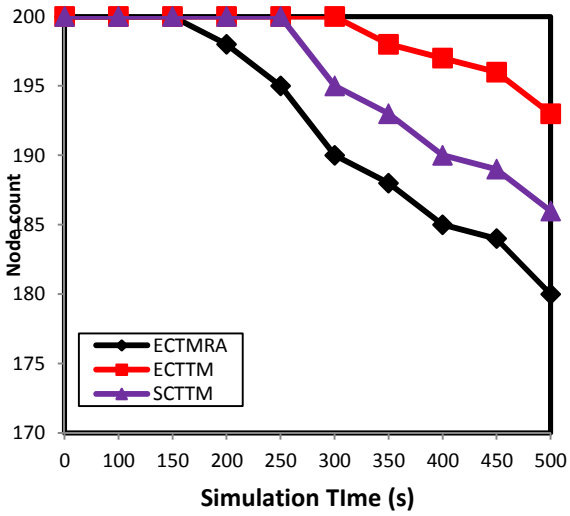

Figure 4: Network Lifetime Analysis

The experimental results show that the network lifetime of SCTTM is lesser than ECTTM, because of enforcing security policies. The enforcement of security policies consumes additional energy and thus the lifetime of the network is minimized. This makes SCTTM to be secure against impersonation, snooze, selective forwarding and replay attacks.

5.5 Attack Detection Rate

The attack detection rate for snooze, impersonation, selective forwarding and replay attacks is presented in the below given graph. We randomly distribute some malicious nodes to check the potentiality of the proposed work. All these attacks are easily detected because of the trust point. The regular arrival of BS enhances the security of the system. BS continuously monitors the status of the nodes, which results in improved security. The experimental results are presented in the below given figure 5.

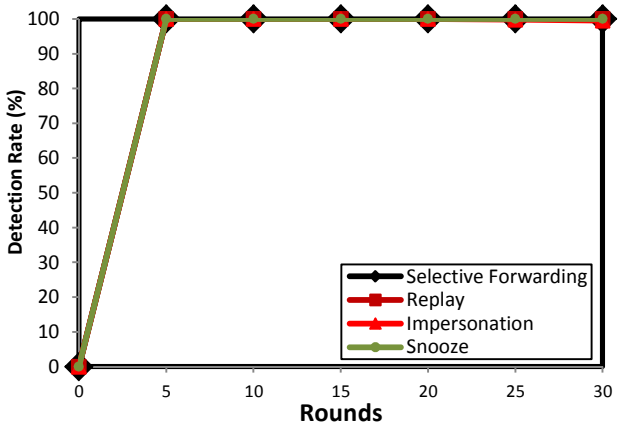

Figure 5: Attack Detection Rate

The above diagram shows that SCTTM detects all the four attacks to its best. The attack detection rate is cent percent, because the BS reaches all the grids for every period of time. It monitors the real status of the nodes and takes actions accordingly. Thus, it detects the attacks all at once.

6. CONCLUSIONS

This article presents a "Secure Cluster based Trustworthy Topology Management Scheme" (SCTTM) for wireless sensor networks. The main objective of this work is to provide security and to conserve energy, so as to improve the lifetime of the network. This work follows the concept of modularity, such that the network area is separated into several equal sized grids and the nodes are equally distributed. The BS reaches all the grids for every time interval to check and monitor the status of nodes. Besides this, BS is the authority to select CL and working nodes. The proposed work is tested against several performance measures and the work prove to be secure and energy efficient. However, the proposed work is resistant against only four attacks, which are selective forwarding, replay, snooze and impersonation attacks. In future, the optimal count of working nodes can be computed by optimization techniques.

References

[1] Gengzhong Z, Qiumei L. A survey on topology control in wireless sensor networks. InFuture Networks, 2010. ICFN'10. Second International Conference on 2010 Jan 22 (pp. 376-380). IEEE.

[2] Wang X, Sheng M, Liu M, Zhai D, Zhang Y. RESP: A k-connected residual energy-aware topology control algorithm for ad hoc

networks. In2013 IEEE Wireless Communications and Networking Conference (WCNC) 2013 Apr 7 (pp. 1009-1014). IEEE.
[3] Li L, Halpern JY, Bahl P, Wang YM, Wattenhofer R. A cone-based distributed topology-control algorithm for wireless multi-hop networks. IEEE/ACM Transactions on Networking. 2005 Feb;13(1):147-59.
[4] Li N, Hou JC. FLSS: a fault-tolerant topology control algorithm for wireless networks. InProceedings of the 10th annual international conference on Mobile computing and networking 2004 Sep 26 (pp. 275-286). ACM.
[5] Li N, Hou JC. Localized fault-tolerant topology control in wireless ad hoc networks. IEEE Transactions on Parallel and Distributed Systems. 2006 Apr;17(4):307-20.
[6] Wang L, Jin H, Dang J, Jin Y. A fault tolerant topology control algorithm for large-scale sensor networks. InEighth International Conference on Parallel and Distributed Computing, Applications and Technologies (PDCAT 2007) 2007 Dec 3 (pp. 407-412). IEEE.
[7] Blough DM, Leoncini M, Resta G, Santi P. The k-neigh protocol for symmetric topology control in ad hoc networks. InProceedings of the 4th ACM international symposium on Mobile ad hoc networking & computing 2003 Jun 1 (pp. 141-152). ACM.
[8] Chen Y, Son SH. A fault tolerant topology control in wireless sensor networks. InThe 3rd ACS/IEEE International Conference onComputer Systems and Applications, 2005. 2005 (p. 57). IEEE.
[9] Chen B, Jamieson K, Balakrishnan H, Morris R. Span: An energy-efficient coordination algorithm for topology maintenance in ad hoc wireless networks. Wireless networks. 2002 Sep 1;8(5):481-94.
[10] Kumar S, Lai TH, Balogh J. On k-coverage in a mostly sleeping sensor network. InProceedings of the 10th annual international conference on Mobile computing and networking 2004 Sep 26 (pp. 144-158). ACM.
[11] Zhan G, Shi W, Deng J. Design and implementation of TARF: a trust-aware routing framework for WSNs. IEEE Transactions on dependable and secure computing. 2012 Mar;9(2):184-97.
[12] Raje RA, Sakhare AV. Routing in wireless sensor network using fuzzy based trust model. InCommunication Systems and Network Technologies (CSNT), 2014 Fourth International Conference on 2014 Apr 7 (pp. 529-532). IEEE.
[13] Crosby GV, Pissinou N, Gadze J. A framework for trust-based cluster head election in wireless sensor networks. InSecond IEEE Workshop on Dependability and Security in Sensor Networks and Systems 2006 Apr 24 (pp. 10-pp). IEEE.
[14] Wang W, Du F, Xu Q. An improvement of LEACH routing protocol based on trust for wireless sensor networks. In2009 5th International Conference on Wireless Communications, Networking and Mobile Computing 2009 Sep 24 (pp. 1-4). IEEE.
[15] Heinzelman WR, Chandrakasan A, Balakrishnan H. Energy-efficient communication protocol for wireless microsensor networks. InSystem sciences, 2000. Proceedings of the 33rd annual Hawaii international conference on 2000 Jan 4 (pp. 10-pp). IEEE.
[16] Rezgui A, Eltoweissy M. Tarp: A trust-aware routing protocol for sensor-actuator networks. In2007 IEEE International Conference on Mobile Adhoc and Sensor Systems 2007 Oct 8 (pp. 1-9). IEEE.
[17] Senthil T, Kannapiran B. ECTTM - Energy Conserving Trustworthy Topology Management Mechanism for Wireless Sensor Networks. Under Review. IJET
[18] Senthil T. Kannapiran B. ECTMRA: Energy Conserving Trustworthy Multipath Routing Algorithm based on Cuckoo Search Algorithm. Wireless Personal Communications, Vol. 88, No. 3, 2016.

Author's Profile

T.Senthil works as a Senior Assistant Professor of Electronics and Communication Engineering Department at Kalasalingam University, Tamil nadu, India. He received his B.E and M.E degree from MK University, India with specialization in Electronics and communication engineering and Microwave & optical engineering in 1988 and 1997 respectively. He has more than twenty years of teaching experience and has published papers in National/International conferences and Journals. His current research focus is on energy efficient protocols in wireless sensor networks. He is the life member of ISTE.

B. Kannapiran was born in 1980. He obtained his

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Bachelor degree in Instrumentation and Control Engineering from Madurai Kamaraj University, India in 2001 and Master degree in Applied Electronics from Madurai Kamaraj University, India in 2002. He also obtained hid Ph.D degree from Anna University Chennai, India in 2013. Presently he is working as Associate Professor in the Department of Instrumentation and Control Engineering, Kalasalingam University. He has published papers in International journals, National and International Conferences. His research topics include soft computing, Fault Diagnosis.