November-December 2019
ISSN: 0193-4120 Page No. 5108 - 5114

Real Time Dynamic Node Scheduling and Key Distribution based Secure Routing in WSN for Improved Lifetime Maximization

R. Senthil Kumar,

Ph.D Research Scholar, Department of Computer Science, VMRF-DU, Salem, e-mail :tclsenthil@gmail.com

Dr. M. Prakash,

Research Supervisor, Department of Computer Science, VMRF-DU, Salem, e-mail: prakashmanis@gmail.com

Article Info
Volume 81
Page Number: 5108 - 5114
Publication Issue:
November-December 2019

Article History
Article Received: *5 March 2019*
Revised: *18 May 2019*
Accepted: *24 September 2019*
Publication: *24 December 2019*

Abstract
The problem of lifetime maximization and secure routing in Wireless Sensor Networks (WSN) has been well studied. Number of techniques available for the secure connectivity and data transmission in WSN. The methods suffer to achieve expected performance in secure routing in WSN and struggle to achieve higher lifetime of network. To improve the performance, an dynamic scheduling and key distribution algorithm is described in this article. The lifetime of network is highly depending on the energy parameter and by scheduling the nodes of WSN the lifetime of network can be improved highly. The scheduling algorithm maintains the node status and energy details in triggering the nodes status. At each session, the method discovery the routes to reach the destination and eliminates the poor energetic routes. For each route, the method estimates the secure routing weight (SRW) and based on that, the method selects a single route to reach the destination. For the nodes of route, the method distributes a key which is active for the current session. The nodes of the selected route only will be active for the session and the rest will be in silent mode. The proposed method improves the performance of security and lifetime of the network.

Keywords: *WSN, Secure Routing, Key Distribution, Dynamic Scheduling, SRW, Lifetime Maximization, QoS.*

I. Introduction:

The wireless sensor network has been a dominant network being used in many domains and can be deployed in a rapid way to support many problems. However, the network can be deployed in rapid way, they have few limitations in terms of energy of nodes and security. As the nodes of WSN have limited power and they can transmit only with the nodes located within the transmission range, the lifetime of the network is highly depending on the energy or power of the nodes. Each transmission claims certain amount of power, the involvement of each sensor node affect the lifetime of the network. Still, to achieve higher quality of service, the energy of the nodes should be used in efficient manner.

The Quality of service (QoS) of the network is depending on many parameters like throughput performance. The throughput performance is depending on the packet delivery and by improving the packet delivery ratio, the throughput performance of the network can be improved. Similarly, the security plays vital role in achieving higher throughput performance. By reducing the packet drop ratio, the throughput performance can be improved. Also, the routing strategy is an important factor to be considered to achieve higher QoS. All these parameters should be considered for the improvement of QoS in WSN.

Scheduling of nodes between sleep and Active conditions is the major issue in utilizing

the power of sensor nodes. Because, when the node is active it spends some amount of energy in listening the incoming signals. By scheduling the nodes properly, the energy of nodes can be used efficiently. There are number of scheduling algorithms available for WSN. For example, the time domain based approaches triggers the status of the nodes in alternate session or time. However, they lose some amount of energy even without participate in any data transmission for the whole time window. To handle this issue, some strategic approaches are necessary. This paper introduces a dynamic scheduling algorithm which acts on each session but triggers only the required nodes to be up and let the other nodes to be sleep for the session.

The security in routing is major concern in this paper. When there exist a malicious node, then entire communication would get spoiled, which must be override completely. To achieve this, a secure routing algorithm is prescribed in this paper. The method would distribute the keys only to the nodes present in the route being selected which improves the security in routing. The key distribution is performed at each session but without any overhead which is followed by the scheduling and the keys are distributed only to the nodes being selected for transmission. The detailed approach is presented the remaining section.

II. RelatedWorks:

There are number of methods available for the secure routing and lifetime maximization of WSN. This section discusses some of the methods related to the problem.

In [1], the author present a energy efficient optimized routing with higher security (EOSR) which works based on the trust of nodes. The trust evaluation is performed in distributed manner which identifies the malicious nodes and isolate them from data transmission. According to the trusts of the nodes and energy, an optimal route has been selected for data transmission.

In [2], an trusted routing with security has been presented for WSN which generates active routes in a dynamic way which avoids black holes. This helps the detection of malicious nodes in rapid manner. The energy of nodes has been used for the efficient detection and to perform secure routing.

Energy efficient Secured Routing model for wireless sensor networks [3], present Hierarchical Cluster Defining Module in which sensor node are divided into number of groups that is called as cluster & define cluster head for each cluster. This cluster head covers a maximum amount of distance and increases the lifetime of the wireless sensor network.

In [4], the author analyzes various secure routing protocols and discusses a novel algorithm which uses energy constraints.

In [5], the author proposes a new secure protocol based on the well-known LEACH routing protocol named Hybrid Cryptography-Based Scheme for secure data communication in cluster-based WSN (HCBS). As a multi-constrained criteria approach, HCBS is built on a combination of the cryptography technique based on Elliptic Curves to exchange keys that uses symmetric keys for data encryption and MAC operations.

In [6], a trust orient approach is developed a novel protocol for the secure routing of WSNs, and named as Trust-Distrust Protocol (TDP). The proposed protocol has four stages, initial stage is topology management, where an improved k-means algorithm is applied. Then the second stage is Link Quality Appraisal, which means fitness evaluation of every nodes in the network. The third stage is Grading, in which based on the fitness value a grade point is allotted to every node. In the last stage the secure path for the routing is determined based on grade point.

Secure routing against DDoS attack in wireless sensor network [7], introduced a secure routing protocol for WSNs, which is able to prevent the network from DDoS attack. The method scan the infected nodes using the proposed algorithm and block that node from any further activities in the network. To protect the network we use intrusion prevention scheme, where specific nodes of the network acts as IPS node. These nodes operate in their radio range for the region of the network and scan the neighbors

regularly. When the IPS node find a misbehavior node which is involves in frequent message passing other than UDP and TCP messages, IPS node blocks the infected.

A novel approach to secure routing protocols in WSN [8], proposed secure and trustable routing technique with utilizing multi data flow topologies (MDT) scheme to defend against this attack and proposed a suite of optimization methods to minimize the energy cost while keeping the system's security in a sufficient level.

In [9], an energy based secure routing protocol for multiple tiers has been presented. The nodes are clustered to perform secure routing and reduce overhead by data transmission. The clustering is performed with K means and the cluster heads is selected according to the energy of nodes.

Wireless sensor networks: Routing protocols and security issues [10], classifies various routing algorithms and analyze various performance measures in detail.

Trust based secure routing protocol using fuzzy logic in wireless sensor networks [11], is proposed in order to obtain the secured routing. The proposed method uses the Bio-inspired Energy Efficient-Cluster (BEE-C) protocol and fuzzy logic to calculate the trust of the nodes. The proposed method finds the black hole and flooding attack and eliminates the attack. The trust values are compared with the threshold value. The trust values above the threshold are considered as trusted nodes and the packets are passed through the node. The trust value below the threshold value is termed as untrusted node and is eliminated.

In [12], the author present a behavior based secure routing algorithm to support the performance development of wireless sensor networks.

Trust and packet load balancing based secure opportunistic routing protocol for WSN [13], presents a new trust and packet load balancing based opportunistic routing (TPBOR) protocol. The proposed protocol is energy efficient and secure by utilizing the trusted nodes in the routing process. Also the proposed protocol balance the overall network traffic and distribute the traffic load equally in the network.

All the methods discussed above suffer with the poor performance in routing and introduces less lifetime of the networks.

Real Time Dynamic Node Scheduling and Key Distribution Based Secure Routing:

The proposed dynamic scheduling and key distribution based routing algorithm identifies the routes. For the routes identified, the method collects the status of nodes to estimate the weight for secure routing. Based on the weight measured, the method selects a single route to involve in transmission. Further, the method schedules the nodes of route and distributes the keys to perform secure routing. The detailed approach is discussed below.

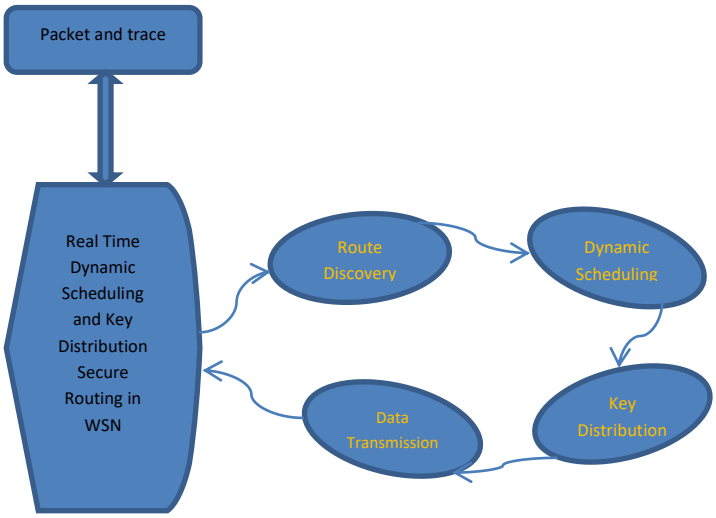

Figure 1: Architecture of proposed Dynamic Scheduling and Key Distribution Routing

The Figure 1, sows the architecture of proposed dynamic routing and key distribution based secure routing algorithm and shows the stages involved. Each section has been detailed clearly in this section.

Route Discovery:

The route discovery is performed based on the network topology. The topology contains the

November-December 2019
ISSN: 0193-4120 Page No. 5108 - 5114

location information's of different sensor nodes. For each sensor nodes, the method identifies the location, energy parameters. Using these details and with the transmission range, the list of nodes within the range are identified as neighbors. Based on these information's, the method identifies the list of routes available in the network.

Input: Network Topology Nt, Node Table NoT

Output: Route List Rl

Start

Read Nt and NoT

For each node n

Identify location and energy

Nl = $\int \sum$ Nodes $\in$ NT

Node Statistic Ns = $\int_{i=1}^{size\ (Nl)}$ Nl(i). Loc & Nl(i). Energy

End

For each node n

Identify list of neighbors

Nelist = $\int_{i=1}^{size\ (Nl)} \sum$ Nl(i). loc <> *Transmission range (n).*

End

For each node n

Identify list of route to reach destination.

Rl = $\int_{i=1}^{size\ (neighbors\ (n))}$ Routes → destination

End

Stop

The working principle of route discovery approach has been presented above which uses node statistics and topology.

Secure Routing Weight Estimation:

The weight of route for secure routing isestimated based on different parameters namely energy, number of hops and number of transmission involved through the route and so on. Using these information, the method estimates the secure routing weight for the route given. Estimated weight is used for the selection of route and perform scheduling towards data transmission.

Algorithm:

Input: Route R, Network Trace Nt

Output: SRW.

Start

Read route R and Network trace Nt.

Identify list of hops H = $\sum$ Hops $\in$ R

Compute energy support Es = $\int_{i=1}^{size\ (H)} \frac{\sum_{i=1}^{size\ (Nt)} Nt(i).Route \in H(j)}{\sum InitialEnergy\ \ (H(j))}$

Compute SRW = ES$\times \frac{1}{\sum_{i=1}^{size\ (Nt)} Nt(i).Route == R}$

Stop

The working principle of route support weight estimation is presented above and used for route selection.

Dynamic Scheduling:

The scheduling of nodes of sensor network is performed according to different conditions of the sensor nodes. First, the list of routes available are identified and for each route identified, the method estimates the secure routing weight (SRW). Based on the value of SRW, a single route with maximum weight has been selected. The nodes of route being selected have been scheduled to be wake and rests of the nodes are scheduled as sleep. The scheduled route and nodes are used to perform data transmission.

Algorithm:

November-December 2019
ISSN: 0193-4120 Page No. 5108 - 5114

Input: Network Topology NT, Network Trace NeT

Output: Boolean

Start

Read NT and NeT

For each session

Route List Rl = Perform Route Discovery

For each route R

SRW = Estimate Secure Routing Weight.

End

Route R = Choose route with maximum SRW.

Identify hops of R as Hl = $\sum$ Hops $\in$ R

For each hop h

If $\int_{i=1}^{size\,(NT)} if(NT(i) \in Hl) then$

Schedule as wake

Else

Schedule as sleep.

End

End

Perform Key Distribution.

Perform Data Transmission.

End

Stop

The working principle of scheduling is presented above which shows how the route being selected to support secures routing.

Key Distribution:

The key distribution is performed according to the result of scheduling performed. The method receives a route from scheduling algorithm. Upon receiving a route, the method generates a key which is dedicated for the current session. Generated key has been forwarded to the destination through the route selected. The same key has been used for both encryption and decryption of the data being forwarded.

Algorithm:

Input: Route R

Output: Null

Start

Read Route R

Key k = $\int$ Random(KeySet)

Forward key through the route R.

Stop

The above discussed algorithm shows how the key for the session has been generated and used for both routing and data security.

Data Forwarding:

The data forwarding is performed through the route being given for the session. The method encrypts the data with the key given and forwarded to the next hop present in the route given. When the data reaches the destination, the node decrypts the data with the same key to obtain the original data.

III. Results and Discussion:

The proposed dynamic scheduling and secure routing algorithm has been implemented in network simulator NS2. The method has been evaluated for its efficiency in various parameters. The method has been verified for its performance in different parameters. The results obtained have been presented in this section.

Parameter	Value
Simulator	NS2
Number of Nodes	100
Transmission Range	100 meters
Residual Energy	100 Joules
Simulation Area	100 meters
Simulation Time	15 minutes

Table 1: Simulation Details

The simulation conditions considered for performance evaluation is displayed in Table 1.

November-December 2019
ISSN: 0193-4120 Page No. 5108 - 5114

According to this, the DSKDR algorithm produces efficient results and compared with the results of other methods.

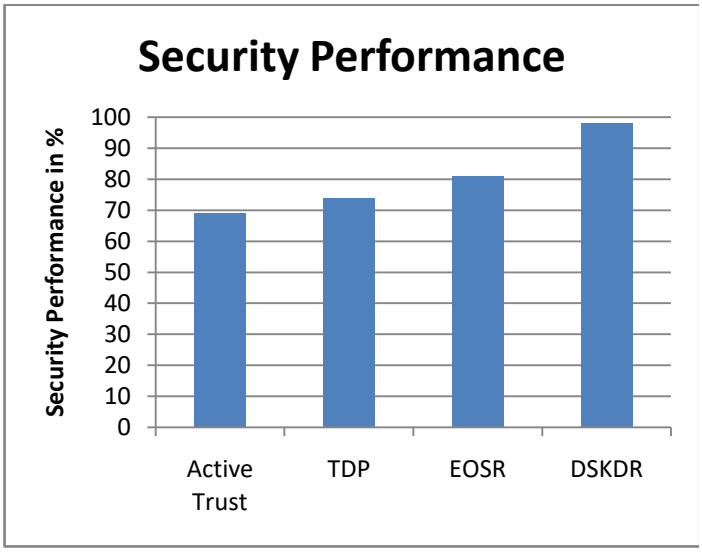

Figure 2: Performance on security

The security performance achieved by DSKDR algorithm is measured and compared with the results of other methods in Figure 2. The proposed DSKDR (Dynamic Scheduling and Key Distribution Routing) algorithm has achieved noticeable growth in security than other methods.

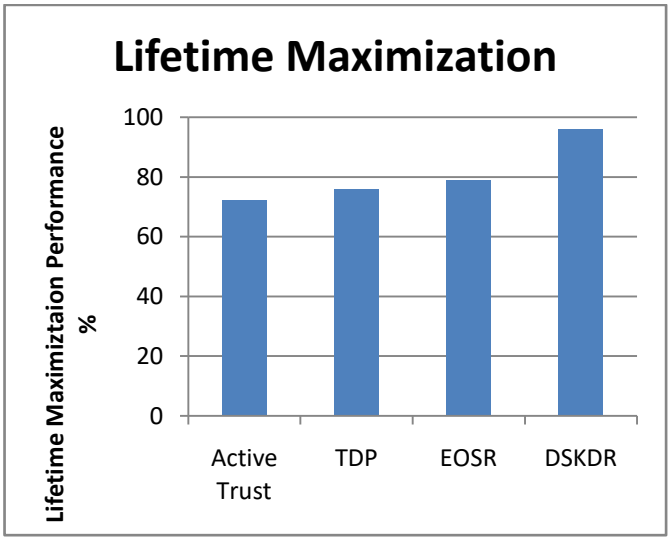

Figure 3: Performance on lifetime maximization

The performance on lifetime maximization has been measured and compared with the result of other methods. The proposed DSKDR algorithm has produced higher performance on lifetime maximization than other methods.

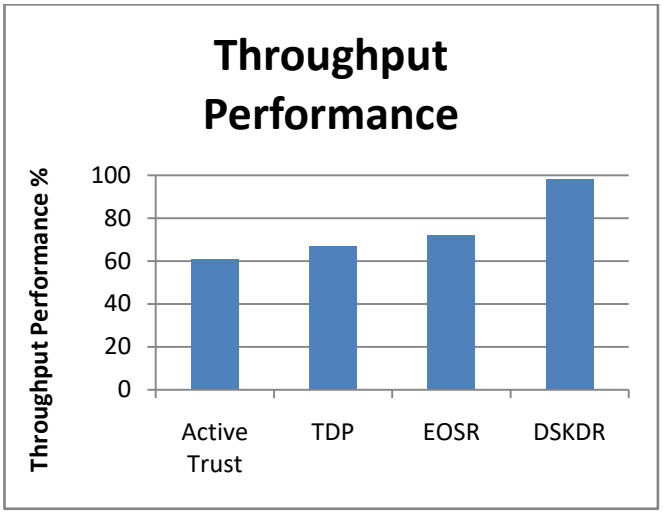

Figure 4: Performance on throughput

The throughput performance achieved by different algorithms are measured and analyzed. The proposed DSKDR algorithm has produced higher throughput performance than other methods.

IV. Conclusion:

This paper presents a dynamic scheduling and key distribution based secure routing algorithm for the lifetime maximization of wireless sensor networks. The method monitors the conditions of the network and uses the topology of the network. Based on the details of topology and nodes statistics, the method identifies the list of routes at each session. Each route has been measured for the secure routing support value and identifies the route with maximum value. For the selected route the key has been distributed to perform secure communication. Similarly, the nodes other than the hops of selected route have been scheduled for sleep mode. This improves the lifetime maximization and improves the throughput performance. Similarly, the security performance is improved by encrypting the data with key allotted for the session and there is no overhead in distributing the keys because it has been forwarded to the destination and all the nodes of the route just like a data transmission.

References:

November-December 2019
ISSN: 0193-4120 Page No. 5108 - 5114

[1] TaoYang, A secure routing of wireless sensor networks based on trust evaluation model, ELSEVIER, Procedia Computer Science, Volume 131, 2018, PP 1156-1163.

[2] Y. Liu, M. Dong, K. Ota and A. Liu, "ActiveTrust: Secure and Trustable Routing in Wireless Sensor Networks," IEEE (IFS), volume 11, number 9, pp. 2013-2027, 2016.

[3] V. P. Bawage and D. C. Mehetre, "Energy efficient Secured Routing model for wireless sensor networks," IEEE (ICACDOT), 2016, pp. 865-869.

[4] FarruhIshmanov, Trust Mechanisms to Secure Routing in Wireless Sensor Networks: Current State of the Research and Open Research Issues, HINDAWI, Journal of Sensors, 2017.

[5] F. Mezrag, S. Bitam and A. Mellouk, "Secure Routing in Cluster-Based Wireless Sensor Networks," IEEE, (GLOBECOM), 2017, pp. 1-6.

[6] S. Karthick, E. S. Devi and R. V. Nagarajan, "Trust-distrust protocol for the secure routing in wireless sensor networks," IEEE (ICAMMAET), 2017, pp. 1-5.

[7] S. Nagar, S. S. Rajput, A. K. Gupta and M. C. Trivedi, "Secure routing against DDoS attack in wireless sensor network," IEEE (CICT), 2017, pp. 1-6.

[8] B. Patil and R. Kadam, "A novel approach to secure routing protocols in WSN," IEEE (ICISC), 2018, pp. 1094-1097.

[9] GeetikaDhand, SMEER: Secure Multi-tier Energy Efficient Routing Protocol for Hierarchical Wireless Sensor Networks, SPRINGER, Wireless Personal Communications, Issue 1, 2019.

[10] Anjali, Shikha and M. Sharma, "Wireless sensor networks: Routing protocols and security issues," IEEE (ICCCNT), 2014, pp. 1-5.

[11] S. Renubala and K. S. Dhanalakshmi, "Trust based secure routing protocol using fuzzy logic in wireless sensor networks," IEEE(ICR), 2014, pp. 1-5.

[12] RenuBala, Secure Routing in Wireless Sensor Network, (IJCSMC), IJCSMC, Vol. 4, Issue. 5, 2015, pp 966 – 973.

[13] N. Kumar and Y. Singh, "Trust and packet load balancing based secure opportunistic routing protocol for WSN," IEEE (ISPCC), 2017, pp. 463-467.